





Review

Enhancing Cybersecurity and Privacy Protection for Cloud Computing-Assisted Vehicular Network of Autonomous Electric Vehicles: Applications of Machine Learning

Tiansheng Yang ^{1,*} , Ruikai Sun ^{2,*} , Rajkumar Singh Rathore ³  and Imran Baig ³ ¹ South Wales Business School, University of South Wales, Cardiff CF37 1DL, UK² Cardiff Business School, Cardiff University, Cardiff CF10 3EU, UK³ Cardiff School of Technologies, Cardiff Metropolitan University, Llandaff Campus, Cardiff CF5 2YB, UK; rsrathore@cardiffmet.ac.uk (R.S.R.); ibaig@cardiffmet.ac.uk (I.B.)

* Correspondence: tiansheng.yang1@southwales.ac.uk (T.Y.); sunr10@cardiff.ac.uk (R.S.)

Abstract: Due to developments in vehicle engineering and communication technologies, vehicular networks have become an attractive and feasible solution for the future of electric, autonomous, and connected vehicles. Electric autonomous vehicles will require more data, computing resources, and communication capabilities to support them. The combination of vehicles, the Internet, and cloud computing together to form vehicular cloud computing (VCC), vehicular edge computing (VEC), and vehicular fog computing (VFC) can facilitate the development of electric autonomous vehicles. However, more connected and engaged nodes also increase the system's vulnerability to cybersecurity and privacy breaches. Various security and privacy challenges in vehicular cloud computing and its variants (VEC, VFC) can be efficiently tackled using machine learning (ML). In this paper, we adopt a semi-systematic literature review to select 85 articles related to the application of ML for cybersecurity and privacy protection based on VCC. They were categorized into four research themes: intrusion detection system, anomaly vehicle detection, task offloading security and privacy, and privacy protection. A list of suitable ML algorithms and their strengths and weaknesses is summarized according to the characteristics of each research topic. The performance of different ML algorithms in the literature is also collated and compared. Finally, the paper discusses the challenges and future research directions of ML algorithms when applied to vehicular cloud computing.

Keywords: machine learning; vehicular networks; vehicular edge computing; vehicular fog computing; privacy preserving; secure communication



Academic Editor: Jiangtao Li

Received: 22 November 2024

Revised: 19 December 2024

Accepted: 24 December 2024

Published: 28 December 2024

Citation: Yang, T.; Sun, R.; Rathore, R.S.; Baig, I. Enhancing Cybersecurity and Privacy Protection for Cloud Computing-Assisted Vehicular Network of Autonomous Electric Vehicles: Applications of Machine Learning. *World Electr. Veh. J.* **2025**, *16*, 14. <https://doi.org/10.3390/wevj16010014>

Copyright: © 2024 by the authors. Published by MDPI on behalf of the World Electric Vehicle Association. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the development of communication technology and vehicle engineering, vehicular networks combining vehicles and the Internet can increase the efficiency of the whole transport system, improve user experience, reduce environmental pollution, and bring economic benefits. Vehicular cloud computing (VCC) is an emerging technology that combines the features of vehicular networks and cloud computing to further enhance the resource utilization and communication efficiency of vehicular networks. Although VCC has many advantages, new variants of VCC, such as vehicular edge computing (VEC) and vehicular fog computing (VFC), have emerged to support the increasingly powerful application software in vehicular networks. The vehicular network architecture that incorporates these new computing paradigms consists of an on-board unit (OBU), edge

devices/fog nodes, a roadside unit (RSU), and cloud servers [1]. As illustrated in Figure 1, the structure of cloud computing-assisted vehicular networks. Information is transmitted from sensors to the vehicular network and then connected to the main network via the edge network, resulting in different types of communication, such as vehicle-to-sensor (V2S), vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), infrastructure-to-infrastructure (I2I), and so on. However, the increase in the types of communication and participating nodes also poses challenges in terms of data security and privacy [2–5].

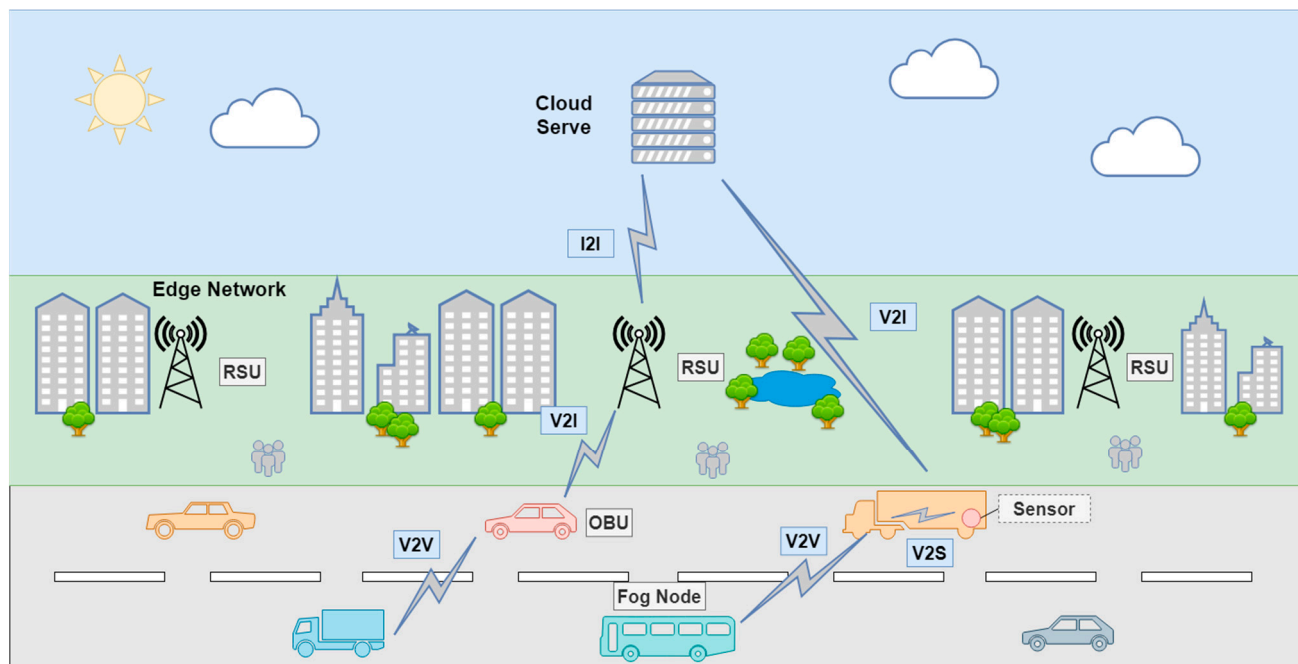


Figure 1. Vehicular network structure.

Cybersecurity protects computers, networks, programs, and data from attack, damage, or unauthorized access through technology and processes [6]. Privacy protection, on the other hand, prevents the disclosure of any information relating to an identifiable person. Both cybersecurity and privacy protection are critical to VCC adoption, as security vulnerabilities can reveal sensitive information, vehicle systems can be attacked, and even lead to large-scale traffic safety accidents. In 2015, a vulnerability was discovered in BMW's ConnectedDrive system that allowed an attacker to remotely unlock a vehicle's doors by simulating a BMW server communicating with the vehicle [7]. In the same year, security researchers discovered and demonstrated a vulnerability that allowed remote control of Jeep Cherokee vehicles [8]. An attacker accessing the vehicle's Uconnect system via the Internet could control critical functions such as braking, acceleration, and steering. In 2016, Tesla fixed a major security vulnerability in its Model S models via an OTA update that allowed an attacker to remotely control the vehicle's braking system [9]. Machine learning (ML) is widely used in the field of artificial intelligence and has rich applications in cybersecurity and privacy protection. The characteristics of data-driven, automated, and generalized capabilities of ML can be exploited to effectively monitor both known and unknown cybersecurity threats. There have been several literature reviews that have started to review the application of machine learning in vehicular networks [10–12] and the challenges of cybersecurity and privacy in vehicular networks [13–15]. The review on applying machine learning to address cybersecurity and privacy is based on all types of vehicular networks [13,16]. As per the information we collected so far, we can say that there has been no particular systematic literature review on cloud computing-assisted vehicular

networks. If not specifically stated, the vehicular cloud computing referred to in this paper includes its variants vehicular edge computing and vehicular fog computing.

This paper focuses on a specific research question. How can machine learning enhance cybersecurity and privacy in cloud computing-assisted vehicular networks? The four main contributions of this paper are as follows:

- (1) A comprehensive overview of computational paradigms and machine learning algorithms for vehicular networks is presented, describing the similarities and differences and the security and privacy challenges faced between VCC and variant computing paradigms (e.g., VEC and VFC).
- (2) Four key themes related to cybersecurity and privacy protection in VCC are summarized: intrusion detection system, anomaly vehicle detection, task offloading security and privacy, and privacy protection-related existing ML algorithms. The strengths and weaknesses of different ML algorithms are also shown.
- (3) A meta-analysis of ML algorithms' performances in intrusion detection systems is conducted.
- (4) The limitations of current ML algorithms to realize VCC network security and privacy protection are presented, and future research directions are discussed.

The rest of the paper is organized as shown in Figure 2.

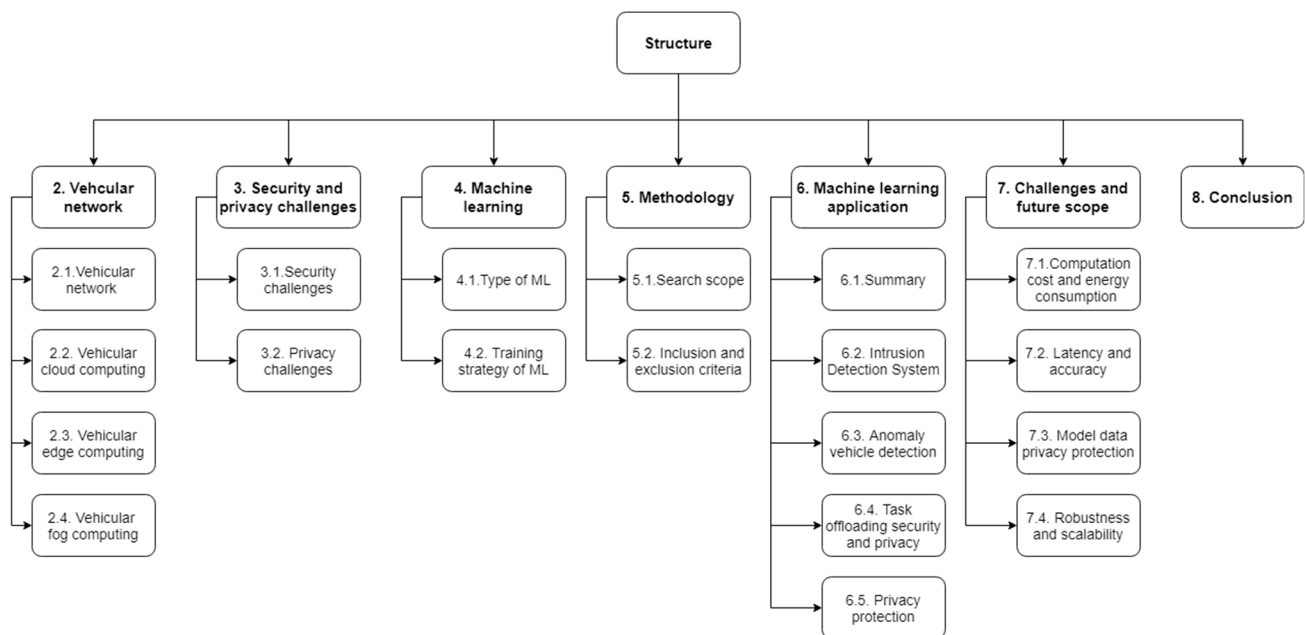


Figure 2. Structure of Context.

2. Vehicular Networks

2.1. Vehicular Networks Concept

A vehicular network is a network composed of automobiles with wireless connectivity. It serves as a platform to support various application software, including path planning, road safety, green transportation, and infotainment services, and is one of the most important supporting technologies for the realization of intelligent transportation systems [17,18]. In such a network, connected vehicles can communicate with their internal and external environments via an on-board unit (OBU) with sensing and communication capabilities [19]. This communication includes V2S, V2V, V2I, and vehicle-to-everything (V2X) communications [20,21]. These data channels to the vehicular information system ensure that drivers receive sufficient information and maintain vehicle situational aware-

ness in complex traffic environments. However, the huge amounts of data and the need for low-latency communication challenge the computational capabilities of vehicles [22–24]. To address these challenges, various computational paradigms can be utilized. The most common computing paradigms for vehicular networks include vehicular cloud computing, vehicular edge computing, and vehicular fog computing. Their similarities and differences are summarized in Table 1.

Table 1. Difference among VCC, VEC, VFC.

	VCC	VEC	VFC
Computer capabilities	Strong	Weak	Moderate
Storage capabilities	Strong	Weak	Moderate
Energy consumption	High	Low	Low
Mobility support	Weak	Strong	Strong
Geographical distribution	Centralized	Decentralized	Decentralized
Cloud serve distance	Far	Near	Near
Edge node	None	RSU	Mobility
Bandwidth cost	High	Low	Low
Latency	High	Low	Low

2.2. Vehicular Cloud Computing

In a traditional cloud-centric approach, data collected by individual vehicles is uploaded to a cloud-based server or data center for centralized processing. This approach leads to unacceptable latency and burdens the backbone network [25]. Therefore, VCC, which is created by combining vehicular networks with cloud computing, can effectively utilize the spare resources of the remaining vehicular computers in the vehicular network as shown in Figure 3. Compared with traditional clouds, the ownership of VCC resources is distributed and highly dynamic but also has much less communication and computational resources [26]. So sometimes vehicles with insufficient cloud computing resources will use an external cloud to ensure computing performance, which will significantly increase communication latency and costs [27]. Therefore, this computing paradigm is more suitable for scenarios with fixed clusters of vehicles, such as parking lots or traffic congestion.

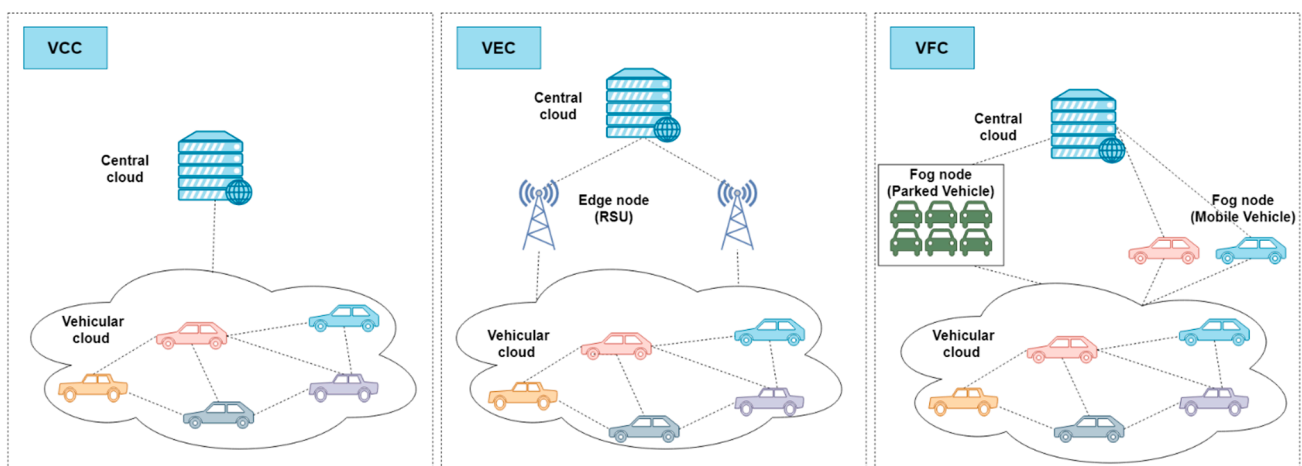


Figure 3. Structure of VCC, VEC, VFC.

2.3. Vehicular Edge Computing

Vehicular edge computing complements vehicular cloud computing. As the communication and computation needs of vehicular applications grow, VEC moves computation to the edge of the network close to the vehicle [28]. As shown in Figure 3, the edge network is the server on the RSU between the vehicle and the remote cloud server. Installing multiple servers on different RSUs can balance the load of a single server. VEC reduces the communication delay and balances the computational load compared with VCC [29].

2.4. Vehicular Fog Computing

Vehicular fog computing can be viewed as a variant of VEC. As shown in Figure 3, VFC outsources computational resources to fog nodes, edge devices in the vicinity of users, and parked/mobile vehicles. Due to the high construction cost of RSUs, VFC reduces the number of infrastructure placements by replacing them with street-parked vehicles. Thus, in a way, the biggest difference between VFC and VEC is that VEC uses RSUs as edge nodes while VFC will use vehicles as fog nodes [30]. Resource allocation is a major challenge for VFCs due to the diversity and geographic dispersion of fog nodes [31].

3. Vehicular Networks Security and Privacy Challenges

The emergence of VCC, VEC, and VFC has made vehicular networks more flexible, allowing vehicle users to fully enjoy the convenience of in-vehicle applications while traveling without worrying about latency and limited computing resources. However, dynamic vehicular networks hide several security and privacy challenges that must be addressed to fully capitalize on the benefits of vehicular networking technologies and expand their adoption.

3.1. Security Challenges

In vehicular networks, VCCs, VECs, and VFCs utilize task offloading techniques to support devices with fewer resources. Due to the limited computing resources of the vehicle itself, tasks with low latency requirements (e.g., fleet data analysis, navigation map updates) can be offloaded to cloud servers for execution. However, other tasks that require fast response time need to be offloaded to edge servers (e.g., RSUs) or other vehicles to provide more computational support to the vehicular network [32,33]. Without efficient offloading of tasks, high-latency communications will reduce the efficiency of the entire network, giving attackers more opportunity and time to threaten vehicular network cybersecurity [34]. When vehicles use V2I and V2V services to offload tasks to edge servers or other vehicles, they encounter malicious nodes [35]. These malicious nodes can perform cyber-attacks on other vehicles or vehicular networks by joining the vehicular network and uploading malicious information by masquerading as a trusted user. For example, malicious nodes can masquerade as other existing vehicles, provide false location information, fake or tamper with events occurring in the target vehicle's surroundings, and so on. It will be a challenge to recognize these cyber-attacks [13,36]. In addition to securing vehicles by detecting cyber-attacks, identifying malicious or anomalous vehicles in the vehicular network can also improve the overall security level of the network [16,37]. Detailed challenges are summarized in Table 2.

Table 2. Summary of security challenges.

Theme	Challenges
Task offloading security	High latency
	Limited computational resource
	High energy consumption
	Resistance to cyber-attack
Intrusion detection system	Cyber-attack detection performance
	Ability to detect unknown risks
	Limited system resource
Anomaly vehicle detection	Vehicle credit assessment
	Anomaly vehicle detection performance

3.2. Privacy Challenges

Privacy includes the vehicle (driver) and the location of the vehicle [38]. Only authorized users can access and control the real identity and location information of the vehicle. In vehicular networks, application software is dependent on beacon messages broadcast periodically by the vehicles [39]. These messages include the GPS coordinates, real-time speed, message timestamps, the real identity of the vehicle, and other information. By analyzing these beacon messages, sensitive data such as location information and the whereabouts of the vehicle and passengers can be obtained. In addition to this, different kinds of data can be collected by different stakeholders in the vehicular network, such as companies, government departments, other users of the vehicular network, or even malicious users [40]. These data can be misused by companies or government departments and can also be exploited by malicious users, which can lead to security risks. Thus, vehicular networks face serious privacy threats. In vehicular networks, privacy challenges are not only present in the data transmitted to each other. Artificial intelligence models are used in various protection programs for vehicular cybersecurity. However, the leakage of AI model parameters can also cause hidden dangers [41,42]. Malicious users can deduce the working principle of the model through the model parameters so that they can bypass or even spoof the AI model to make the cybersecurity protection program ineffective. How to protect model training parameters has become a new challenge in the privacy protection field. Detailed challenges are summarized in Table 3.

Table 3. Summary of privacy challenges.

Theme	Challenges
Data privacy	Data encryption
	Data authorization
	User authentication
	Data transmission
Model privacy	Model parameter encryption
	Model performance based on transformed data

4. Machine Learning in Vehicular Cloud Computing

Machine learning is a product of the intersection of computer science and statistics. Learning from experience from large amounts of data enables machine learning models to improve their algorithms automatically. In vehicular networks, the interaction between

vehicles and their environment generates a large amount of data. These data will drive machine learning algorithms to have better performance in vehicular cloud computing. As shown in Figure 4, machine learning, when applied to vehicular cloud networks, usually involves three steps, i.e., training, testing, and validation. First, the raw data are divided into two parts: training and testing. In the training phase, the machine learning algorithm generates a model based on the training data collected by vehicles or historical data. In the testing phase, the trained model is used for prediction or classification on the test dataset. Finally, in the validation phase, the performance of the model is evaluated, and the model is optimized by updating the data or adding more features. Once the model is trained, the vehicle can use the model to accomplish specific tasks. Existing machine learning can be categorized in terms of types: supervised learning, unsupervised learning, and reinforcement learning [43]. In terms of learning strategies, they can be categorized as centralized learning, federated learning, and transfer learning.

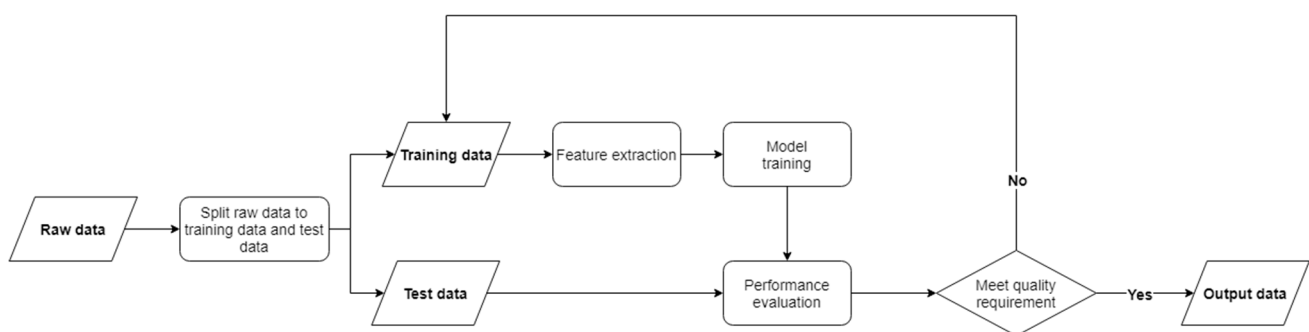


Figure 4. ML training progress.

4.1. The Use of Various Types of Machine Learning in Vehicular Cloud Computing

4.1.1. Supervised Learning

A key feature of supervised learning is that the dataset on which the algorithm is trained must contain the correct labels or results [44]. Therefore, in vehicular cloud computing, after the data have been collected, it needs to be labeled before training or using historical data. When training the model, the real results of the training dataset are fed in and compared with the model's predictions; thus, supervised algorithms continuously learn and improve the model, ultimately making the model's predictions as accurate as desired. Supervised learning is generally divided into two categories, classification algorithms and regression algorithms. Machine learning applied to the security of vehicular cloud networks mainly uses classification algorithms. The common supervised algorithms include Bayesian networks (BNs), logistic regression (LR), decision trees (DTs), random forests (RFs), support vector machines (SVMs), neural networks, and so on [45,46].

4.1.2. Unsupervised Learning

The biggest difference between unsupervised learning and supervised learning is that the training dataset is not labeled in advance. Thus, unsupervised learning is well suited for recognizing unknown categories or anomaly detection in vehicular cloud computing. By feeding the features of the training objects into the unsupervised learning algorithm, the model can infer some intrinsic connections of the data. Unsupervised learning algorithms can be divided into six main categories: hierarchical learning, data clustering, latent variable models, dimensionality reduction, and anomaly detection [47]. Common unsupervised learning algorithms include K-means, restricted Boltzmann machine, auto-encoder, and GAN [48]. In addition, RNNs belonging to neural networks are also widely used in unsupervised learning [49]. Thus, it can be noticed that the boundaries of supervised and unsupervised learning are gradually intermingling as the technology is updated.

4.1.3. Reinforcement Learning

Unlike supervised and unsupervised learning, the nature of reinforcement learning is to learn by interacting with the environment. This is ideal for offloading tasks in vehicular cloud computing and searching for optimal strategies in changing environments. The agent controlled by the reinforcement learning algorithm observes the state, which is sufficient statistical data about the environment. Based on these data, the agent can infer the best action for the moment. The agent will optimize the agent's behavioral pattern based on the rewards it will receive after performing each action, thus deciding the best order of actions to maximize the expected reward from the environment. Thus, the agent needs to update the algorithm by generating more information with the environment through repeated experiments. This learning paradigm of repeated experimentation is derived from behaviorist psychology and is one of the main foundations of reinforcement learning [50]. The process of transferring states and actions is constructed through Markov Decision Processes (MDP), which enable mathematically analyzing the interactions between the agent and the environment. Common algorithms include Q-learning, Monte Carlo (MC) control methods, Q-network (DQN), trust region policy optimization (TRPO), and asynchronous advantage actor-critic (A3C) [51,52].

4.2. Machine Learning Training Strategy in Vehicular Cloud Computing Environment

4.2.1. Centralized Training

Centralized training strategy refers to uploading data to a central server to train machine learning models using a centralized approach [53]. As shown in Figure 5, each node in the vehicular cloud acquires raw data from the environment, performs some simple initial preprocessing on it, and then transmits the training data to the central cloud. The central cloud performs the corresponding computational tasks using centralized machine learning models. The centralized training strategy has the advantages of simplicity and economy. There is no need to add additional equipment to the vehicular cloud computing environment. Individual nodes only require lower power and performance compared with the central cloud. However, this training strategy imposes a huge transmission burden on the vehicular cloud network. Meanwhile, the centralized cloud requires powerful computing power and data storage space. Moreover, centralized data storage in the cloud poses privacy risks [54].

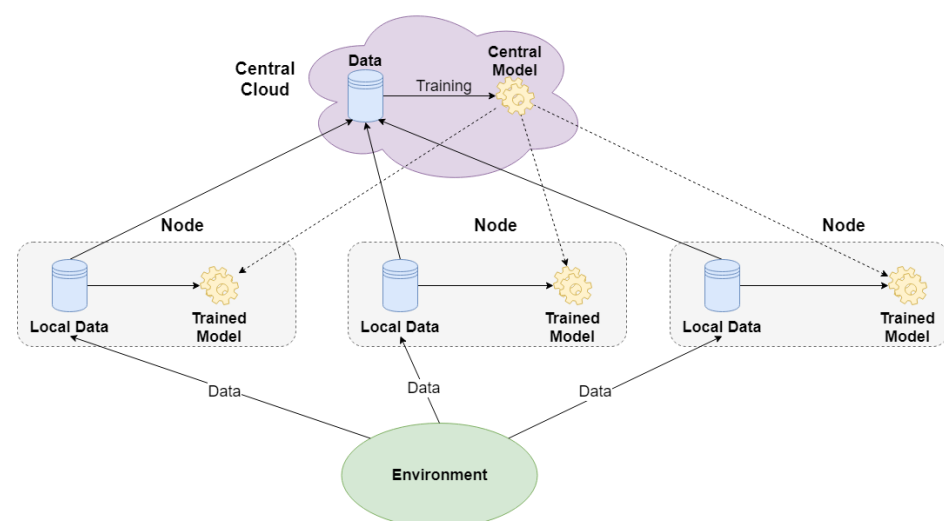


Figure 5. Centralized training structure.

4.2.2. Federated Learning

Distributed machine learning utilizes multiple processing nodes to overcome the limitations of centralized machine learning as compared with centralized training strategies [55,56]. Federated learning belongs to the distributed training approach, which allows collaboration between different nodes to learn machine learning models. This training strategy is well suited for vehicular cloud computing structures. As shown in Figure 6, the central cloud sends the machine learning model to all the nodes, and then the local data collected by the nodes are fed into the model for training and updating the parameters and weights of the local model. Afterwards, the parameters and weights of the model are uploaded to the central cloud, fed into the global model for improvement, and again the upgraded model is sent back to the nodes for further iteration. This process reduces the communication burden on the vehicular cloud network and eliminates the need for extensive data transfer. At the same time, all the local data are stored in the local nodes, reducing the risk of data privacy leakage [57].

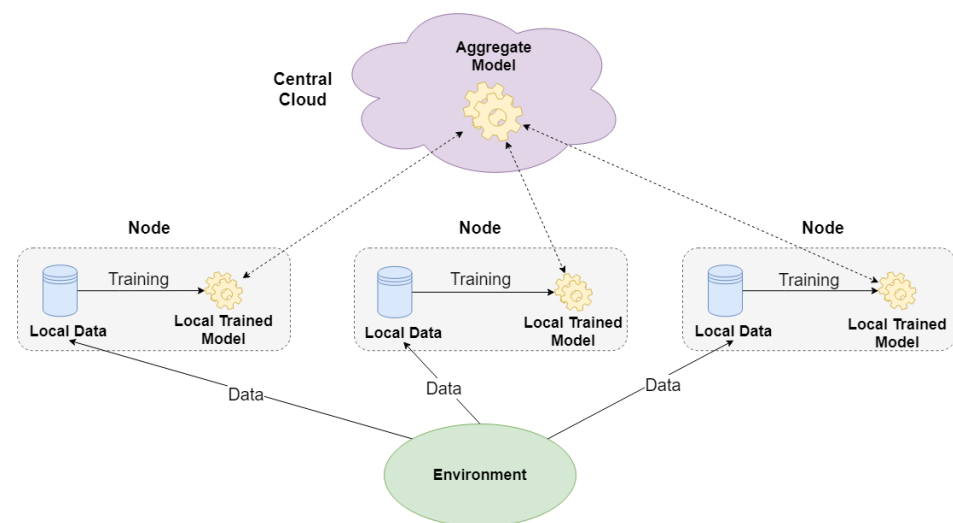


Figure 6. Federated training structure.

4.2.3. Transfer Learning

The transfer learning strategy is to transfer knowledge from similar domain tasks to the target task to speed up model training and performance [58]. Vehicular cloud computing requires a large amount of training data to build the model, but the processing of the data and the initial training process will consume a lot of resources. Therefore, inputting trained model parameters from similar domains into the vehicular cloud and fine-tuning them according to the input data will greatly improve the efficiency of model training. Transfer learning can be divided into two categories: homogeneous transfer learning and heterogeneous transfer learning [58,59]. Homogeneous transfer learning applies when the domains have the same feature space and adapts to the domain by correcting sample selection bias or covariate bias. Heterogeneous transfer learning is the process of transferring knowledge when the domains have different feature spaces. Unlike centralized and federated learning, which have clear boundaries, transfer learning strategies can be combined with other learning strategies such as federated transfer learning strategies [60].

5. Methodology

Semi-systematic evaluation was used in this study. This method is applicable to cross-disciplinary research topics, which are often not amenable to full systematic evaluation.

The literature for the semi-systematic evaluation consisted mainly of research articles that provided a clear and critical description of the existing knowledge on the topic using a combination of quantitative and qualitative methods [61]. The literature review process consists of three steps: planning, conducting, and reporting the review [62]. Translated into the research process of this paper, the first step is to formulate the research question, the second step is to determine the scope of the literature search, the third step is to screen the literature that meets the criteria, and finally, to analyze and evaluate the selected literature. The research question has been stated in the introduction section, and the literature search and screening will be described next.

5.1. Search Scope

In this paper, the Web of Science and Scopus databases were selected for literature search. The search terms based on the research questions then included keywords in the four areas of vehicular networks, cybersecurity, computing paradigms, and machine learning. Based on the previous literature review [16,29,63–65], the following search terms were selected to search in the two databases in the topic of literature, and a total of 575 papers were included in the initial literature base for further screening.

Search term: (connected AND vehicles) OR (vehicular AND networks) OR (internet AND vehicles) OR VANETs OR CAV) AND (cybersecurity OR security) AND ("Edge Computing" OR "Fog Computing" OR "Cloud Computing") AND ("Machine learning" OR "Deep learning" OR "Artificial intelligence").

5.2. Inclusion and Exclusion Criteria

The development of precise inclusion and exclusion criteria allowed for the selection of appropriate literature for review. The search for this paper was conducted up to June 2024. Also, only peer-reviewed academic journal papers and conference papers were included in the search process. Literature needs to be written in English and have full-text permission. The research must include the application of machine learning in vehicular network cybersecurity and privacy. Gray literature, such as book chapters, theses, etc., is not included, and review literature is also excluded. The specific search process is shown in Figure 7, Based on these criteria, after screening by type, duplication, title, abstract, and full text, we finally selected 85 literatures for analysis and review.

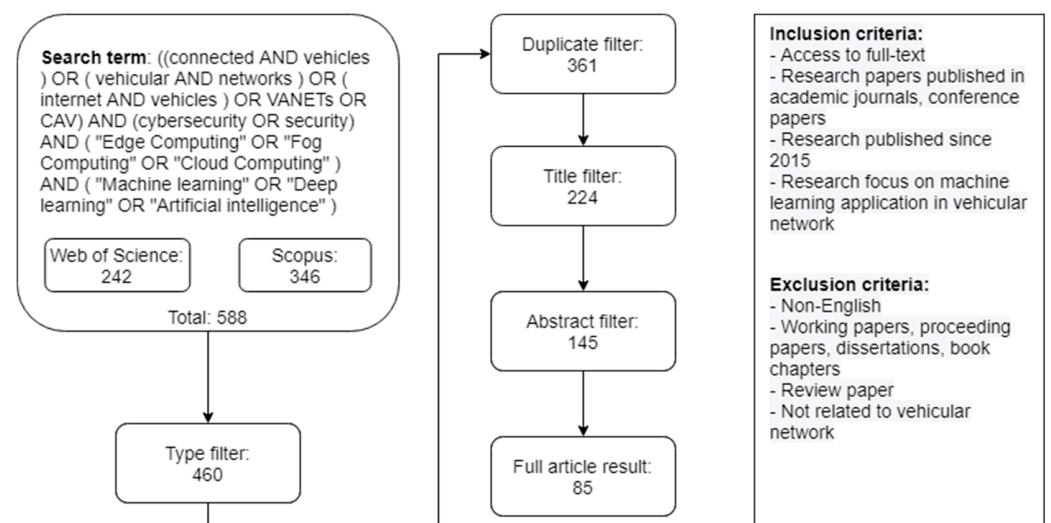


Figure 7. Semi-systematic literature review selection process.

6. Machine Learning Applications in Security and Privacy Challenges for Vehicular Cloud Computing

6.1. Machine Learning Application Summary

Out of the semi-systematic review, 85 relevant papers were selected after a comprehensive review. Figure 8 shows the publication trend of the literature and the distribution of the training strategies involved. From this figure, we can find that the literature on the topic of cybersecurity and privacy in vehicular networks has been increasing year by year, and the publication volume in 2024 is twice that of 2023. This indicates that the concern for security and privacy in vehicular networks continues to rise. There is also a trend in the distribution of machine learning training strategies, with the number of publications using federated learning trending upwards from 2021, and the proportion of centralized learning declining over time. Transfer learning is currently seen only once in 2023.

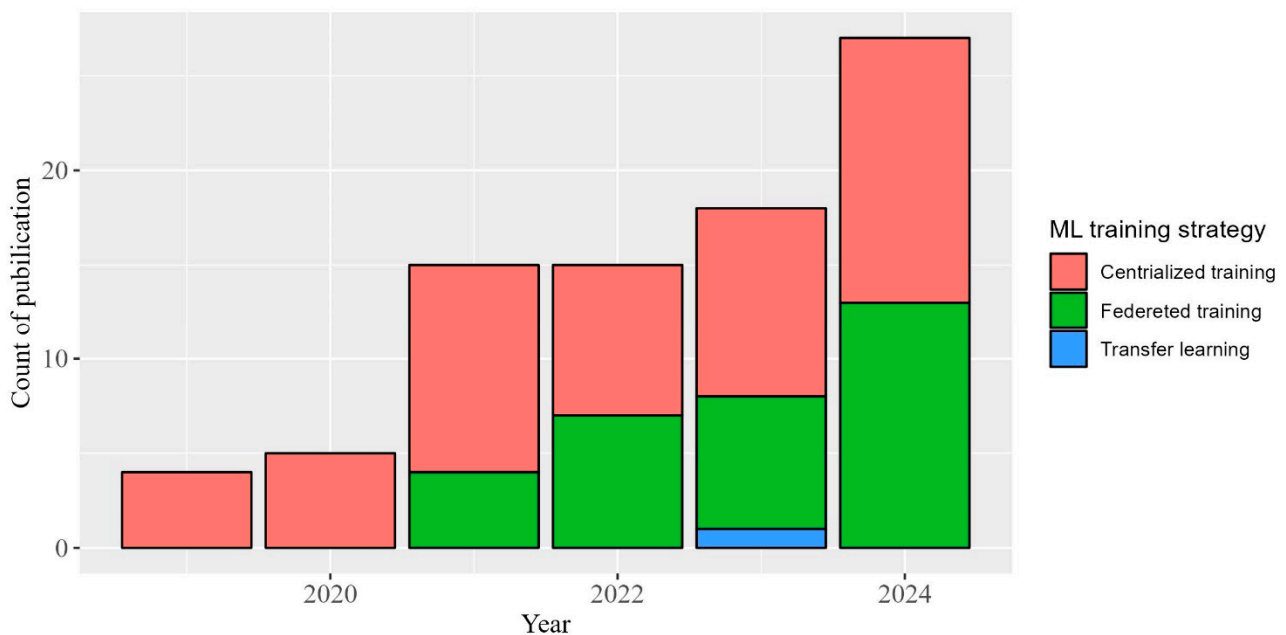


Figure 8. Publication and ML training strategy trend.

From the literature, four themes can be summarized for the application of machine learning in vehicular networks, which are intrusion detection systems, anomaly vehicle detection, task offloading security and privacy, and privacy protection. They correspond to Theme A, Theme B, Theme C, and Theme D in Figure 9. An alluvial diagram is used to show the relationship between machine learning algorithms and research themes. The different colors represent the machine learning categories, and the grey areas in the figure represent the existence of two or more machine learning categories. The first column shows the machine learning algorithms that appear in the literature; the machine learning algorithms that were used as benchmarks were not counted. If there is a variant, it is counted into its base algorithm; e.g., two-layer Q-learning is counted as Q-learning, and asynchronous advantage actor-critic (A3C) is counted as actor-critic (AC). It can be seen that AC and Q-learning are reinforcement learning algorithms; auto-encoders, generative adversarial networks (GANs), and particle swarm optimization (PSO) are unsupervised learning; and decision trees (DTs), k-nearest neighbors (KNNs), random forests (RFs), support vector machines (SVMs), and extreme gradient boosting (XGB) are supervised learning algorithms. Convolutional neural networks (CNNs), gated recurrent units (GRUs), long short-term memory (LSTM), and recurrent neural networks (RNNs) have the potential to be supervised or unsupervised learning depending on the input and output. The preferred

machine learning algorithms for different research topics are also different; intrusion detection systems and anomaly vehicle detection mostly use supervised and unsupervised learning. On the contrary, for task offloading security and privacy, only reinforcement learning is used. Because of the wide range of privacy protection research, all three types of machine learning algorithms are covered. The reasons for this will be explained in the following sections.

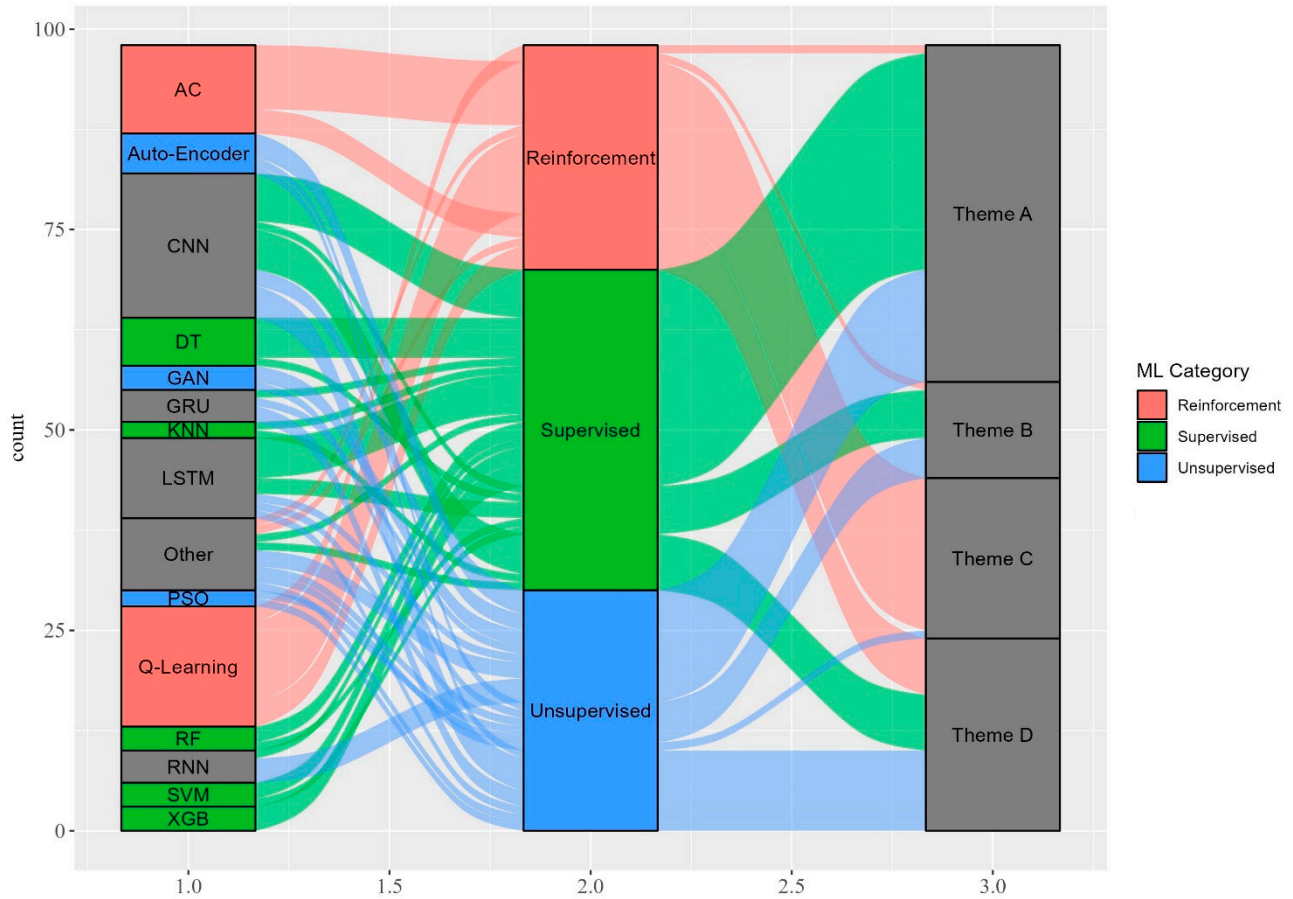


Figure 9. Relationship between ML method and research theme.

6.2. Intrusion Detection System (IDS) for Vehicular Cloud Computing

Due to the existence of numerous connectivity interfaces between vehicular networks and external networks, it increases the ways for malicious attackers to intrude. Intrusion detection systems (IDSs) are low-cost and easy to deploy and can effectively defend against attacks implemented on vehicular networks. IDSs can be categorized into two categories based on the detection strategy: signature-based detection and anomaly-based detection [66–68]. Signature-based IDSs are weak in detecting novel attacks as they require updating the database of known attacks. Anomaly-based detection is highly adaptable and can find attacks not recorded in the database; thus, it has become a popular research direction and is also more suitable for machine learning applications [68]. A total of 30% of the selected literature pertains to the application of machine learning in intrusion detection techniques, which reflects the fact that machine learning has been widely used to identify various kinds of intrusions into vehicular cloud networks. An IDS essentially classifies and identifies categories of cyber-attacks, and hence is well suited for the application of learning. An IDS mainly uses supervised and unsupervised learning to train machine learning models, with the majority of the literature (69%) employing supervised learning algorithms. There is only one case of reinforcement learning use, as IDS decisions

do not affect the state of the environment. The algorithms that appear most frequently in this literature are CNN and LSTM. Most of the literature uses four performance metrics to measure the model: accuracy rate, precision, recall, and F1-score. Accuracy rate indicates the proportion of correct predictions made in the entire dataset; precision indicates the proportion of true positive predictions out of all positive predictions; recall denotes the proportion of true positive predictions among actual positive instances; and F1-score is a metric that balances precision and recall. All metrics are closer to 1, indicating better model performance. For an IDS with a low accuracy rate, it may not be able to detect all attacks, thus making the system vulnerable to attacks. On the contrary, if the IDS has low precision, it may generate costly false alarms. In this paper, we have collected the detection results of the models that have appeared in the selected literature, including the benchmark model, to compare the performance of IDS machine learning algorithms. The performance of the different machine learning models is illustrated in Figure 10. The accuracy rate was chosen as a comparison metric because it is more intuitive and appears most frequently in the literature. Although the literature uses different datasets and includes different types of attacks, the results in the figure can describe the overall performance of the models as a reference for model selection. Most of the machine learning models have an accuracy rate higher than 95%, with PSO, CNNs, and CNN-LSTMs having an accuracy rate of 99%, which is in line with our previous observation that most of the studies will use CNNs and LSTMs as the base model for development. Naive Bayes (NB), auto-encoders (AEs), GANs, and simple RNNs are less accurate compared with other algorithms.

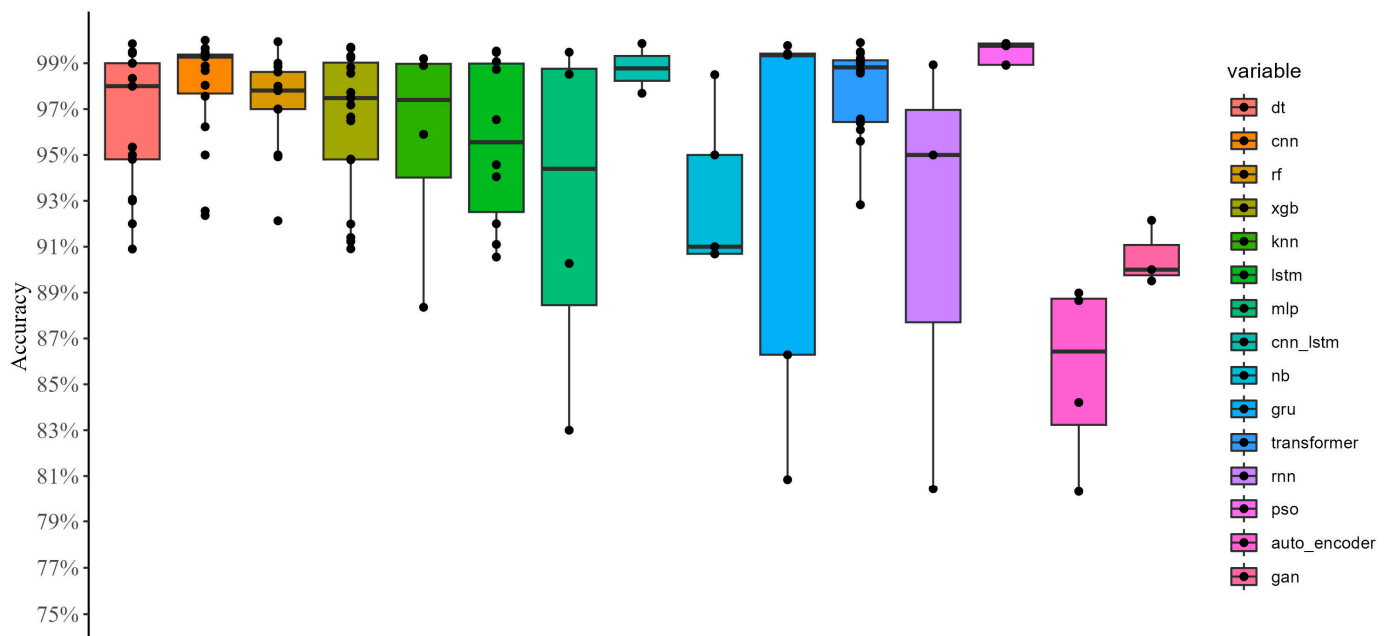


Figure 10. Comparison of ML accuracy performance.

In addition, 64% of the literature uses a centralized learning strategy, and 32% uses a federated learning strategy. Some of the literature also compares the performance of algorithms under different learning strategies [69–72]. As shown in Figure 11, we can find that the accuracies of federated learning and centralized learning are basically close in most cases. Although decentralized training reduces the detection rate of most models [69], the adoption of federated learning in vehicular cloud networks can provide data privacy protection, as well as improve the efficiency of the training process and reduce the latency associated with data transmission [73]. It was also found that in vehicular edge networks, the higher the number of edge vehicles involved, the better the federated learning [69,74].

There is also a literature that employs a transfer learning strategy [75] to test eight pre-trained models trained on large-scale datasets with an F1-score of 99.47%.

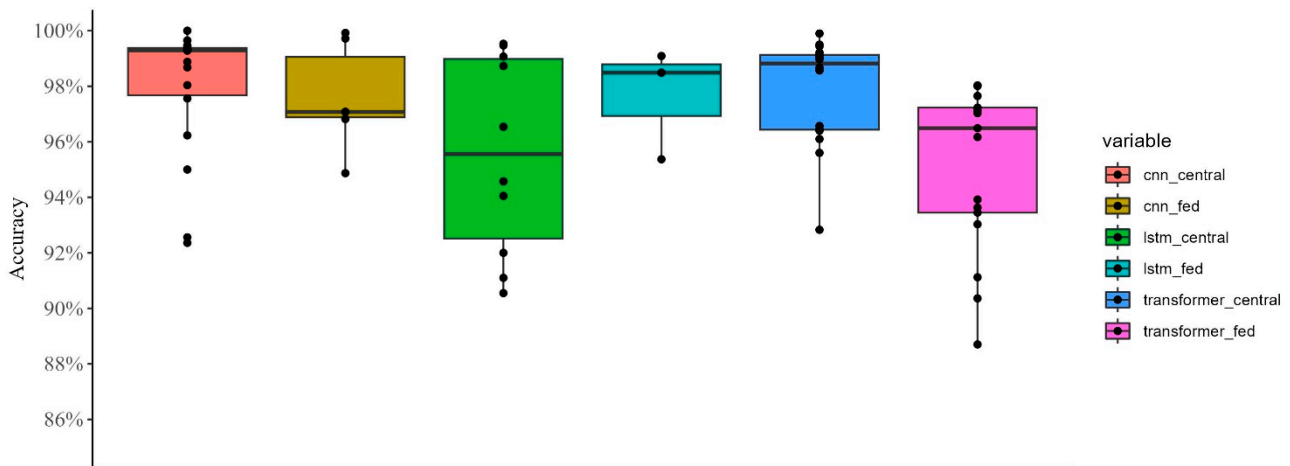


Figure 11. Comparison of ML strategy accuracy performance.

The training datasets used in these literatures focus on ToN-IoT, CICIDS-2017, UNSW-NB15, NSL-KDD, and Car-Hacking. ToN-IoT is a comprehensive dataset that integrates multiple data sources, including network traffic, IoT device telemetry, and system logs, making it suitable for cross-domain attack detection research [76]. The CICIDS-2017 dataset, developed by the Canadian Institute for Cybersecurity (CIC), captures modern network traffic with realistic normal and malicious activities. NSL-KDD, an improved version of the KDD Cup 1999 dataset, is widely utilized for network intrusion detection tasks. UNSW-NB15, developed by the University of New South Wales, addresses the limitations of older datasets such as NSL-KDD. The Car-Hacking dataset focuses on evaluating the security of in-vehicle communication systems, particularly the Controller Area Network (CAN) bus. While these datasets are widely used in cybersecurity and intrusion detection research, only the Car-Hacking dataset specifically targets vehicular networks. Most existing datasets (e.g., CICIDS-2017, UNSW-NB15, NSL-KDD) primarily focus on traditional networks and fail to capture the unique characteristics of vehicular networks. For example, specialized communication protocols in automotive networks, such as the CAN bus, and specific attack patterns, including replay and spoofing attacks, are absent in these datasets. Additionally, some datasets, such as NSL-KDD, are outdated, with data characteristics and attack methods that no longer align with modern network environments, making them not suitable for addressing the security requirements of real-world scenarios. Consequently, there is a critical need for more dedicated and realistic datasets in the field of automotive network security to effectively evaluate IDS. Furthermore, Sousa et al. [77] state that the higher the diversity of the training data, the better the model's ability to generalize on the test set. Multiple datasets are significantly better than using a single dataset for training. Kumar et al. [72] tested that transforming the dataset does not affect the model accuracy, which allows the model to perform unsupervised learning on the transformed data to improve the applicability of the model while providing privacy protection of the training data. More detailed information is shown in Table 4.

Table 4. Summary of characteristics of ML applications in IDS.

Sources	Computing Paradigms	ML Training Strategy	ML Method	Blockchain Enabled	Performance Metric	Database	Accuracy Rate
[78]	VCC	Centralized training	DT	No	Accuracy rate; detection rate; false positive rate; false negative rate; service retrieval delay	NSL-KDD	99.43%
[74]	VEC	Federated training	CNN	Yes	Accuracy rate; time cost; precision rate; recall rate	KDDCup99	95.00%
[79]	VEC	Centralized training	RF	No	Accuracy rate; precision; recall; F1-score; false negative rate	CICIDS-2017	99.94%
[80]	VFC	Centralized training	CNN	No	Accuracy rate; precision; recall; F1-score	VeReMi Extension	99.65%
[81]	VFC	Centralized training	Neuro-fuzzy algorithm (FNN)	Yes	Accuracy rate; precision; recall; F1-score	NS-3	91.50%
[82]	VCC	Federated training	ConvLSTM	No	Accuracy rate; precision; recall; F1-score	CAN messages	94.58%
[83]	VEC	Centralized training	SAE-ABIGRU	Yes	Accuracy rate; precision; recall; F1-score; false alarm rate	ToN-IoT CICIDS2017	99.09% 98.49%
[71]	VEC	Federated training	Transformer	Yes	Accuracy rate; F1-score	ToN-IoT Car-Hacking	94.85% 97.82%
[84]	VCC	Centralized training	A-RNN	Yes	Accuracy rate; Precision; detection rate; F1-score; false alarm rate	ToN-IoT CICIDS-2017	99.77% 99.35%
[85]	VEC	Centralized training	GAN	No	Accuracy rate; network latency	Independent	90.00%
[86]	VCC	Centralized training	LSTM	No	Accuracy rate; precision; recall; F1-score	NSL-KDD UNSW-NB15	99.47% 78.88%
[77]	VCC	Centralized training	DT	No	Accuracy rate; precision; recall; F1-score	NS-3	97.00%
[87]	VFC	Centralized training	CAaDet	No	precision; recall; F1-score	NSL-KDD	Not available
[72]	VCC	Centralized training	ABiLSTM	Yes	Accuracy rate; Precision; detection rate; F1-score; false alarm rate	ToN-IoT CICIDS-2017	98.97% 98.80%
[73]	VEC	Federated training	Extra Trees Classification	Yes	Accuracy rate; precision; recall; F1-score; time to train; time to predict; total time	UNSW-NB15	93.07%
[75]	VCC	Transfer learning	CNN	No	Accuracy rate; precision; recall; F1-score	AV-CPS	99.47%

Table 4. Cont.

Sources	Computing Paradigms	ML Training Strategy	ML Method	Blockchain Enabled	Performance Metric	Database	Accuracy Rate
[88]	VEC	Centralized training	CNN	No	Accuracy rate; precision; recall; F1-score	Car-Hacking	100.00%
[89]	VFC	Centralized training	CNN-LSTM	No	Accuracy rate; precision; recall	CICIDS-2017	99.86%
[90]	VEC	Centralized training	BiGAN	No	Accuracy rate; precision; recall; F1-score	NSL-KDD	92.15%
[70]	VEC	Federated training	PCC-CNN	No	Accuracy rate; loss; time	NSL-KDD Car-Hacking	97.08% 99.92%
[91]	VCC	Centralized training	XGBoost multi-classification	No	Accuracy rate; precision; recall; false positive rate; false negative rate	Independent	96.30%
[69]	VEC	Federated training	Feature Select Transformer	No	Accuracy rate; precision; recall; F1-score	UNSW-NB15 CICIDS2018	99.79% 97.10%
[92]	VFC	Federated training	CNN	Yes	Accuracy rate; precision; recall; F1-score	UNSW-NB15	99.00%
[93]	VCC	Centralized training	CNN	No	Accuracy rate; precision; recall; F1-score	Independent	98.88%
[94]	VEC	Centralized training	ESA-DBGRU	No	Accuracy rate; precision; recall; F1-score	Car-Hacking ToN-IoT CICIDS-2017	99.97% 99.2% 99.02%
[95]	VEC	Centralized training	CV-DRNN	No	Accuracy; specificity; positive likelihood ratio; bookmaker informedness; Fowlkes–Mallows index	CICIDS-2017 Car-Hacking KDDCup99 UNSW-NB15	Not available Not available Not available Not available
[96]	VCC	Centralized training	GA-EBT	No	Accuracy rate; precision; recall; F1-score	Car-Hacking	99.99%
[97]	VEC	Federated training	CNN	No	Accuracy	CICIDS-2017	97.07%
[98]	VEC	Centralized training	One-Class Support Vector Machine (OCSVM)	No	Accuracy rate; precision; recall; F1-score	VeReMi UNSW-NB15	98% 98%

6.3. Anomaly Vehicle Detection in Vehicular Cloud Computing

Anomaly vehicle detection is also an area where machine learning algorithms can be applied. It is very similar to the concept of Intrusion Recognition Systems, but while IDS recognizes the subject of its own vehicular state, anomaly vehicle detection is specific to the vehicles in the vehicular network. Anomaly vehicle detection can be used to enhance the overall system security of a network [99,100]. Anomaly vehicle detection is removed from the vehicular network to ensure the safety of the remaining vehicles. The dataset used to train the anomaly vehicle detection machine learning model typically includes features of the vehicle's external environment, such as timestamps, pseudo-identity of the vehicle, and X and Y coordinates of position, velocity, acceleration, and heading. A traffic simulator is required to create an operational environment simulating a real vehicular network. Anomaly vehicle detection is essentially a classification and recognition problem like IDS, and the most commonly used algorithm in the selected literature is LSTM. There is

only one case for reinforcement learning use since the decision-making for anomaly vehicle detection does not affect the state of the environment. More detailed information is shown in Table 5.

Table 5. Summary of characteristics of ML applications in anomaly vehicle detection.

Sources	Computing Paradigms	ML Training Strategy	ML Method	Strength	Weakness
[101]	VEC	Centralized training	LSTM	High efficiency in learning spatio-temporal parameters	More parameters need to be input
[102]	VCC	Centralized training	Q-Learning	High average number of true feedback; low communication costs; low computational costs	Need to add more research cases of cyber-attacks
[103]	VEC	Centralized training	PSO	High detection rate; Low classification error	Probability of misclassification needs to be improved
[99]	VEC	Federated training	Random Forest	Able to detect passive mobile attackers with high speed and accuracy	A large number of features and FL clients are required to maintain the accuracy of the model.
[99]	VFC	Centralized training	Sparse auto-encoders	High throughput; low jitter	High computation cost
[104]	VCC	Federated training	FedTimeDis LSTM	Improves the accuracy and robustness of the models, both within the same region and across different regions	Model performance needs further enhancement
[100]	VEC	Federated training	CNN-LSTM	Effective for different data distributions and under different deep learning models	Need to improve robustness and accuracy
[105]	VEC	Centralized training	Graph Neural Networks (GNN)	Comprehensive detection; scalability and resource optimization	Dependency on high-quality sensor data; challenges with real-time applications
[106]	VCC	Centralized training	GAN	Lightweight model for deployment; balanced accuracy and efficiency	Performance degradation with high pruning ratios

6.4. Task Offloading Security and Privacy

To support the operation of vehicular networks, application software requires a large amount of computational resources and generates a large amount of data. However, some application software is latency sensitive [107,108]. If the vehicle resources are limited, the tasks cannot be completed within the specified time constraints. To avoid this situation, relying on VEC or VFC, task offloading is a technique to solve the resource limitation problem. It enables resource-limited vehicles to perform their computational tasks on nearby resource-rich vehicles or edge server nodes. However, data sharing also poses security risks; task offloading involves sensitive data of vehicles, which will seriously threaten cybersecurity and privacy if there are malicious nodes in the roadside servers or collaborating vehicles [109,110]. Machine learning algorithms are effective in assisting vehicles with safe, reliable task offloading. Most studies transform the task offloading process into a Markov chain and then optimize it using machine learning [109,111]. It has also been pointed out that VCC is a multi-agent environment, so it is more appropriate to introduce Markov games [112]. Therefore, most of the literature (95%) uses reinforcement learning algorithms to address security challenges in task offloading. Two of the most common reinforcement learning algorithms are Q-learning and AC. Improved algorithms based on these two algorithms have also emerged. Zhang et al. [113] found that the AC algorithm is prone to suboptimal solutions, and the entropy introduced by soft actor-critic (SAC) encourages the algorithm to explore better results. The emergence of double-layer deep Q-learning can efficiently balance the different objectives and perform complex trade-off analysis, which can better optimize the overall performance of the algorithm compared with Q-learning [34,114].

The most direct application of machine learning in task offloading security is to ensure the integrity of data transmission by optimizing the efficiency of task offloading, thus ensuring cybersecurity [34,115]. Incorporating PLS techniques into task offloading and then optimizing it using machine learning is also one of the common applications. VCCs are also vulnerable to eavesdropping due to the open nature of the wireless offload channel. Many works have investigated physical layer security (PLS) techniques that exploit the inherent physical characteristics of the wireless channel, thereby weakening eavesdropper reception in wireless networks. Using non-orthogonal multiple access (NOMA) in conjunction with task offloading and optimization using A3C learning algorithms can further improve the confidentiality performance and reduce the transmission delay [116,117]. Utilizing the Wyner eavesdropping coding scheme in PLS technology and optimizing it using double-layer deep Q-learning is also a strategy [110,118]. The third type of application is the use of blockchain technology to solve the problem of secure computational offloading in VCC. Under blockchain technology, data confidentiality, integrity, authentication, and privacy for task offloading can be achieved, but at the same time, it brings the problem of high dimensionality and time-varying features [119]. Introducing reinforcement learning algorithms can result in suboptimal blockchain task offloading decisions [113,120]. The last category of application is assisting IDS task offloading. Mourad et al. [121] proposed a VEC-enabled scheme to offload intrusion detection tasks to joint vehicular nodes in a temporary vehicular fog formed nearby and optimized using genetic algorithms to execute them collaboratively with minimal latency. More detailed information for ML applications in task offloading security and privacy is shown in Table 6.

Table 6. Summary of characteristics of ML applications in task offloading security and privacy.

Sources	Computing Paradigms	ML Training Strategy	ML Method Used	Optimization Target	Strength	Weakness	Blockchain Enabled
[115]	VEC	Centralized training	Q-Learning	Utility of system	High learning efficiency; avoid local optimum; reliable transmission	Unable to sustainably improve offloading utility; no reinforcement learning methods benchmark	No
[34]	VEC	Centralized training	DDQN	Customer cost	Fast convergence; high offloading rate; multiple sub-models	Inadequate experimental scenarios; reliability not considered	No
[121]	VFC	Centralized training	GA	Offloading survivability; computation execution time; energy consumption	Extensive experimental scenarios	Unstable vehicular fog federation formation	No
[122]	VFC	Centralized training	MAB	Average task offloading delay	Enable smart contract; good convergence performance; high robust	Insufficient experimental scenarios	Yes
[123]	VEC	Centralized training	Q-Learning	Long-term system of delays; energy consumption; flow costs	Low energy consumption; low latency	Need to design lightweight blockchain; sensitive to bandwidth allocation	Yes
[124]	VEC	Federated training	Q-Learning	Time delay; computing cost	Fast convergence; reduce system cost; low latency	Need to be tested in real road environment	No
[109]	VEC	Centralized training	AC	Task latency	Low latency; consider multi-vehicle coordination	Only suitable for vehicle to rsu	Yes

Table 6. Cont.

Sources	Computing Paradigms	ML Training Strategy	ML Method Used	Optimization Target	Strength	Weakness	Blockchain Enabled
[119]	VEC	Distributed training	Distributed Deep Q-Learning (DDQL)	Time consumption; energy consumption; pricing cost	Consider scenarios of malicious user attacks	Need to consider more general situation	Yes
[110]	VEC	Centralized training	DDQN	System processing delay	Enable pls; improved resource utilization	Insufficient benchmark; insufficient scenario	No
[125]	VEC	Centralized training	DDPG	Delay; energy consumption	Improve training speed; reduce time latency; reduce energy consumption	Low adaptability	No
[113]	VEC	Centralized training	SAC	Processing time	Avoid local optimum; low total computing time	Not suitable for large number of tasks	Yes
[117]	VEC	Centralized training	AC	Energy consumption	Enable PLS; moderate computation latency	Small resource block increases energy consumption	No
[116]	VEC	Centralized training	AC	Energy consumption	Enable PLS; moderate computation latency	Only consider a single-cell base station scenario	No
[118]	VEC	Centralized training	DDQN	System processing delay	Enable PLS; use spectrum sharing architecture; improve resource utility	Some V2V link quality is sacrificed to improve system latency performance	No
[120]	VEC	Distributed training	AC	Latency	Consider multiple calculation methods	Low task complete rate	Yes
[126]	VFC	Federated training	AC	Expected discounted future utility	Fast convergence	Low network utilization; vulnerable to gradient spoofing attacks	No
[114]	VEC	Centralized training	DDQN	Energy efficiency; data offloading ratio; block generation time; transaction validation time	Consider the dynamic and heterogeneous character of vehicular networks	Not suited to handle larger, more complex networks	Yes
[127]	VFC	Federated training	Deep Q-learning Network	Energy consumption; time consumption; survivability	Optimized resource utilization; scalability	Communication latency becomes high with a high speed	No

6.5. Privacy Protection

Machine learning has a very large number of applications for privacy protection in vehicular networks, focusing on two main areas: sensitive data classification and model encryption. Sensitive data classification is a classification and identification problem. Vehicles need to continuously collect data from the surrounding environment through sensors while traveling. At this time, it is necessary to distinguish which are sensitive data and which are non-sensitive data. Kaci and Rachedi [128] used a machine learning classifier, k-Nearest Neighbors (k-NNs), to classify data based on its confidentiality so that data classified as sensitive are protected and unnecessary processing of non-sensitive data is reduced. Machine learning models are also required to further classify the data when it is encrypted so that the data are given new features but without compromising privacy. Lidkea et al. [129] used a CNN framework to perform classification by partially decrypting encrypted images so that sensitive private information carried by the classified data are not exposed.

Not only is the data collected by cars a privacy risk, but if the parameters and data used to train the model are in the hands of a malicious user, the user's information could be accessed through reverse engineering [130]. Federated learning is a very effective method for data privacy protection, which enables user training data to be kept locally and only model parameters to be uploaded. Compared with centralized learning, federated learning has less communication time [131]. However, traditional federated learning with server-side weighted averaging based on the number of samples is difficult to overcome the variance due to vehicle heterogeneity, which leads to an increase in communication costs and a decrease in model accuracy. To further ensure reliability and trust, blockchain can be combined with machine learning [132–134]. By converting machine learning data to blockchain before transmission, we can increase the throughput of the system and also prevent data leakage during transmission. Since block generation is very resource intensive, it will consume a lot of computational power in the vehicular network, and the allocation of computational resources needs to be optimized by machine learning. Chen et al. [135] goes a step further by simultaneously applying machine learning, blockchain, and full homomorphic encryption (FHE) techniques to VEC to propose a decentralized privacy protection deep learning (DPDL) model. It first performs full homomorphic encryption on the data and then inputs it into the model training and then communicates the data via blockchain, thus effectively protecting data privacy protection and trustworthiness. In addition to using fully homomorphic encrypted data, including local differential privacy (LDP) in the data ensures that malicious users are unable to derive valid information from compromised data [130,136–138]. More detailed information on the characteristics of ML applications in privacy protection is shown in Table 7.

Table 7. Summary of characteristics of ML applications in privacy protection.

Sources	Computing Paradigms	ML Method	Application	Strength	Weakness	Blockchain Enabled
[133]	VEC	DDPG	Design blockchain content caching scheme	High permanence and security	Communication distance and block size affect utility	Yes
[128]	VCC	KNN	Selective encryption and adaptive security	High efficiency of the encryption process; low computational resources	The accuracy of the model needs to be improved	No
[129]	VCC	CNN	Classify encrypted images	Less training data; low computation time	The accuracy of the model needs to be improved	No
[133]	VEC	DDPG	Design blockchain content caching scheme	High permanence and security	Communication distance and block size affect utility	Yes
[139]	VEC	PPO-A3C	Resource optimization for blockchain	Improve blockchain throughput and resource efficiency; against multiple types of attacks	Higher demand for computing resources	Yes
[136]	VEC	CNN	Improve model privacy	High resilience to adversarial attacks	Not consider computational complexity and delays	Yes
[134]	VEC	CNN	Improve model privacy	High scalability; high robust; resistant to malicious attacks	Network communication needs to be further enhanced; faster filtering of malicious upload models is needed	Yes

Table 7. Cont.

Sources	Computing Paradigms	ML Method	Application	Strength	Weakness	Blockchain Enabled
[135]	VEC	Q-Learning	Improve model privacy	Low channel loss; high block mining rate; high edge latency; High FL-learning rate	Need to further improve algorithm performance and communication efficiency	Yes
[132]	VEC	CNN	Improve model privacy	Combining federated learning with LDP to enhance model privacy and accuracy	Need to enhance effectiveness, multifunctionality and adaptability	No
[137]	VFC	GRU	Improve model privacy	Combining federated learning with LDP to enhance model privacy and accuracy; considered simulation scenarios for cyber attacks	The computational and communication costs of the model need to be further increased	Yes
[141]	VEC	CNN	Improve model privacy	Encrypts data using multi-key homomorphic encryption (MKHE) and optimizes computational and communication costs	Enhancements are needed for inference in ICVs through zero-knowledge proofs; encrypted data increases the program runtime.	No
[142]	VEC	DQN-BPO	Blockchain parameter optimization	Balancing transaction throughput and energy consumption	Need to improve model robustness and introduce a reputation system to prevent potential attacks	Yes
[143]	VEC	ANN	Improve model privacy	High training accuracy; low communication burden; high computing performance	Need to balance training performance with training time	Yes
[144]	VCC	QPSO	Blockchain parameter optimization	Low average access delay; low backhaul load	Vehicle movement will impact on data acquisition efficiency	Yes
[145]	VEC	Double-dueling DQN	Improve model privacy	Reliable service delivery; low energy consumption	High latency; security needs to be enhanced	Yes
[146]	VEC	CNN	Capturing RFF Features	Fast convergence; high recognition accuracy; smaller training samples required	Huge computational resources and stable communication are needed	No
[147]	VEC	DNN	Improve model privacy	Decentralized framework; efficient communication; security against attacks	Scalability challenges; limited real-world testing	No
[148]	VEC	AD-GRU	Improve model privacy	Resilience to attacks; improved scalability	High initial costs; computational complexity	Yes
[138]	VCC	GAN-LSTM	Improve model privacy	Improved model convergence; personalized privacy	Loss of fine-grained data; potential overhead in privacy budget allocation	No
[149]	VEC	VED-PPFE	Improve model privacy	Effective against MI attacks; good privacy-preserving ability	Dependency on stable infrastructure; slight utility degradation	No

7. Challenges and Future Scope

Although advances in machine learning have enhanced the security of vehicular networks. However, it still faces multiple challenges based on the new network computing paradigm. The relationships among challenges, solutions, and future scope are shown in Figure 12. Emerging technology may also offer innovative solutions to cybersecurity and privacy issues in vehicular networks.

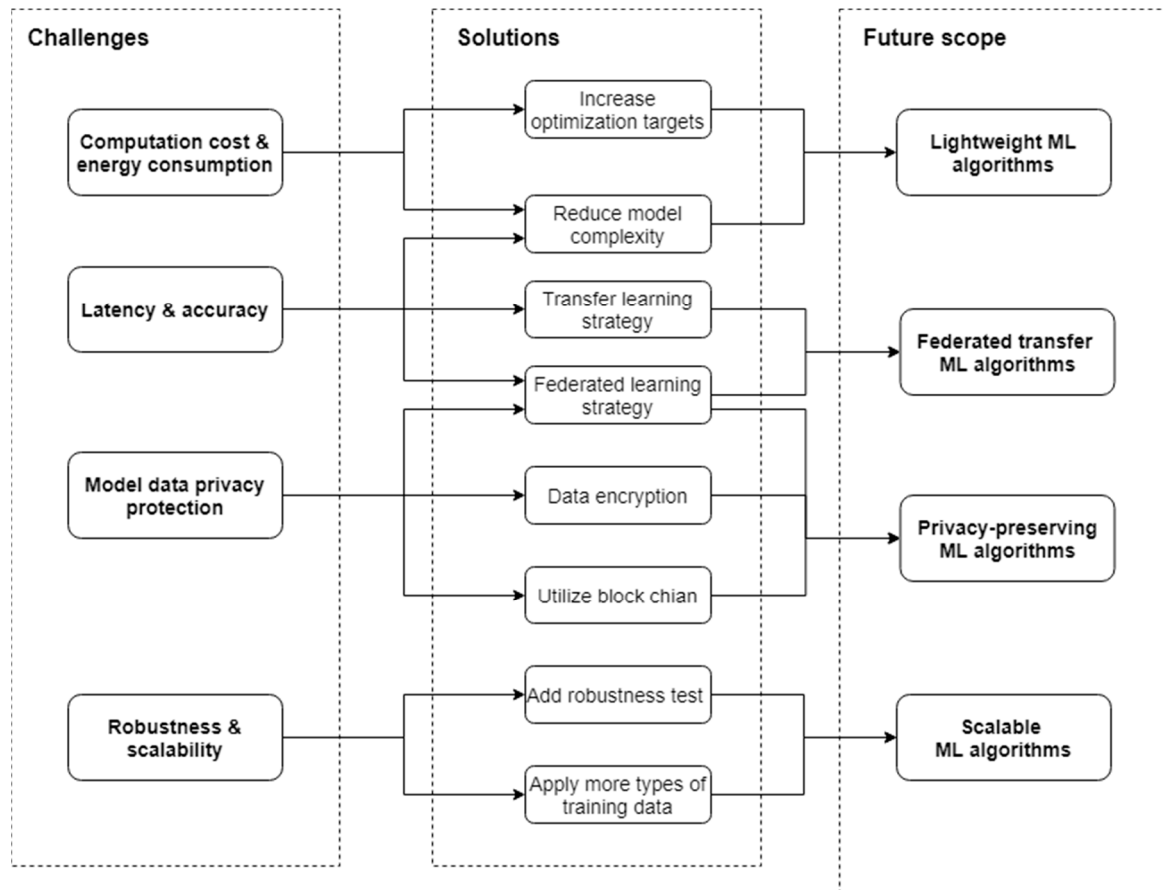


Figure 12. Challenges, solutions, and future scope.

7.1. Computation Cost and Energy Consumption

Vehicle systems have limited computing power, storage space, and energy supply. And machine learning schemes need to repeatedly compute a large amount of data, so the computational cost and energy consumption need to be paid attention to when designing machine learning schemes. In the themes of task offloading security and privacy and privacy protection, most of the literature considers the optimization of communication cost, energy consumption, and other indexes when adopting machine learning schemes, instead of pursuing the performance of model accuracy. However, in the themes of intrusion detection systems and anomaly vehicle detection, only a portion of the literature considers these metrics. Therefore, lightweight machine learning solutions are an important area for further research.

By applying feature selection techniques tailored to vehicular network data, the most relevant features can be identified to reduce the dimensionality of input data while maintaining model accuracy [150]. Compressing input data before processing can further decrease energy consumption during transmission and storage [151]. According to the unique characteristics of vehicular networks, model frameworks can be optimized, and distributed multi-agent algorithms can be developed to improve model efficiency [12]. Dur-

ing the training and deployment of machine learning algorithms, energy-aware objective functions can minimize power usage. Additionally, optimizing resource distribution across the network can balance energy and computation costs by offloading locally processed tasks to central servers or edge nodes during periods of low network traffic or when more energy-efficient resources are available [34]. These advancements effectively reduce the computational cost and energy consumption of the model, promoting more sustainable and efficient vehicular network operations.

7.2. Latency and Accuracy

The balance between latency and accuracy is also an unavoidable challenge. Although high-accuracy machine learning schemes can protect the security and privacy protection of vehicular networks more effectively, the communication latency brought about makes some latency-sensitive applications unable to run. Therefore, the use of federated learning or other distributed learning can effectively reduce the latency of vehicular networks. However, many studies have pointed out that the performance of federated learning is slightly inferior to centralized learning under the same conditions. In addition, the latency problem can also be addressed in transfer learning. By migrating models trained locally at the edge between nodes, more knowledge is gained, and less data need to be migrated. And federated learning and transfer learning can be combined with each other, and future research on federated transfer learning can be expanded. When training models, Latency-Aware Neural Architecture Search (LA-NAS) can be utilized to add both latency and accuracy into the objective function. LA-NAS is a neural architecture search (NAS) method that optimizes latency and performance simultaneously. Specifically designed for deploying efficient deep learning models in resource-constrained environments, it achieves an optimal balance between latency and accuracy. For machine learning, hierarchical models can be designed to allocate workloads according to task requirements. Lightweight models are well-suited for real-time decision-making, while more complex models can be reserved for batch processing or offline analysis [152]. A collection of models with varying complexity can also be employed, dynamically selecting the appropriate model based on latency constraints [153]. Similarly, real-time adaptive models can dynamically adjust their complexity in response to current network conditions, achieving comparable results. Adjusting model complexity based on task complexity can further optimize performance, ensuring efficient resource utilization and improved adaptability.

7.3. Model Data Privacy Protection

When designing machine learning solutions, it is essential to protect training data privacy. Techniques such as data encryption and local differential privacy can effectively mitigate privacy risks. Homomorphic encryption enables computations to be performed on encrypted data, preserving data privacy throughout the cloud processing cycle. Differential privacy enhances individual privacy by adding statistical noise to data before sharing or processing, effectively concealing sensitive information while maintaining the utility of traffic analysis, such as preventing the identification of personal driving patterns. However, training models on transformed data can impact model accuracy, highlighting a research direction: improving model learning capabilities on encrypted data. To ensure the confidentiality of training model parameters, blockchain technology can be used to prevent data theft during transmission. Blockchain offers an anonymous and traceable data-sharing mechanism, ensuring that only authorized entities can access vehicle data. Additionally, self-sovereign identity frameworks can protect the identities of vehicles and drivers. Nevertheless, blockchain implementation requires substantial computational resources, making

the optimization of resource allocation across the vehicular network a critical challenge for future research.

7.4. Robustness and Scalability

Maintaining the robustness and scalability of machine learning models is also an important challenge in vehicular cloud computing. Training machine learning algorithms with accuracy as the only metric can result in overfitting the data. This makes the model sensitive to data noise and abnormalities. As a result, the model may perform poorly on new data and have reduced scalability. Vehicular cloud networks receive data collected from different sources, such as various sensors, vehicles, and infrastructures. The structure and quality of these data will be different and thus require good robustness of the model. Overfitting can be avoided by increasing the variety of experimental datasets and performing robustness tests on the model. Future research can focus on the study and application of transfer models. Also enhancing the scalability of the model is a necessary research direction. Decomposing machine learning functionalities into modular components that can be independently scaled and updated would facilitate better combinations across functionalities. Additionally, the open sharing of models could promote collaboration within the research community and enable cross-validation of experimental results. Currently, most studies rely on general network datasets rather than specialized datasets for vehicle networks. Future research should use real vehicle data and investigate systems employing advanced communication protocols beyond CAN, such as Ethernet and FlexRay. Establishing unified standards for data collection is also critical to ensuring interoperability of training data across regions. Consequently, studying methods for collecting training data for machine learning models across different applications of vehicular cloud computing is a valuable research direction.

7.5. Emerging Technology with Machine Learning for Cybersecurity

The introduction of emerging technologies brings new possibilities to vehicular network security. When combined with machine learning, these technologies enable more intelligent and efficient identification and defense against various cybersecurity threats. The decentralized and tamper-proof nature of blockchain can enhance the integrity and reliability of vehicular network data. Combined with machine learning, blockchain can be used for anomaly detection and attack tracing. Blockchain can be used to build distributed trust models, preventing forged data or identities. Machine learning can analyze transaction data recorded in the blockchain to identify potential malicious activities [154]. Quantum computing can significantly accelerate the training of complex machine learning models, facilitating large-scale optimization and encryption analysis for vehicular network security [155]. Quantum machine learning can rapidly analyze massive vehicular network data, while quantum cryptography-based secure communication protocols can be developed for vehicular networks. Additionally, machine learning can process biometric data (e.g., driver facial or behavioral features) to enhance authentication and behavior monitoring capabilities. An anomaly detection system based on driver behavior can identify unauthorized vehicle takeovers using multimodal biometric technologies [156]. Digital twin technology is crucial to the development of vehicular networks as it enables the monitoring and evaluation of dynamic and complex vehicle environments [157]. When combined with machine learning, digital twins can simulate and predict security risks in real time, perform virtual simulations and tracing analysis of network attacks, and optimize defense strategies and vulnerability scanning in real time. Privacy-preserving computing is another vital emerging technology. Techniques such as secure multi-party computation and differential privacy, combined with machine learning, can protect user privacy data in

vehicular networks, enabling collaborative network threat modeling while ensuring privacy protection [158]. Beyond software protection, hardware security modules combined with machine learning can monitor and protect vehicular network devices from physical-layer threats [158]. Machine learning-based analysis of hardware signals can detect anomalies and improve defenses against physical attacks, such as side-channel attacks. Urban air mobility (UAM) expands the scope of vehicular network applications while presenting new security challenges. Adding UAM systems with vehicular networks will create a multimodal transportation network, necessitating robust security mechanisms to ensure seamless coordination between ground and aerial vehicles [159]. Machine learning can be employed to monitor communication data between vehicles and aerial systems in real time, detecting abnormal behaviors or potential attacks. Furthermore, the development of multimodal traffic signal coordination algorithms can optimize ground-air collaborative path planning and enhance emergency response capabilities. In the future, as these technologies continue to evolve, the security and reliability of vehicular networks are expected to improve significantly.

8. Conclusions

This paper is all concerned with the applications of machine learning in ensuring cybersecurity and privacy in cloud computing-assisted vehicular networks. It provides a literature review of vehicular networks and three recent computing paradigms, defining the scope of the types of vehicular networks studied in this paper. The characteristics of different machine learning types and learning strategies under a vehicular cloud computing environment are then discussed. A total of seventy-two papers were selected through a semi-systematic review and categorized into four research themes: intrusion detection systems, anomaly vehicle detection, task offloading security and privacy, and privacy protection. The review summarizes the applicable machine learning algorithms for vehicular cloud computing, highlighting their advantages and disadvantages according to the characteristics of each research theme. For intrusion detection systems, this paper collects the test results from the literature for the study and demonstrates the selection of the current optimal machine learning algorithms. For anomaly vehicle detection, task offloading security and privacy, and privacy protection. This paper further breaks down the application scenarios of machine learning algorithms and briefly describes how machine learning algorithms can safeguard vehicular cloud computing cybersecurity and privacy. In addition, the challenges that the application of machine learning algorithms for vehicular cloud computing can face are analyzed based on the review results. It provides a good reference for researchers on cybersecurity and privacy protection in cloud computing-assisted vehicular networks.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chen, D.; Zhao, H. Data security and privacy protection issues in cloud computing. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; pp. 647–651.
2. Kalmykov, I.A.; Olenov, A.A.; Kononova, N.V.; Peleshenko, T.A.; Dukhovnyj, D.V.; Chistousov, N.K.; Kalmykova, N.I. Improvement of the Cybersecurity of the Satellite Internet of Vehicles through the Application of an Authentication Protocol Based on a Modular Error-Correction Code. *World Electr. Veh. J.* **2024**, *15*, 278. [[CrossRef](#)]

3. Mirzarazi, F.; Danishvar, S.; Mousavi, A. The Safety Risks of AI-Driven Solutions in Autonomous Road Vehicles. *World Electr. Veh. J.* **2024**, *15*, 438. [[CrossRef](#)]
4. Javed, M.; Arslan Akram, M.; Noor Mian, A.; Kumari, S. On the security of a novel privacy-preserving authentication scheme for V2G networks. *Secur. Priv.* **2024**, *7*, e357. [[CrossRef](#)]
5. Lu, Z.; Qu, G.; Liu, Z. A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 760–776. [[CrossRef](#)]
6. Sarker, I.H.; Kayes, A.; Badsha, S.; Alqahtani, H.; Watters, P.; Ng, A. Cybersecurity data science: An overview from machine learning perspective. *J. Big Data* **2020**, *7*, 41. [[CrossRef](#)]
7. Bécsi, T.; Aradi, S.; Gáspár, P. Security issues and vulnerabilities in connected car systems. In Proceedings of the 2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), Budapest, Hungary, 3–5 June 2015; pp. 477–482.
8. Mili, S.; Nguyen, N.; Chelouah, R. Transformation-based approach to security verification for cyber-physical systems. *IEEE Syst. J.* **2019**, *13*, 3989–4000. [[CrossRef](#)]
9. Al Zaabi, A.O.; Yeun, C.Y.; Damiani, E. Autonomous vehicle security: Conceptual model. In Proceedings of the 2019 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific), Jeju, Republic of Korea, 8–10 May 2019; pp. 1–5.
10. Balkus, S.V.; Wang, H.; Cornet, B.D.; Mahabal, C.; Ngo, H.; Fang, H. A survey of collaborative machine learning using 5G vehicular communications. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1280–1303. [[CrossRef](#)]
11. Ali, E.S.; Hasan, M.K.; Hassan, R.; Saeed, R.A.; Hassan, M.B.; Islam, S.; Nafi, N.S.; Bevinakoppa, S. Machine learning technologies for secure vehicular communication in internet of vehicles: Recent advances and applications. *Secur. Commun. Netw.* **2021**, *2021*, 8868355. [[CrossRef](#)]
12. Tan, K.; Bremner, D.; Le Kernec, J.; Zhang, L.; Imran, M. Machine learning in vehicular networking: An overview. *Digit. Commun. Netw.* **2022**, *8*, 18–24. [[CrossRef](#)]
13. Sheikh, M.S.; Liang, J.; Wang, W. Security and privacy in vehicular ad hoc network and vehicle cloud computing: A survey. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 5129620. [[CrossRef](#)]
14. Masood, A.; Lakew, D.S.; Cho, S. Security and privacy challenges in connected vehicular cloud computing. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2725–2764. [[CrossRef](#)]
15. Alalwany, E.; Mahgoub, I. Security and trust management in the internet of vehicles (IoV): Challenges and machine learning solutions. *Sensors* **2024**, *24*, 368. [[CrossRef](#)]
16. Talpur, A.; Gurusamy, M. Machine learning for security in vehicular networks: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2021**, *24*, 346–379. [[CrossRef](#)]
17. Karagiannis, G.; Altintas, O.; Ekici, E.; Heijenk, G.; Jarupan, B.; Lin, K.; Weil, T. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 584–616. [[CrossRef](#)]
18. Zheng, K.; Zheng, Q.; Chatzimisios, P.; Xiang, W.; Zhou, Y. Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2377–2396. [[CrossRef](#)]
19. Campolo, C.; Molinaro, A.; Scopigno, R. (Eds.) *Vehicular ad hoc Networks. Standards, Solutions, and Research*; Springer Nature: Berlin, Germany, 2015.
20. Lu, N.; Cheng, N.; Zhang, N.; Shen, X.; Mark, J.W. Connected vehicles: Solutions and challenges. *IEEE Internet Things J.* **2014**, *1*, 289–299. [[CrossRef](#)]
21. Lv, S.; Qin, Y.; Gan, W.; Xu, Z.; Shi, L. A systematic literature review of vehicle-to-everything in communication, computation and service scenarios. *Int. J. Gen. Syst.* **2024**, *53*, 1042–1072. [[CrossRef](#)]
22. Ma, Z.; Xiao, M.; Xiao, Y.; Pang, Z.; Poor, H.V.; Vucetic, B. High-reliability and low-latency wireless communication for internet of things: Challenges, fundamentals, and enabling technologies. *IEEE Internet Things J.* **2019**, *6*, 7946–7970. [[CrossRef](#)]
23. Ahmed, M.; Mirza, M.A.; Raza, S.; Ahmad, H.; Xu, F.; Khan, W.U.; Lin, Q.; Han, Z. Vehicular communication network enabled CAV data offloading: A review. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 7869–7897. [[CrossRef](#)]
24. Gao, B.; Liu, J.; Zou, H.; Chen, J.; He, L.; Li, K. Vehicle-Road-Cloud Collaborative Perception Framework and Key Technologies: A Review. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 19295–19318. [[CrossRef](#)]
25. Lim, W.Y.B.; Luong, N.C.; Hoang, D.T.; Jiao, Y.; Liang, Y.-C.; Yang, Q.; Niyato, D.; Miao, C. Federated learning in mobile edge networks: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2031–2063. [[CrossRef](#)]
26. Olariu, S. A survey of vehicular cloud research: Trends, applications and challenges. *IEEE Trans. Intell. Transp. Syst.* **2019**, *21*, 2648–2663. [[CrossRef](#)]
27. Hussain, R.; Son, J.; Eun, H.; Kim, S.; Oh, H. Rethinking vehicular communications: Merging VANET with cloud computing. In Proceedings of the 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, Taipei, Taiwan, 3–6 December 2012; pp. 606–609.

28. Khan, W.Z.; Ahmed, E.; Hakak, S.; Yaqoob, I.; Ahmed, A. Edge computing: A survey. *Future Gener. Comput. Syst.* **2019**, *97*, 219–235. [[CrossRef](#)]
29. Wang, X.; Han, Y.; Leung, V.C.; Niyato, D.; Yan, X.; Chen, X. Convergence of edge computing and deep learning: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 869–904. [[CrossRef](#)]
30. Silva, L.; Magaia, N.; Sousa, B.; Kobusińska, A.; Casimiro, A.; Mavromoustakis, C.X.; Mastorakis, G.; De Albuquerque, V.H.C. Computing paradigms in emerging vehicular environments: A review. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 491–511. [[CrossRef](#)]
31. Hou, X.; Li, Y.; Chen, M.; Wu, D.; Jin, D.; Chen, S. Vehicular fog computing: A viewpoint of vehicles as the infrastructures. *IEEE Trans. Veh. Technol.* **2016**, *65*, 3860–3873. [[CrossRef](#)]
32. Fan, W.; Hua, M.; Zhang, Y.; Su, Y.; Li, X.; Tang, B.; Wu, F.; Liu, Y.a. Game-based task offloading and resource allocation for vehicular edge computing with edge-edge cooperation. *IEEE Trans. Veh. Technol.* **2023**, *72*, 7857–7870. [[CrossRef](#)]
33. Yang, J.; Yang, K.; Dai, X.; Xiao, Z.; Jiang, H.; Zeng, F.; Li, B. Service-Aware Computation Offloading for Parallel Tasks in VEC Networks. *IEEE Internet Things J.* **2024**. [[CrossRef](#)]
34. Wang, K.; Wang, X.; Liu, X.; Jolfaei, A. Task offloading strategy based on reinforcement learning computing in edge computing architecture of internet of vehicles. *IEEE Access* **2020**, *8*, 173779–173789. [[CrossRef](#)]
35. Xiao, Z.; Xiao, Y. Security and privacy in cloud computing. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 843–859. [[CrossRef](#)]
36. Alshathri, S.; Sayed, A.; Hemdan, E.E.-D. An Intelligent Attack Detection Framework for the Internet of Autonomous Vehicles with Imbalanced Car Hacking Data. *World Electr. Veh. J.* **2024**, *15*, 356. [[CrossRef](#)]
37. Solaas, J.R.V.; Mariconti, E.; Tuptuk, N. Systematic Literature Review: Anomaly Detection in Connected and Autonomous Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2024**, *1*, 1–16. [[CrossRef](#)]
38. Manivannan, D.; Moni, S.S.; Zeadally, S. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETWORKS (VANETs). *Veh. Commun.* **2020**, *25*, 100247. [[CrossRef](#)]
39. Lai, C.; Lu, R.; Zheng, D.; Shen, X. Security and privacy challenges in 5G-enabled vehicular networks. *IEEE Netw.* **2020**, *34*, 37–45. [[CrossRef](#)]
40. He, W.; Yan, G.; Da Xu, L. Developing vehicular data cloud services in the IoT environment. *IEEE Trans. Ind. Inf.* **2014**, *10*, 1587–1595. [[CrossRef](#)]
41. Fu, Y.; Li, C.; Yu, F.R.; Luan, T.H.; Zhang, Y. A survey of driving safety with sensing, vehicular communications, and artificial intelligence-based collision avoidance. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 6142–6163. [[CrossRef](#)]
42. Bendiab, G.; Hameurlaine, A.; Germanos, G.; Kolokotronis, N.; Shiaeles, S. Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 3614–3637. [[CrossRef](#)]
43. Jordan, M.I.; Mitchell, T.M. Machine learning: Trends, perspectives, and prospects. *Science* **2015**, *349*, 255–260. [[CrossRef](#)] [[PubMed](#)]
44. Kotsiantis, S.B.; Zaharakis, I.; Pintelas, P. Supervised machine learning: A review of classification techniques. *Emerg. Artif. Intell. Appl. Comput. Eng.* **2007**, *160*, 3–24.
45. Hastie, T.; Tibshirani, R.; Friedman, J.H.; Friedman, J.H. *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*; Springer: Berlin/Heidelberg, Germany, 2009; Volume 2.
46. Caruana, R.; Niculescu-Mizil, A. An empirical comparison of supervised learning algorithms. In Proceedings of the 23rd International Conference on Machine Learning, Pittsburgh, PA, USA, 25–29 June 2006; pp. 161–168.
47. Usama, M.; Qadir, J.; Raza, A.; Arif, H.; Yau, K.-L.A.; Elkhatib, Y.; Hussain, A.; Al-Fuqaha, A. Unsupervised machine learning for networking: Techniques, applications and research challenges. *IEEE Access* **2019**, *7*, 65579–65615. [[CrossRef](#)]
48. Alzubaidi, L.; Zhang, J.; Humaidi, A.J.; Al-Dujaili, A.; Duan, Y.; Al-Shamma, O.; Santamaria, J.; Fadhel, M.A.; Al-Amidie, M.; Farhan, L. Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions. *J. Big Data* **2021**, *8*, 1–74. [[CrossRef](#)]
49. Ergen, T.; Kozat, S.S. Unsupervised anomaly detection with LSTM neural networks. *IEEE Trans. Neural Netw. Learn. Syst.* **2019**, *31*, 3127–3141. [[CrossRef](#)]
50. Sutton, R.S.; Barto, A.G. *Reinforcement Learning: An Introduction*; MIT Press: Cambridge, MA, USA, 2018.
51. Arulkumaran, K.; Deisenroth, M.P.; Brundage, M.; Bharath, A.A. Deep reinforcement learning: A brief survey. *IEEE Signal Process. Mag.* **2017**, *34*, 26–38. [[CrossRef](#)]
52. Nguyen, T.T.; Nguyen, N.D.; Nahavandi, S. Deep reinforcement learning for multiagent systems: A review of challenges, solutions, and applications. *IEEE Trans. Cybern.* **2020**, *50*, 3826–3839. [[CrossRef](#)] [[PubMed](#)]
53. Naik, D.; Naik, N. The changing landscape of machine learning: A comparative analysis of centralized machine learning, distributed machine learning and federated machine learning. In Proceedings of the UK Workshop on Computational Intelligence, Birmingham, UK, 6–8 September 2023; pp. 18–28.
54. Drainakis, G.; Katsaros, K.V.; Pantazopoulos, P.; Sourlas, V.; Amditis, A. Federated vs. centralized machine learning under privacy-elastic users: A comparative analysis. In Proceedings of the 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 24–27 November 2020; pp. 1–8.

55. AbdulRahman, S.; Tout, H.; Ould-Slimane, H.; Mourad, A.; Talhi, C.; Guizani, M. A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. *IEEE Internet Things J.* **2020**, *8*, 5476–5497. [[CrossRef](#)]
56. Hu, S.; Chen, X.; Ni, W.; Hossain, E.; Wang, X. Distributed machine learning for wireless communication networks: Techniques, architectures, and applications. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1458–1493. [[CrossRef](#)]
57. Li, L.; Fan, Y.; Tse, M.; Lin, K.-Y. A review of applications in federated learning. *Comput. Ind. Eng.* **2020**, *149*, 106854. [[CrossRef](#)]
58. Pan, S.J.; Yang, Q. A survey on transfer learning. *IEEE Trans. Knowl. Data Eng.* **2009**, *22*, 1345–1359. [[CrossRef](#)]
59. Zhuang, F.; Qi, Z.; Duan, K.; Xi, D.; Zhu, Y.; Zhu, H.; Xiong, H.; He, Q. A comprehensive survey on transfer learning. *Proc. IEEE* **2020**, *109*, 43–76. [[CrossRef](#)]
60. Liu, Y.; Kang, Y.; Xing, C.; Chen, T.; Yang, Q. A secure federated transfer learning framework. *IEEE Intell. Syst.* **2020**, *35*, 70–82. [[CrossRef](#)]
61. Snyder, H. Literature review as a research methodology: An overview and guidelines. *J. Bus. Res.* **2019**, *104*, 333–339. [[CrossRef](#)]
62. Brereton, P.; Kitchenham, B.A.; Budgen, D.; Turner, M.; Khalil, M. Lessons from applying the systematic literature review process within the software engineering domain. *J. Syst. Softw.* **2007**, *80*, 571–583. [[CrossRef](#)]
63. Hu, P.; Dhelim, S.; Ning, H.; Qiu, T. Survey on fog computing: Architecture, key technologies, applications and open issues. *J. Netw. Comput. Appl.* **2017**, *98*, 27–42. [[CrossRef](#)]
64. Whaiduzzaman, M.; Sookhak, M.; Gani, A.; Buyya, R. A survey on vehicular cloud computing. *J. Netw. Comput. Appl.* **2014**, *40*, 325–344. [[CrossRef](#)]
65. Tang, F.; Mao, B.; Kato, N.; Gui, G. Comprehensive survey on machine learning in vehicular network: Technology, applications and challenges. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2027–2057. [[CrossRef](#)]
66. Wu, W.; Li, R.; Xie, G.; An, J.; Bai, Y.; Zhou, J.; Li, K. A survey of intrusion detection for in-vehicle networks. *IEEE Trans. Intell. Transp. Syst.* **2019**, *21*, 919–933. [[CrossRef](#)]
67. Lampe, B.; Meng, W. Intrusion detection in the automotive domain: A comprehensive review. *IEEE Commun. Surv. Tutor.* **2023**, *5*, 869–906. [[CrossRef](#)]
68. Rajapaksha, S.; Kalutarage, H.; Al-Kadri, M.O.; Petrovski, A.; Madzudzo, G.; Cheah, M. Ai-based intrusion detection systems for in-vehicle networks: A survey. *ACM Comput. Surv.* **2023**, *55*, 1–40. [[CrossRef](#)]
69. Lai, Q.; Xiong, C.; Chen, J.; Wang, W.; Chen, J.; Gadekallu, T.R.; Cai, M.; Hu, X. Improved Transformer-Based Privacy-Preserving Architecture for Intrusion Detection in Secure V2X Communications. *IEEE Trans. Consum. Electron.* **2024**, *70*, 1810–1820. [[CrossRef](#)]
70. Bhavsar, M.H.; Bekele, Y.B.; Roy, K.; Kelly, J.C.; Limbrick, D. FL-IDS: Federated Learning-Based Intrusion Detection System Using Edge Devices for Transportation IoT. *IEEE Access* **2024**, *12*, 52215–52226. [[CrossRef](#)]
71. Abdel-Basset, M.; Moustafa, N.; Hawash, H.; Razzak, I.; Sallam, K.M.; Elkomy, O.M. Federated Intrusion Detection in Blockchain-Based Smart Transportation Systems. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 2523–2537. [[CrossRef](#)]
72. Kumar, R.; Kumar, P.; Aljuhani, A.; Jolfaei, A.; Islam, A.N.; Mohammad, N. Secure Data Dissemination Scheme for Digital Twin Empowered Vehicular Networks in Open RAN. *IEEE Trans. Veh. Technol.* **2023**, *73*, 9234–9246. [[CrossRef](#)]
73. Sandosh, S.; Doshi, S.; Joshi, A. Enhancing Security in Automobile Edge Computing through Federated Learning and Blockchain. In Proceedings of the iQ-CHESS 2023–2023 IEEE International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security, Kottayam, India, 15–16 September 2023.
74. Liu, H.; Zhang, S.; Zhang, P.; Zhou, X.; Shao, X.; Pu, G.; Zhang, Y. Blockchain and Federated Learning for Collaborative Intrusion Detection in Vehicular Edge Computing. *IEEE Trans. Veh. Technol.* **2021**, *70*, 6073–6084. [[CrossRef](#)]
75. Alsulami, A.A.; Al-Haija, Q.A.; Alturki, B.; Alqahtani, A.; Alsini, R. Security strategy for autonomous vehicle cyber-physical systems using transfer learning. *J. Cloud Comput.* **2023**, *12*, 181. [[CrossRef](#)]
76. Gad, A.R.; Nashat, A.A.; Barkat, T.M. Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset. *IEEE Access* **2021**, *9*, 142206–142217. [[CrossRef](#)]
77. Sousa, B.; Magaia, N.; Silva, S. An Intelligent Intrusion Detection System for 5G-Enabled Internet of Vehicles. *Electronics* **2023**, *12*, 1757. [[CrossRef](#)]
78. Aloqaily, M.; Otoum, S.; Ridhawi, I.A.; Jararweh, Y. An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Netw.* **2019**, *90*, 101842. [[CrossRef](#)]
79. Mirzaee, P.H.; Shojafar, M.; Bagheri, H.; Chan, T.H.; Cruickshank, H.; Tafazolli, R. A Two-layer Collaborative Vehicle-Edge Intrusion Detection System for Vehicular Communications. In Proceedings of the IEEE Vehicular Technology Conference, Norman, OK, USA, 27–30 September 2021.
80. Alladi, T.; Kohli, V.; Chamola, V.; Yu, F.R.; Guizani, M. Artificial Intelligence (AI)-Empowered Intrusion Detection Architecture for the Internet of Vehicles. *IEEE Wirel. Commun.* **2021**, *28*, 144–149. [[CrossRef](#)]
81. Ogundoyin, S.O.; Kamil, I.A. An efficient authentication scheme with strong privacy preservation for fog-assisted vehicular ad hoc networks based on blockchain and neuro-fuzzy. *Veh. Commun.* **2021**, *31*, 100384. [[CrossRef](#)]
82. Yang, J.; Hu, J.; Yu, T. Federated AI-Enabled In-Vehicle Network Intrusion Detection for Internet of Vehicles. *Electronics* **2022**, *11*, 3658. [[CrossRef](#)]

83. Kumar, P.; Kumar, R.; Gupta, G.P.; Tripathi, R. BDEdge: Blockchain and Deep-Learning for Secure Edge-Envisioned Green CAVs. *IEEE Trans. Green Commun. Netw.* **2022**, *6*, 1330–1339. [[CrossRef](#)]
84. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Kumar, N.; Hassan, M.M. A Privacy-Preserving-Based Secure Framework Using Blockchain-Enabled Deep-Learning in Cooperative Intelligent Transport System. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 16492–16503. [[CrossRef](#)]
85. Sedjelmaci, H. Attacks detection and decision framework based on generative adversarial network approach: Case of vehicular edge computing network. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4073. [[CrossRef](#)]
86. Kasongo, S.M. A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. *Comput Commun* **2023**, *199*, 113–125. [[CrossRef](#)]
87. Yaqoob, S.; Hussain, A.; Subhan, F.; Pappalardo, G.; Awais, M. Deep Learning Based Anomaly Detection for Fog-Assisted IoVs Network. *IEEE Access* **2023**, *11*, 19024–19038. [[CrossRef](#)]
88. Mondal, K.K.; Mahendia, D.; Das, D.; Kalra, S. Edge-Centric Security Framework for Electric Vehicle Connectivity: A Deep Learning Approach. In Proceedings of the 2023 28th Asia Pacific Conference on Communications, APCC 2023, Sydney, Australia, 19–22 November 2023; pp. 448–453.
89. Sonker, S.K.; Raina, V.K.; Sagar, B.B.; Bansal, R.C. A Cyber Physical Security for Electrical Vehicles using Deep learning. In Proceedings of the 2024 International Conference on Automation and Computation, AUTOCOM 2024, Dehradun, India, 14–16 March 2024; pp. 519–523.
90. Khalil, A.; Farman, H.; Nasralla, M.M.; Jan, B.; Ahmad, J. Artificial Intelligence-based intrusion detection system for V2V communication in vehicular adhoc networks. *Ain Shams Eng. J.* **2024**, *15*, 102616. [[CrossRef](#)]
91. Qin, J.; Xun, Y.; Liu, J. CVMIDS: Cloud-Vehicle Collaborative Intrusion Detection System for Internet of Vehicles. *IEEE Internet Things J.* **2024**, *11*, 321–332. [[CrossRef](#)]
92. Houda, Z.A.E.; Moudoud, H.; Brik, B.; Khoukhi, L. Blockchain-Enabled Federated Learning for Enhanced Collaborative Intrusion Detection in Vehicular Edge Computing. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 7661–7672. [[CrossRef](#)]
93. Bergies, S.; Aljohani, T.M.; Su, S.-F.; Elsis, M. An IoT-based deep-learning architecture to secure automated electric vehicles against cyberattacks and data loss. *IEEE Trans. Syst. Man Cybern. Syst.* **2024**, *54*, 5717–5732. [[CrossRef](#)]
94. Kumar, P.; Kumar, R.; Jolfaei, A.; Mohammad, N. An Automated Threat Intelligence Framework for Vehicle Road Cooperation Systems. *IEEE Internet Things J.* **2024**, *11*, 35964–35974. [[CrossRef](#)]
95. Balaji, P.; Cengiz, K.; Babu, S.; Alqahtani, O.; Akleylek, S. Metaheuristic optimized complex-valued dilated recurrent neural network for attack detection in internet of vehicular communications. *PeerJ Comput. Sci.* **2024**, *10*, e2366. [[CrossRef](#)] [[PubMed](#)]
96. Zeng, L.; An, Y.; Zhou, H.; Luo, Q.; Lin, Y.; Zhang, Z. A Hybrid Machine Learning-Based Data-Centric Cybersecurity Detection in the 5G-Enabled IoT. *Secur. Priv.* **2024**, *7*, e472. [[CrossRef](#)]
97. Hossain, S.; Senouci, S.-M.; Brik, B.; Boualouache, A. A privacy-preserving Self-Supervised Learning-based intrusion detection system for 5G-V2X networks. *Ad Hoc Netw.* **2025**, *166*, 103674. [[CrossRef](#)]
98. Cui, J.; Xiao, J.T.; Zhong, H.; Zhang, J.; Wei, L.; Bolodurina, I.; He, D.B. LH-IDS: Lightweight Hybrid Intrusion Detection System Based on Differential Privacy in VANETs. *IEEE Trans. Mob. Comput.* **2024**, *23*, 12195–12210. [[CrossRef](#)]
99. Boualouache, A.; Engel, T. Federated learning-based scheme for detecting passive mobile attackers in 5G vehicular edge computing. *Ann. Telecommun.* **2022**, *77*, 201–220. [[CrossRef](#)]
100. Tham, C.K.; Yang, L.; Khanna, A.; Gera, B. Federated Learning for Anomaly Detection in Vehicular Networks. In Proceedings of the IEEE Vehicular Technology Conference, Hong Kong, China, 10–13 October 2023.
101. Grover, H.; Alladi, T.; Chamola, V.; Singh, D.; Choo, K.K.R. Edge Computing and Deep Learning Enabled Secure Multitier Network for Internet of Vehicles. *IEEE Internet Things J.* **2021**, *8*, 14787–14796. [[CrossRef](#)]
102. Gyawali, S.; Qian, Y.; Hu, R. Deep reinforcement learning based dynamic reputation policy in 5g based vehicular communication networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 6136–6146. [[CrossRef](#)]
103. Gawas, M.; Patil, H.; Govekar, S.S. An integrative approach for secure data sharing in vehicular edge computing using Blockchain. *Peer-Peer Netw. Appl.* **2021**, *14*, 2840–2857. [[CrossRef](#)]
104. Gupta, D.; Moni, S.S.; Tosun, A.S. Integration of Digital Twin and Federated Learning for Securing Vehicular Internet of Things. In Proceedings of the 2023 Research in Adaptive and Convergent Systems RACS 2023, Gdansk, Poland, 6–10 August 2023.
105. Zhang, Y.; Lin, L.; Huang, Y.; Wang, X.; Hsieh, S.-Y.; Gadekallu, T.; Piran, M.J. A Cooperative Vehicle-Road System for Anomaly Detection on Vehicle Tracks With Augmented Intelligence of Things. *IEEE Internet Things J.* **2024**, *11*, 35975–35988. [[CrossRef](#)]
106. Wang, W.; Zhu, Q.; Lee, C.-W.; Zhang, Z. A Vehicle Abnormal Behavior Detection Model in Single Intelligent Vehicle Scenarios. *J. Internet Technol.* **2024**, *25*, 771–780. [[CrossRef](#)]
107. Lin, C.; Han, G.; Qi, X.; Guizani, M.; Shu, L. A distributed mobile fog computing scheme for mobile delay-sensitive applications in SDN-enabled vehicular networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5481–5493. [[CrossRef](#)]
108. Häckel, T.; Meyer, P.; Korf, F.; Schmidt, T.C. Secure time-sensitive software-defined networking in vehicles. *IEEE Trans. Veh. Technol.* **2022**, *72*, 35–51. [[CrossRef](#)]

109. Lang, P.; Tian, D.; Duan, X.; Zhou, J. Mobility-Aware Computation Offloading and Blockchain-based Handover in Vehicular Edge Computing Networks. In Proceedings of the IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC, Macau, China, 8–12 October 2022; pp. 176–182.
110. Ju, Y.; Chen, Y.; Cao, Z.; Wang, H.; Liu, L.; Pei, Q.; Kumar, N. Learning Based and Physical-layer Assisted Secure Computation Offloading in Vehicular Spectrum Sharing Networks. In Proceedings of the INFOCOM WKSHPS 2022–IEEE Conference on Computer Communications Workshops, Virtual Conference, 2–5 May 2022.
111. Huang, Q.; Xu, X.; Chen, J. Learning-aided fine grained offloading for real-time applications in edge-cloud computing. *Wirel. Netw.* **2021**, *30*, 3805–3820. [[CrossRef](#)]
112. Xu, S.; Guo, C.; Hu, R.Q.; Qian, Y. Blockchain-Inspired Secure Computation Offloading in a Vehicular Cloud Network. *IEEE Internet Things J.* **2022**, *9*, 14723–14740. [[CrossRef](#)]
113. Zhang, G.; Luo, Z.; Yang, T. Distributed Computation Offloading Based on Deep Reinforcement Learning and Blockchain in Internet of Vehicles. In Proceedings of the 2023 IEEE/CIC International Conference on Communications in China, ICC3 2023, Dalian, China, 10–12 August 2023.
114. Moghaddasi, K.; Rajabi, S.; Gharehchopogh, F.S. Multi-Objective Secure Task Offloading Strategy for Blockchain-Enabled IoV-MEC Systems: A Double Deep Q-Network Approach. *IEEE Access* **2024**, *12*, 3437–3463. [[CrossRef](#)]
115. Zhang, K.; Zhu, Y.X.; Leng, S.P.; He, Y.J.; Maharjan, S.; Zhang, Y. Deep Learning Empowered Task Offloading for Mobile Edge Computing in Urban Informatics. *IEEE Internet Things J.* **2019**, *6*, 7635–7647. [[CrossRef](#)]
116. Ju, Y.; Cao, Z.W.; Chen, Y.C.; Liu, L.; Pei, Q.Q.; Mumtaz, S.; Dong, M.X.; Guizani, M. NOMA-Assisted Secure Offloading for Vehicular Edge Computing Networks With Asynchronous Deep Reinforcement Learning. *IEEE Trans. Intell. Transp. Syst.* **2023**, *25*, 2627–2640. [[CrossRef](#)]
117. Ju, Y.; Cao, Z.; Chen, Y.; Liu, L.; Pei, Q.; Mumtaz, S. Energy Efficient Secure Offloading in NOMA-aided Vehicular Networks Using A3C Learning. In Proceedings of the IEEE International Conference on Communications, Rome, Italy, 28 May–1 June 2023; pp. 6114–6119.
118. Ju, Y.; Chen, Y.; Cao, Z.; Liu, L.; Pei, Q.; Xiao, M.; Ota, K.; Dong, M.; Leung, V.C.M. Joint Secure Offloading and Resource Allocation for Vehicular Edge Computing Network: A Multi-Agent Deep Reinforcement Learning Approach. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 5555–5569. [[CrossRef](#)]
119. Samy, A.; Elgendy, I.A.; Yu, H.; Zhang, W.; Zhang, H. Secure Task Offloading in Blockchain-Enabled Mobile Edge Computing With Deep Reinforcement Learning. *IEEE Trans. Netw. Serv. Manage.* **2022**, *19*, 4872–4887. [[CrossRef](#)]
120. Lang, P.; Tian, D.; Duan, X.; Zhou, J.; Sheng, Z.; Leung, V.C.M. Blockchain-Based Cooperative Computation Offloading and Secure Handover in Vehicular Edge Computing Networks. *IEEE Trans. Intell. Veh.* **2023**, *8*, 3839–3853. [[CrossRef](#)]
121. Mourad, A.; Tout, H.; Wahab, O.A.; Otrok, H.; Dbouk, T. Ad Hoc Vehicular Fog Enabling Cooperative Low-Latency Intrusion Detection. *IEEE Internet Things J.* **2021**, *8*, 829–843. [[CrossRef](#)]
122. Liao, H.; Mu, Y.; Zhou, Z.; Sun, M.; Wang, Z.; Pan, C. Blockchain and Learning-Based Secure and Intelligent Task Offloading for Vehicular Fog Computing. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4051–4063. [[CrossRef](#)]
123. Zheng, X.; Li, M.; Chen, Y.; Guo, J.; Alam, M.; Hu, W. Blockchain-Based Secure Computation Offloading in Vehicular Networks. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4073–4087. [[CrossRef](#)]
124. Wang, K.; Wang, X.; Liu, X. A High Reliable Computing Offloading Strategy Using Deep Reinforcement Learning for IoVs in Edge Computing. *J. Grid Comput.* **2021**, *19*, 15. [[CrossRef](#)]
125. Sun, H.; Ma, D.; She, H.; Guo, Y. EC-DDPG: DDPG-Based Task Offloading Framework of Internet of Vehicle for Mission Critical Applications. In Proceedings of the 2023 IEEE International Conference on Communications Workshops: Sustainable Communications for Renaissance, ICC Workshops 2023, Rome, Italy, 28 May–1 June 2023; pp. 984–989.
126. Shabir, B.; Rahman, A.U.; Malik, A.W.; Buyya, R.; Khan, M.A. A federated multi-agent deep reinforcement learning for vehicular fog computing. *J. Supercomput.* **2023**, *79*, 6141–6167. [[CrossRef](#)]
127. Liang, P.; Chen, W.; Fan, H.; Zhu, H. Leveraging Time-Critical Computation and AI Techniques for Task Offloading in Internet of Vehicles Network Applications. *Electronics* **2024**, *13*, 3334. [[CrossRef](#)]
128. Kaci, A.; Rachedi, A. Mc-track: A cloud based data oriented vehicular tracking system with adaptive security. In Proceedings of the IEEE Global Communications Conference, GLOBECOM, Waikoloa, HI, USA, 9–13 December 2019.
129. Lidkea, V.M.; Muresan, R.; Al-Dweik, A. Convolutional neural network framework for encrypted image classification in cloud-based ITS. *IEEE Open J. Intell. Transp. Syst.* **2020**, *1*, 35–50. [[CrossRef](#)]
130. Vinita, L.J.; Vetriselvi, V. SEAFL: Transforming Federated Learning for Enhanced Privacy in 6G-Enabled Vehicles. In Proceedings of the 2023 Annual International Conference on Emerging Research Areas: International Conference on Intelligent Systems, AICERA/ICIS 2023, Kanjirapally, India, 16–18 November 2023.
131. Teimoori, Z.; Yassine, A.; Hossain, M.S. Smart Vehicles Recommendation System for Artificial Intelligence-Enabled Communication. *IEEE Trans Consum Electron* **2024**, *70*, 3914–3925. [[CrossRef](#)]

132. Patel, V.A.; Bhattacharya, P.; Tanwar, S.; Jadav, N.K.; Gupta, R. BFLEdge: Blockchain based federated edge learning scheme in V2X underlying 6G communications. In Proceedings of the Confluence 2022-12th International Conference on Cloud Computing, Data Science and Engineering, Virtual Conference, 27–28 January 2022; pp. 146–152.
133. Dai, Y.; Xu, D.; Zhang, K.; Maharjan, S.; Zhang, Y. Deep Reinforcement Learning and Permissioned Blockchain for Content Caching in Vehicular Edge Computing and Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4312–4324. [[CrossRef](#)]
134. He, Y.; Huang, K.; Zhang, G.; Li, J.; Chen, J.; Leung, V.C.M. A Blockchain-Enabled Federated Learning System with Edge Computing for Vehicular Networks. In Proceedings of the 2021 IEEE Globecom Workshops, GC Wkshps 2021-Proceedings 2021, Madrid, Spain, 7–11 December 2021.
135. Chen, J.; Li, K.; Yu, P.S. Privacy-Preserving Deep Learning Model for Decentralized VANETs Using Fully Homomorphic Encryption and Blockchain. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 11633–11642. [[CrossRef](#)]
136. Olowononi, F.O.; Rawat, D.B.; Liu, C. Federated learning with differential privacy for resilient vehicular cyber physical systems. In Proceedings of the 2021 IEEE 18th Annual Consumer Communications and Networking Conference, CCNC 2021, Las Vegas, NV, USA, 9–12 January 2021.
137. Devarajan, G.G.; Thirunnavukkarasan, M.; Amanullah, S.I.; Vignesh, T.; Sivaraman, A. An integrated security approach for vehicular networks in smart cities. *Trans. Emerg. Telecommun. Technol.* **2023**, *34*, e4757. [[CrossRef](#)]
138. Fan, N.; Liu, J.; Zhao, S.; Dai, Y.; Fan, W. TLPP: Deep Learning Based Two-layer Privacy Preserving Mechanism for Protecting Vehicle Trajectory Data. *IEEE Internet Things J.* **2024**, *11*, 36084–36098. [[CrossRef](#)]
139. Xiao, H.; Qiu, C.; Yang, Q.; Huang, H.; Wang, J.; Su, C. Deep reinforcement learning for optimal resource allocation in blockchain-based IoV secure systems. In Proceedings of the 2020 16th International Conference on Mobility, Sensing and Networking, MSN 2020, Tokyo, Japan, 17–19 December 2020; pp. 137–144.
140. Bai, T.; Fu, S.; Yang, Q. Privacy-Preserving Object Detection with Secure Convolutional Neural Networks for Vehicular Edge Computing. *Future Internet* **2022**, *14*, 316. [[CrossRef](#)]
141. Yang, W.; Guan, Z.; Wu, L.; He, Z. A Secure Neural Network Inference Framework for Intelligent Connected Vehicles. *IEEE Netw.* **2024**, *38*, 120–127. [[CrossRef](#)]
142. Dai, P.; Huang, Y.; Wu, X.; Li, K.; Xing, H.; Liu, K. Freshness and Security-Aware Cache Update in Blockchain-Based Vehicular Edge Networks. *IEEE Trans. Consum. Electron.* **2024**, *70*, 108–121. [[CrossRef](#)]
143. Shang, Y.; Li, Z.; Li, S.; Shao, Z.; Jian, L. An Information Security Solution for Vehicle-to-grid Scheduling by Distributed Edge Computing and Federated Deep Learning. *IEEE Trans. Ind. Appl.* **2024**, *60*, 4381–4395. [[CrossRef](#)]
144. Li, C.L.; Zhang, Y.; Wu, J.Y.; Luo, Y.L.; Yu, S. Smart Contract-Based Decentralized Data Sharing and Content Delivery for Intelligent Connected Vehicles in Edge Computing. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 14535–14545. [[CrossRef](#)]
145. Fardad, M.; Muntean, G.; Tal, I. A Blockchain-Enabled Vehicular Edge Computing Framework for Secure Performance-oriented V2X Service Delivery. *IEEE Trans. Veh. Technol.* **2024**, *73*, 13853–13867. [[CrossRef](#)]
146. Zhang, T.; Xu, D.; Ren, P.; Yu, K.; Guizani, M. DFLNet: Deep Federated Learning Network With Privacy Preserving for Vehicular LoRa Nodes Fingerprinting. *IEEE Trans. Veh. Technol.* **2024**, *73*, 2901–2905. [[CrossRef](#)]
147. Tang, M.; Huang, Z.; Deng, G. FEDL: Confidential Deep Learning for Autonomous Driving in VANETs Based on Functional Encryption. *Trans. Intell. Transport. Sys.* **2024**, *25*, 21074–21085. [[CrossRef](#)]
148. Kalidoss, L.; Thouti, S.; Arunachalam, R.; Ramamurthy, P. An efficient model of enhanced optimization and dilated-GRU based secured multi-access edge computing with blockchain for VANET sector. *Expert Syst. Appl.* **2025**, *260*, 125275. [[CrossRef](#)]
149. Chen, T.; Bai, X.; Zhao, J.; Wang, H.; Du, B.; Li, L.; Zhang, S. ShieldTSE: A Privacy-Enhanced Split Federated Learning Framework for Traffic State Estimation in IoV. *IEEE Internet Things J.* **2024**, *11*, 37324–37339. [[CrossRef](#)]
150. Ji, H.; Wang, L.; Qin, H.; Wang, Y.; Zhang, J.; Chen, B. In-Vehicle Network Injection Attacks Detection Based on Feature Selection and Classification. *Automot. Innov.* **2024**, *7*, 138–149. [[CrossRef](#)]
151. Su, Y.; LiWang, M.; Huang, L.; Du, X.; Guizani, N. Green communications for future vehicular networks: Data compression approaches, opportunities, and challenges. *IEEE Netw.* **2020**, *34*, 184–190. [[CrossRef](#)]
152. He, Y.; Wang, Y.; Lin, Q.; Li, J. Meta-hierarchical reinforcement learning (MHRL)-based dynamic resource allocation for dynamic vehicular networks. *IEEE Trans. Veh. Technol.* **2022**, *71*, 3495–3506. [[CrossRef](#)]
153. Marwah, G.P.K.; Jain, A. A hybrid optimization with ensemble learning to ensure VANET network stability based on performance analysis. *Sci. Rep.* **2022**, *12*, 10287. [[CrossRef](#)]
154. Ahmad, J.; Zia, M.U.; Naqvi, I.H.; Chattha, J.N.; Butt, F.A.; Huang, T.; Xiang, W. Machine learning and blockchain technologies for cybersecurity in connected vehicles. *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.* **2024**, *14*, e1515. [[CrossRef](#)]
155. Sutradhar, K. A quantum cryptographic protocol for secure vehicular communication. *IEEE Trans. Intell. Transp. Syst.* **2023**, *25*, 3513–3522. [[CrossRef](#)]
156. Salek, M.S.; Khan, S.M.; Rahman, M.; Deng, H.-W.; Islam, M.; Khan, Z.; Chowdhury, M.; Shue, M. A review on cybersecurity of cloud computing for supporting connected vehicle applications. *IEEE Internet Things J.* **2022**, *9*, 8250–8268. [[CrossRef](#)]

157. Yigit, Y.; Maglaras, L.; Buchanan, W.J.; Canberk, B.; Shin, H.; Duong, T.Q. AI-Enhanced Digital Twin Framework for Cyber-Resilient 6G Internet-of-Vehicles Networks. *IEEE Internet Things J.* **2024**, *11*, 36168–36181. [[CrossRef](#)]
158. Xie, Y.; Zhou, Y.; Xu, J.; Zhou, J.; Chen, X.; Xiao, F. Cybersecurity protection on in-vehicle networks for distributed automotive cyber-physical systems: State-of-the-art and future challenges. *Softw. Pract. Exp.* **2021**, *51*, 2108–2127. [[CrossRef](#)]
159. Xie, Y.; Gardi, A.; Sabatini, R. Cybersecurity trends in low-altitude air traffic management. In Proceedings of the 2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC), Portsmouth, VA, USA, 18–22 September 2022; pp. 1–9.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.