Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.053037

REVIEW

Deep Transfer Learning Techniques in Intrusion Detection System-Internet of Vehicles: A State-of-the-Art Review

Wufei Wu[1], Javad Hassannataj Joloudari[2,3,4], Senthil Kumar Jagatheesaperumal[5], Kandala N. V. P. S. Rajesh[6], Silvia Gaftandzhieva[7,*], Sadiq Hussain[8], Rahimullah Rabih[9], Najibullah Haqjoo[10], Mobeen Nazar[11], Hamed Vahdat-Nejad[9] and Rositsa Doneva[12]

[1]School of Information Engineering, Nanchang University, Nanchang, 330031, China

[2]Department of Computer Engineering, Technical and Vocational University (TVU), Tehran, 4631964198, Iran

[3]Department of Computer Engineering, University of Birjand, Birjand, 9717434765, Iran

[4]Department of Computer Engineering, Babol Branch, Islamic Azad University, Babol, 3738147471, Iran

[5]Department of Electronics & Communication Engineering, Mepco Schlenk Engineering College, Sivakasi, 626 005, India

[6]School of Electronics Engineering, VIT-AP University, Near Vijayawada, 522 237, India

[7]Faculty of Mathematics and Informatics, University of Plovdiv Paisii Hilendarski, Plovdiv, 4000, Bulgaria

[8]Examination Branch, Dibrugarh University, Dibrugarh, 786004, India

[9]Department of Computer Engineering, Faculty of Engineering, University of Birjand, Birjand, 9717434765, Iran

[10]Faculty of Electrical and Computer Engineering, University of Birjand, Birjand, 9717434765, Iran

[11]Malaysian Institute of Information Technology, Universiti Kuala Lumpur, Kuala Lumpur, 50250, Malaysia

[12]Faculty of Physics and Technology, University of Plovdiv Paisii Hilendarski, Plovdiv, 4000, Bulgaria

*Corresponding Author: Silvia Gaftandzhieva. Email: sissiy88@uni-plovdiv.bg

Received: 23 April 2024 Accepted: 09 July 2024 Published: 15 August 2024

ABSTRACT

The high performance of IoT technology in transportation networks has led to the increasing adoption of Internet of Vehicles (IoV) technology. The functional advantages of IoV include online communication services, accident prevention, cost reduction, and enhanced traffic regularity. Despite these benefits, IoV technology is susceptible to cyber-attacks, which can exploit vulnerabilities in the vehicle network, leading to perturbations, disturbances, non-recognition of traffic signs, accidents, and vehicle immobilization. This paper reviews the state-of-the-art achievements and developments in applying Deep Transfer Learning (DTL) models for Intrusion Detection Systems in the Internet of Vehicles (IDS-IoV) based on anomaly detection. IDS-IoV leverages anomaly detection through machine learning and DTL techniques to mitigate the risks posed by cyber-attacks. These systems can autonomously create specific models based on network data to differentiate between regular traffic and cyber-attacks. Among these techniques, transfer learning models are particularly promising due to their efficacy with tagged data, reduced training time, lower memory usage, and decreased computational complexity. We evaluate DTL models against criteria including the ability to transfer knowledge, detection rate, accurate analysis of complex data, and stability. This review highlights the significant progress made in the field, showcasing how DTL models enhance the performance and reliability of IDS-IoV systems. By examining recent advancements, we provide insights into how DTL can effectively address cyber-attack challenges in IoV environments, ensuring safer and more efficient transportation networks.

KEYWORDS

Cyber-attacks; internet of things; internet of vehicles; intrusion detection system

1 Introduction

The rapid expansion of smart devices in real life has led to the increasing use of the smallest common smart object to the largest specialised smart object. This rapid expansion is unprecedented, estimated to be 38.6 billion by 2025 and 50 billion by 2030 [1]. Its important area is the transportation network, which is not only for the transportation of commercial goods but also a vital need for the development and improvement of the smart city, which is the comfort and satisfaction of the main users. A large part of the transportation network is included in the Internet of Vehicles (IoV), derived from smart transportation. It includes modern technologies such as sensors and actuators connected to the environment and its surroundings. This connection includes connecting to other cars, city networks, etc. The IoV has a direct impact due to intelligent transportation, increasing the driving experience and providing acceptable services according to the user's wishes. From this point of view, the main goal of the IoV is to increase the level of intelligence and capacity of vehicle manufacturing and create new forms of transportation services [1,2]. According to the World Automobile Industry Organization (OICA) statistics, global vehicle ownership in 2015 was nearly 1.3 billion and 92 million cars were produced in 2019 [3]. According to the Statista 2021 report, self-driving cars in the USA alone by 2030 will be between 20.8 and 146 million [4,5]. With this rapid expansion of the connection of vehicles with heterogeneous communications, the challenges in the security system of the IoV network increased. Millions of cars face various security risk. Also, the high interaction of humans creates safety issues and involves human lives. These problems are directly related to the architecture of the automotive electronics system, which by not taking into account monitoring technologies, detection, etc., causes the loss of human lives, so the attackers have taken advantage of these gaps and put the car system under their control. Malicious attackers can control the entire automotive electronic system by accessing in-vehicle networks such as Controller Area Networks (CAN), thus requiring a more technical process than an electronic unit (ECU) controller, as the system wants an effective and fast diagnostic system that can detect various types of attacks. Due to the security protection of cars, the intrusion detection system (IDS) is considered the most efficient and effective method that has attracted the attention of most researchers [6–8]. This system can detect different types of attacks with constant monitoring of data exchange in the network and reacts according to the pre-defined model through machine learning techniques. The authors in [9] proposed an extended lattice model for controlling traffic flow in connected vehicle environments under cyber-attacks, integrating continuous delay feedback control signals. They demonstrate that integrating continuous traffic information and the controller helps mitigate traffic congestion, enhancing the stability as shown by Bode plots of transfer functions. The most efficient machine learning technique in the detection of cyber-attacks in the field of IoV is transfer learning, which is fast and compatible with the intrusion detection system and distinguishes malicious data from normal data. Transfer learning is a machine learning technique in which a model trained for a specific task can be used in a related task [4]. Works of the IDS-IoV using machine and deep learning algorithms are summarised in Table 1.

Table 1: Popular ML & DL algorithms used along with the standard datasets and their performances observed from recent IoV literature

Ref.	Year	ML & DL algorithms	Datasets	Performance (Accuracy)	Data for train	Data for test
[10]	2022	CNN	Private dataset	99%	60%	Validation = 20%, Test = 20%
[11]	2022	TL and CNN	CICIDS2017	99.25%	N/A	N/A
[12]	2022	CNN-LSTM	KDD-CUP99, UNSW-NB15	99.70%	N/A	N/A
[13]	2022	CNN	ToN-IoT	98.33%	N/A	N/A
[14]	2021	CNN-GRU	Private dataset	94%	75%	Validation = 15%, Test = 10%
[15]	2017	RNN	Real-time generating data	86.90%	N/A	N/A
[16]	2022	VGG16 XGBoost	HCRL, Hacking	97.80%, 99.99%	80%	20%
[17]	2023	MTD, VGGNET-16	VGGNet-16	97.20%	N/A	N/A
[18]	2022	STC-IDS, RLS	CAN dataset	99.96%	80%	20%
[19]	2021	P-LeNet model	Combined dataset	98.10%	80%	20%
[20]	2022	CNN-LSTM	CAV datasets	97.30%	70%	30%
[21]	2022	LSTM GRU	DDoS and a car-hacking dataset	99.50%	80%	20%
[22]	2018	CNN	Image Net & Private Dataset	97.20%	1264 samples	1770 samples
[23]	2022	DCNN	CAN	100%	80%	20%

The researchers and practitioners today have been focusing on dealing with the intrusion challenges in IoV independently through deep learning techniques. The last motivates and calls for developing robust and reliable deep learning frameworks for IDS-IoV. In addition, different machine learning and deep transfer learning must be appropriately tailored and optimised to meet the real-time requirements of in-vehicle network IDS, providing promising solutions for IDS-IoV. The main contribution of the study is summarised as follows:

- introducing the current cyber threats faced by IoVs and the relevant background of existing IDS to address their threats.
- review state-of-the-art machine learning and deep learning techniques to address the issues involved in IDS-IoV.
- summarising how to address the attacks on IDS-IoV, with the solutions pointed through ML and DL techniques.
- emphasising the necessity of using deep transfer learning techniques for IDS-IoV issues.
- discussing open research challenges and future research directions for using AI techniques in IDS-IoV.

The rest of the paper is organised as follows. Section 2 provides the survey methodology and the strategy followed for framing the contents of this work. This section also presents sufficient background on the IoV and IDS and the need of the hour for integrating them. Subsequently, Section 3 includes an elaborate discussion on IoV and IDS accumulated from recent literature. Section 4 presents the open research challenges that could drive new research in this domain. Following this, Section 5 summarises the future directions in using modern AI tools and services for addressing the issues in IDS-IoV. Finally, we conclude the paper in Section 6 with the key findings found in this study.

2 Survey Methodology

The analysis in this survey was performed using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology. The study was initiated through a careful exploration of recent literature and certain relevant summaries were considered for inclusion and exclusion of non-relevant articles was performed. Based on the summarised data from the literature and the statistical procedures followed for analysis, effective outcomes on the deep transfer learning for IDS-IoV are presented.

The literature sources were identified from the electronic databases, including IEEE, Elsevier, Springer, MDPI, and other leading publishers. The literature was collected from Google Scholar and the publisher mentioned above. The articles were searched with the use of keywords such as “IoV” and “IDS” or “IoV-IDS” and “deep learning” or “transfer learning”. The articles considered were without any date restriction till December 2023. Searchers were also done on recent thesis works, and technical reports to seek additional advancements in the IoV and IDS. Additionally, an exploration of the list of popular references cited in the chosen standards articles was also considered, which were not screened during the original search.

In the choice of literature considered for the study, there was a classification on the geographic location, and the nativity of the authors was applied. For the meta-analysis, editorial reports, letters, and commentaries were excluded from the search. The detailed strategy followed for shortlisting the core articles for this study is shown in Fig. 1. The inclusion criteria for the literature review were considered the most famous works on IoV, IDS, and the combination of both as main players for the analysis. Further from the abstracts and titles, articles with the key terms on deep learning and transfer learning were considered for this meta-analysis. We screened and classified independently the key characteristics from all abstracts. Further, the articles with inconsistent information content were excluded from the study.

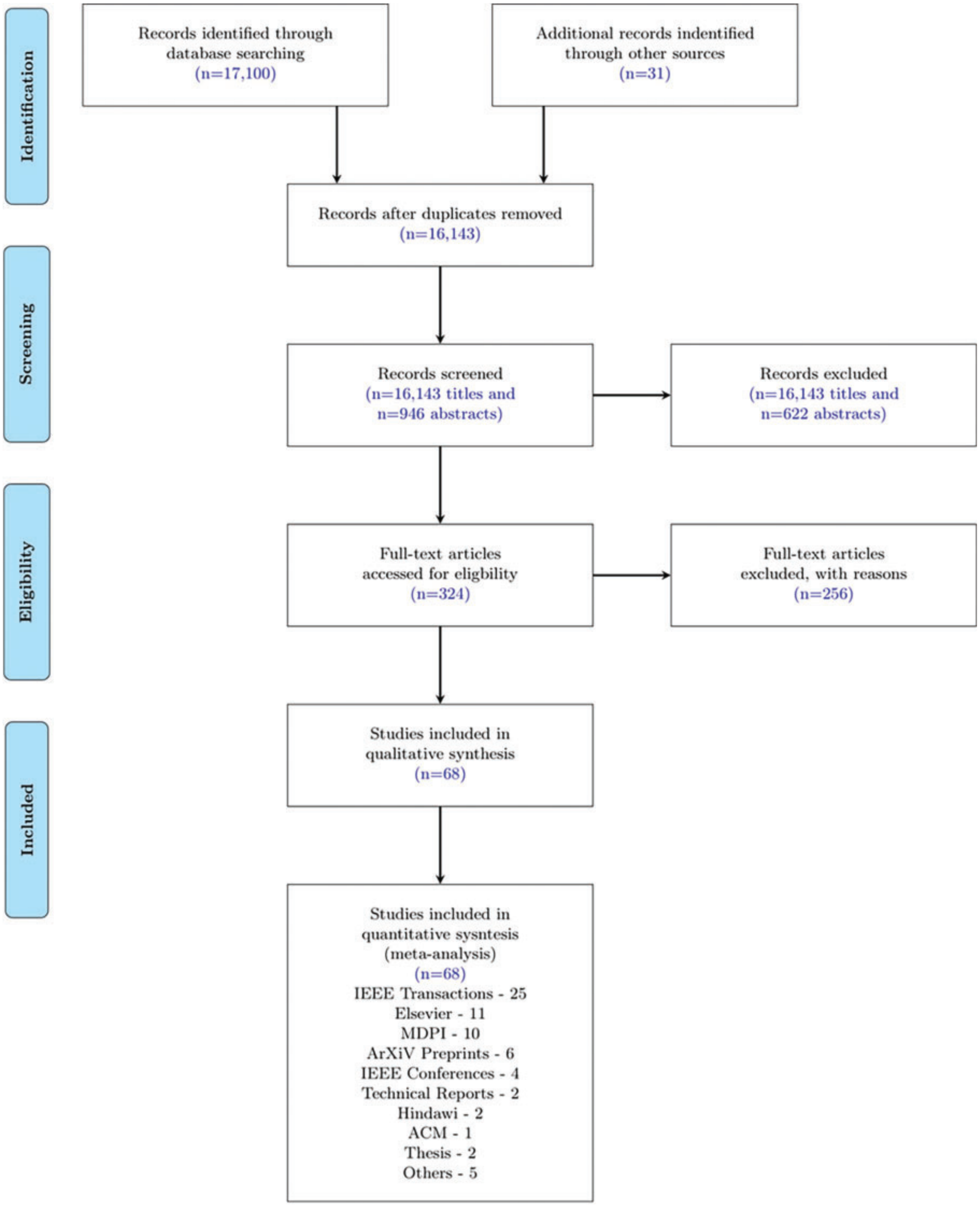
Identification
Screening
Eligibility
Included
Records identified through database searching (n=17,100)
Additional records indentified through other sources (n=31)
Records after duplicates removed (n=16,143)
Records screened (n=16,143 titles and n=946 abstracts)
Records excluded (n=16,143 titles and n=622 abstracts)
Full-text articles accessed for eligbility (n=324)
Full-text articles excluded, with reasons (n=256)
Studies included in qualitative synthesis (n=68)
Studies included in quantitative sysntesis (meta-analysis) (n=68)
IEEE Transactions - 25
Elsevier - 11
MDPI - 10
ArXiV Preprints - 6
IEEE Conferences - 4
Technical Reports - 2
Hindawi - 2
ACM - 1
Thesis - 2
Others - 5

Figure 1: PRISMA flow chart representation of the literature review and the article selection process

2.1 Background

This section starts with a brief introduction to IoV technology. Following that, it explains the implications of IDS over IoV networks. The appealing characteristics of IDS are also discussed, along with its association with the deep learning approach. This section introduces readers to the IoV and IDS-IoV technology and its key principles.

Concerning the recent statistics reported by Allied Market Research, the global market of IoV is anticipated to cross over $200 billion by the end of 2024 [24]. Further, several automobile manufacturers, including BMW, have started developing platforms to integrate IoV services like smart parking, route management, and other infotainment services. Subsequently, vendors from the Information Technology (IT) industry, such as Google, IBM, Apple, Intel, Cisco, etc., are also engaging actively with the governing organisations and manufacturers to help them build robust IoV platforms for this generation.

As most cities are being transformed to be smarter and more connected, it is expected nearly that connected vehicles will be revolutionised as autonomous ones. This could not be realised without an advanced and more sophisticated backbone network. In this regard, IoV is intended to establish a distributed means of the network that integrates the data accumulated from the connected vehicles in vehicular ad hoc networks (VANETs) [25]. Further, a primary goal of IoV is to allow vehicles to communicate with human drivers in real time. Moreover, it is also provisioned with utilising the IoV infrastructure for pedestrians, roadside smart units, fleet management, and other vehicles. Very often, the IoV network communication includes the interactions among modules in the networks, such as 1) Intra vehicle units, 2) Vehicle-to-Vehicle (V2V), 3) Vehicle-to-Infrastructure (V2I), 4) Vehicle-to-Cloud (V2C) and 5) Vehicle-to-Pedestrians (V2P) [26]. Based on such infrastructures, IoV architectures commonly include the capability of robust perception modules and strong backbone networking modules targeted for the intended applications. While modern vehicles are a nodal point in the IoT, it increases convenience and versatility. Further, it also presents a significant potential target for cyber attackers. This fact demands multi-level protection, considering the complexity of the modern vehicle's electrical/electronic (EE) architecture [27]. From the control unit level, which is the core nerve centre for modern vehicles, the state-of-the-art security solutions protect electronic control unit (ECU) firmware and the data from being manipulated and misused. Here, secure on-board communication ensures the integrity and confidentiality of critical network signals. Domain separation and secure gateways allow the overall security of automotive electronics and electrical architecture. In addition, secure communication protocols protect the connection to the cloud, as the firewalls shield the vehicle network and ensure multi-level security solutions.

However, as the threat landscapes are constantly changing with every new connectivity service, the long service of the vehicles opens up new attack vectors [28]. Attackers are continuously perfecting their methods to undermine existing protection mechanisms, find loopholes, and anticipate that they might succeed at one of their attempts. As hackers may gain complete control of the vehicle, it is observed that state-of-the-art security solutions do not provide sufficient assurance when they roll off the production line.

This fact drives the demand for automotive intrusion detection and prevention systems that could provide reliable protection against vehicle cyber-attacks. The embedded intrusion detection software monitors the data traffic on the vehicle network, detects anomalies, and reports them to a cyber-defence backend based on big data analysis technologies. This automated backend solution analyses the attack patterns, and security experts then use the results to decide on countermeasures [29]. Security updates can be broadcast by air to all connected vehicles as a possible countermeasure. As they are connected to the vehicles, the immune system of vehicles gets stronger with every attack and becomes steadily smarter. It was also possible due to the constantly expanding attack signature database, which puts the original equipment manufacturers in a position to adapt their defence systems to modified attack strategies and new cyber risks at any time.

2.2 Internet of Vehicles

From the network perspective, IoV is more like a mobile terminal in the Internet of Vehicles architecture. Its internal part is a distributed real-time system composed of high-speed real-time heterogeneous networks. The communication with the external part is mainly completed through the vehicle gateway, as shown in Fig. 2. The network architecture is heterogeneous, real-time, and cost-sensitive [30].

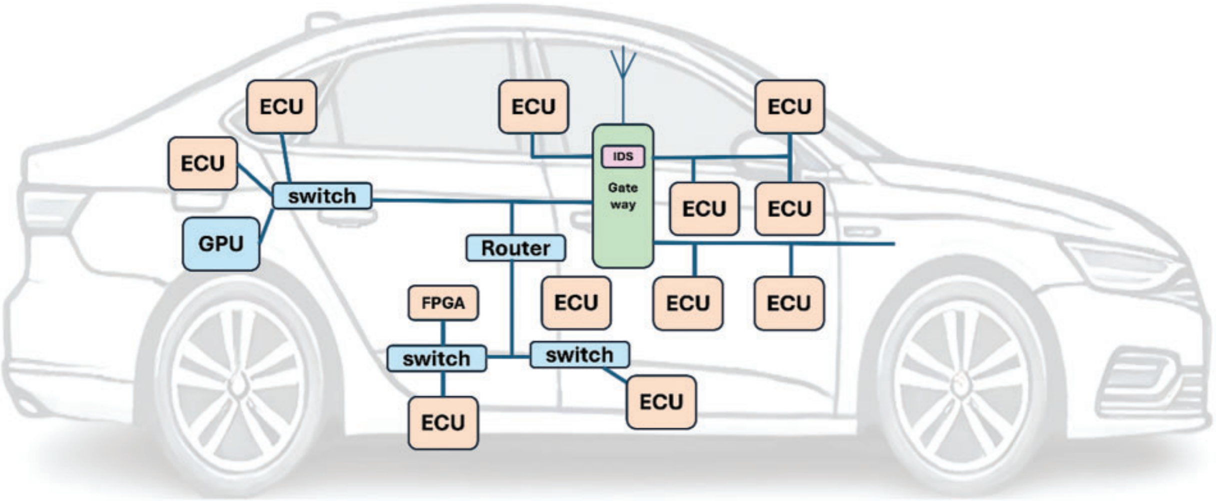

Figure 2: The electronic system structure of the Intelligent and Connected Vehicle from the network

The traditional vehicle network design did not initially consider external cybersecurity threats, resulting in the lack of basic security mechanisms for vehicles, such as authentication, encryption, and access control. With the development of IoV technology, the automobile is no longer a closed individual. The decision-making framework of IoV (see Fig. 3). From it, we can find that with the increasing demand for in-vehicle and external communication, the cybersecurity threats faced by IoV have become more diverse. In recent years, there have been cyberattacks against IoVs, which often cause serious consequences [31,32]. Therefore, it is urgent to explore the network security technology of IVs to improve cybersecurity.

In recent years, with the development of autonomous driving technology, IoV has put forward new requirements for the internal on-board network, such as high bandwidth (to meet the communication requirements of a large amount of data), information security, and low latency (to ensure real-time communication and security). The authors in [21] proposed a hybrid DL approach for detecting cyber-attacks in IoV with LSTM and GRU. Using a car-hacking dataset to demonstrate the robustness of this approach to avoid fatal accidents due to privacy and security issues, a detection accuracy of 99.5% was achieved.

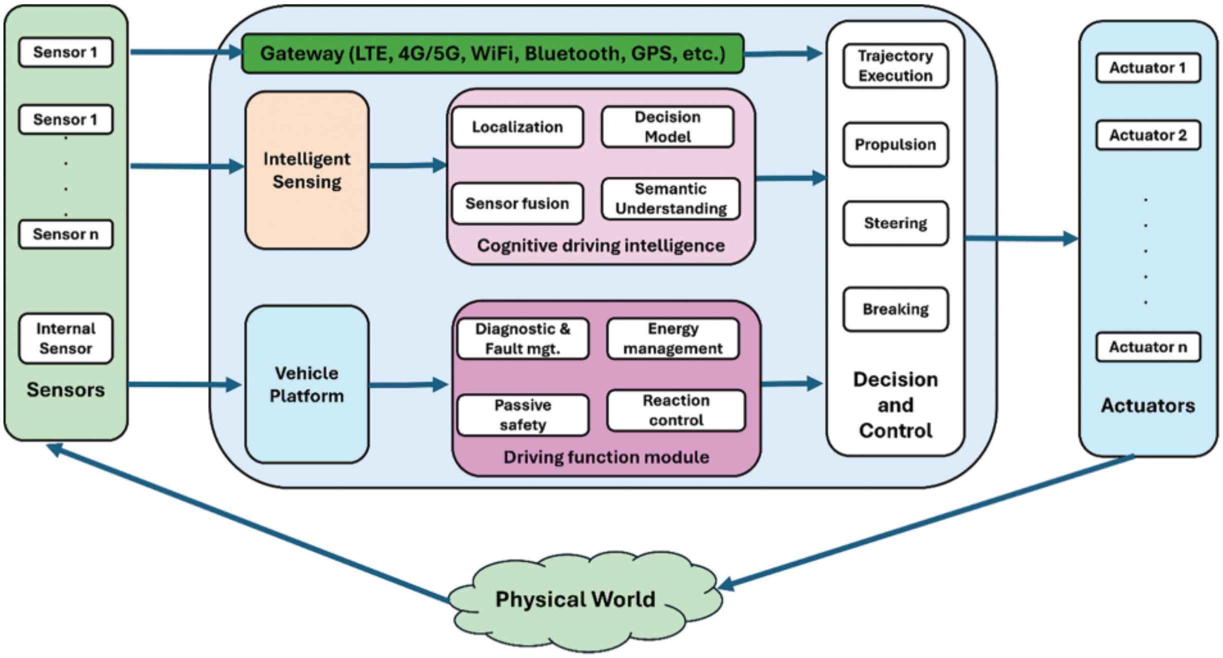

Figure 3: Internet of Vehicles decision-making framework

Alladi et al. [33] developed an AI-based intrusion detection platform for the IoV networks subjected to various cyberattacks on a mobile vehicle. Here, the deep learning models are deployed on multi-access edge computing frameworks rather than the conventional means of cloud setup. Anzer et al. [34] focused on using multilayer perceptions for intrusion detection on the IoV networks and demonstrated its effectiveness in addressing the specific vulnerabilities in V2V communication. The authors in [35] provided a comprehensive means of securing the IoV backbone networks using DL-based network traffic predictions. The article discussed the implications of end-to-end prediction of the network by observing the spatiotemporal features from a real network traffic dataset.

An intruder detection system in the IoV (IDS IoV) is a security measure designed to detect and alert of any unauthorised access or tampering of connected vehicles. These systems utilise a variety of sensors, such as GPS, accelerometers, and RFID readers, along with machine and deep learning algorithms, to analyse data in real-time and identify potential threats. The goal of an IDS in the IoV is to ensure the security and integrity of connected vehicles and protect against cyber threats like malware and hacking attempts. These systems are essential for maintaining the safety and reliability of self-driving and traditional cars connected to the IoV [36].

Vulnerabilities and security requirements for ICV IDS systems aim to protect the IoV from the following attack types [1]. If the research and deployment of in-vehicle network security enhancements are not carried out in time, they will suffer from various malicious attacks due to potential security vulnerabilities. Distributed denial-of-service (DDoS) steals crucial information from the network data packets in the communication using a software package or hardware equipment. A sniffing attack is a process for stealing significant information from the network data packets in communication using a software package or hardware equipment. A Brute Force Attack is a stealing attack using a trial-and-error fashion, especially passwords, login information, and encryption keys. An integrity attack is a type of data-spoiling attack. Here, using malware intruders delete and alter the intended messages or information. A web attack is an application layer attack. The intruders follow various strategies like cross-site scripting, SQL injection, path traversal, and cand local file inclusion to delete, change, or add harmful content to the web pages. Fuzzy attack: The fuzzy attack is one of the most common attacks which CANs can face. Because these attacks arbitrarily inject random messages, increase the complexity of the traffic, and reduce the stability of the IoVs.

DL-based IDS scheme for IoV in [36] is considered to protect the CAN bus in vehicles. The authors considered the VGG architecture and the CAN-intrusion dataset, trained the model on various intrusion patterns, and derived a robust solution to detect malicious attacks. It was shown that a false positive rate of 0.6% was achieved with an overall accuracy of 96%. The work in [8] used CNN to enable data-driven IDS for intelligent IoV. It highlights the analysis performed on roadside units and the link load behaviour for assessing attacks through malware. Further, based on the convergence analysis, it was observed to be a perfect candidate for the ITS in smart cities. The transfer learning-based IDS for IoV presented in [4] used multi-task learning to transfer the knowledge gained from the chosen benchmark datasets. The implementation and investigations performed in this work through CNN promise to provide efficient computational intelligence as a transfer of the acquired knowledge among the datasets.

Yang et al. [11] focused on using the transfer learning technique and the ensemble-based IDS for intrusion detection in IoV in association with CNN. This work experimented with a car hacking dataset and tested the impact of cyber-attack detection in both intra and external vehicular networks. The multi-tiered hybrid IDS for IoV proposed in [37] incorporates a signature-based strategy and an anomaly-based IDS to detect strange attacks over vehicular networks. From the experimentation on a car dataset, the model detects zero-day attacks and computes the average processing time of the data transmission between the vehicles. In [38], cloud-based and local update methods were considered to ensure timely data exchange with the IoV cloud. It employs transfer learning on the pseudo-labelled data, which could find new attacks without needing labelled data. Such timely updates to the IoV cloud enable better and enhanced detection accuracy for the IDS employed to estimate the attacks over IoV. Alferaidi et al. [12] investigated how a distributed Deep CNN-LSTM model can detect intrusion in IoV. They use the Apache Spark framework and the developed model to estimate the abnormal behaviour of the car networks and the associated intrusions. Further, the experimental results show that the model delivers quick convergence with a 99.7 accuracy range.

The leader class and confidence decision ensemble [39] technique is used to detect attacks over IoV networks with an ensemble IDS framework, which was constructed using sophisticated ML models to classify the attacks. The experiments were performed with standard CICIDS2017 and car-hacking datasets, and the authors demonstrated effective intrusion detection over intra and external vehicular networks. The privacy-preserving-based secured framework for IoV [40] incorporates DL and blockchain frameworks to address the privacy, vulnerabilities, verifiability, and data integrity challenges among the involved vehicles in the IoV network. It encompasses a cloud interface with the roadside unit and the cloud server, designed to handle the data and detect intrusion with the support of the blockchain module. Based on the implementation performed over the IoT-Botnet dataset, the developed framework emphasises a better privacy-preservation platform for the IoV network. The developed IDS based on gradient descent in [41] can be efficiently evaluated and validated for use in real vehicles. The experimentation employing the deep learning approach uses gradient descent with momentum and adaptive gain to detect anomaly data so that attacks over vehicles could be addressed. Since they use log-ratio sampling and outlier detection for intrusion detection in IoV [3], they consider the minority classes and imbalance ratio and rescale the samples to learn the metrics. Using the UNSW-NB15 dataset, the authors evaluated the false alarm rates for the attacks over IoV, providing a secure means of in-vehicle communications. The authors in [42] studied the characteristics of malfunctioning IoV-based systems in terms of deployment scenario, with different malware attacks and ensuring user security in the IoV infrastructure.

Machine learning (ML) techniques help detect different cyber-attack types for improving IoV security. The performance of the ML models varies based on the types of attacks. ML models are utilised to design classifier-oriented IDS that can discriminate between cyber-attacks and benign networks through network traffic data analysis. Due to the advancement of ML techniques, automotive manufacturers and researchers have been employing ML-driven IDS in IoV. At the outset, we discuss the pros and cons of several supervised and unsupervised learning techniques in identifying malicious activities. These unsupervised and supervised methods design the IDS with low false reports and robust detection [42]. In addition, the systems adjust fast to the changing malicious behaviour.

Supervised Learning, like Naive Bayes (NB), K-Nearest Neighbour (KNN), Decision Trees (DTs), Support Vector Machines (SVMs), Ensemble Learning (EL) and Random Forest (RF), the advantages and limitations. Different IDS exploited NB techniques for being easy to implement and simple algorithms. It can classify both multi-label and binary classification and the requirement for classification sample is minimal. The accuracy is affected as the method fails to consider interdependencies between features for classification. In KNN, determining the optimal value of K and detecting missing nodes are costly and time-consuming, but it is simple to use. The method provided good accuracy for identifying Remote-to-Local (R2L) and User to Root (U2R) attacks. DTs have the potential to be used in IDS, but computational complexity and bigger storage are some of the concerns of this technique. The benefits of SVM algorithms are less memory usage and high scalability due to their simplicity. It is a challenge to the technique to acquire the classification speed by utilising the optimal kernel function that is applied to isolate data when it is not linearly separable. As no ML technique can be depicted as suitable for all solution types, EL may be best suited for enhancing accuracy by avoiding overfitting and reducing variance. The time complexity increases due to the application of various classifiers in parallel. RF produces more accurate and robust output requires significantly lower inputs and is resistant to overfitting. It does not require the process of feature selection. Since RF constructs numerous DTs, RF may not be suitable in real-time applications having huge datasets.

Unsupervised Learning, e.g., K-Means clustering, does not require labelled data but proves less effective when compared to supervised learning methods in particular identifying known attacks.

The Principal Component Analysis (PCA), employed as a feature reduction or selection technique transforms a huge set of features into a minimal and effective set of variables without losing much information. We discussed some of the state-of-the-art machine-learning techniques used for IDS in the IoV environment. A new ensemble technique dubbed LCCDE (Leader Class and Confidence Decision Ensemble) was presented by Yang et al. [39] to yield optimal performance on all types of attacks in IoV networks. They determined the final prediction classes through the prediction confidence information. They employed three cutting-edge gradient-boosting ML techniques CatBoost, LightGBM, and XGBoost, to devise the ensemble model. Their IDS framework showcased 99.81% and 99.99% F1-scores on the CICIDS2017 and Car-Hacking datasets representing the external vehicular network and intra-vehicle data respectively. Another method called multi-tiered hybrid intrusion detection system (MTH-IDS) was introduced by [37] to identify different types of zero-day and known cyber-attacks on both external-vehicular networks and intra-vehicle. Their technique comprised feature engineering, data pre-processing ML stages and four prime tiers of learners applying different ML classifiers. They used four tree-based supervised classifiers for known attack detection and supervised learning optimisation, a Bayesian optimisation with a tree Parzen estimator (BO-TPE), and a stacking ensemble method exploited.

For zero-day attack identification, cluster labelling (CL) K-Means was utilised as an unsupervised learner and unsupervised learner optimisation, a Bayesian optimisation with Gaussian process (BO-GP) and two biased classifiers were employed. In [43], the authors proposed machine learning methods to classify and cluster the intrusions in vehicular ad hoc networks (VANETs) by SVM and KNN techniques to detect Fuzzy and DoS attacks. Their IDS relied on the time interval between the message request and the response and the offset ratio in the CAN analysis. They used two car-hacking datasets called the "Fuzzy dataset" and the "DoS dataset" provided by the Hacking and Countermeasure Research Lab (HCRL). An intelligent IDS was presented by [44] based on tree-structure-oriented machine learning algorithms. The empirical results demonstrated that their framework can detect different types of cyber-attacks in autonomous vehicle (AV) networks. Their system uses feature selection and ensemble learning approaches and achieves low computational cost and high detection rate.

Injadat et al. [45] devised a new multi-stage optimised ML-based IDS approach that exploited mini-mum training sample size and oversampling techniques. They examined several ML hyper-parameter optimisation methods and their performance enhancement in the framework. They investigated their model's performance using two state-of-the-art datasets (UNSW-NB 2015 and CICIDS 2017). It is challenging to get good performance in the multi-class scenario to detect each attack type rather than only identify the intrusion, which involves binary classification. ML models perform differently for identification in each class, hence it is perplexing to choose one ML model applicable to the prediction of all classes. Chen et al. [46] presented a novel ensemble learning approach dubbed All Predict Wisest Decides (APWD) built on the training ML techniques and testing them individually to predict the performance for all classes. They selected an expert model (i.e., wisest) based on the lowest false detection rate, best accuracy and F1-score for each attack category. Complex connections among divergent nodes and frequent data transmission enhance the complexity of malicious attacks in IoV. Jin et al. [3] introduced an IDS to detect such attacks rapidly and accurately by integrating metric learning, outlier detection, and oversampling. An optimal subset of features was extracted by employing a genetic algorithm and LightGBM was exploited for the classification task.

In [47], the authors applied Artificial Bee Colony optimisation combined with SVM to devise Sec-IoV, a multi-stage technique for the detection of the anomaly of anomalous traffic in vehicle-to-vehicle (V2V) communications in IoV networks. In [48], the authors proposed ML-based probabilistic cross-layer IDS identifying spoofing attacks with comparable accuracy. They introduced a novel metric using Relative Speed, called Position Verification (PVRS), demonstrating a positive impact on the classification outcome. Sharma et al. [49] designed an ML framework by combining plausibility checks and instantiating it with six ML techniques and the results demonstrated the technique's efficacy. Incorporating the plausibility checks for the maximum position attack types improved the recall and precision by 2% and 5%, respectively. Their framework yielded favourable outcomes in being autonomous without human intervention, privacy-preserving compatible with the security credential management system (SCMS), and real-time by a local process. Table 2 describes some of the state-of-the-art ML-based IDS for IoV are listed below.

Table 2: State-of-the-art ML-based IDS for IoV

Ref.	Year	ML methods	Dataset used	Performance
[39]	2022	CatBoost, LightGBM, and XGBoost	CICIDS2017 and Car-Hacking datasets	99.81% and 99.99% F1-scores on the CI-CIDS2017 and Car-Hacking datasets
[37]	2021	DT, RF, ET, XGBoost, BOTPE, BO-GP	CAN-intrusion-dataset and CICIDS2017	99.88% accuracy on the CICIDS2017 dataset
[43]	2018	KNN and SVM	DoS dataset and fuzzy dataset	98.3% accuracy by KNN on the DoS dataset
[44]	2019	Decision tree, Random forest, Extra trees, XG-Boost	CAN-intrusion-dataset and CI CIDS2017 datasets	accuracy of CAN-intrusion and CI-CIDS2017dataset reaches 100% and 99%, respectively.
[45]	2020	KNN and RF with optimizers GA, Bayesian Optimization, PSO and Random Search	CICIDS 2017 and the UNSW-NB 2015 datasets	99% accuracy on both the datasets
[46]	2021	Adaboost, XGBoost and RF	NSL-KDD dataset	Overall accuracy 79.7%
[3]	2021	LightGBM with GA	UNSW-NB15, ROAD, Car-hacking and CAN-intrusion datasets	98.51% accuracy on the UNSW-NB15 dataset
[48]	2020	Bagging, KNN and RF	Simulation of Urban Mobility (SUMO) and the OMNET++/VEINS	K-NN and RF algorithms achieved equal accuracy scores of 91.3%
[49]	2020	SVM, KNN, NB, RF, Boosting and Voting	VeReMi dataset	Ensemble algorithms (AUC = 0.85)

In [10], an IDS for an in-vehicle (IV) network was proposed using convolutional neural networks (CNNs). Electronic control units (ECUs) of IV establish communication with the outside vehicles for information exchange, which can lead a chance to cyber-attacks. The communication protocol, namely, the controller area network (CAN), is vulnerable to these attacks. Therefore, the authors have developed this IDS system based on recurrence plots (RPs) and CNN. Firstly, the sequence of arbitration IDs is converted into images using RPs, then these images are trained, and a model is developed using CNN. The authors tested various attacks in this process, e.g., drop, fuzzy, and insertion attacks. The proposed model was examined on a publicly available and an author's private dataset.

The authors have taken advantage of the ***deep learning (DL)*** model CNN by converting the raw data to RPs, which can provide the temporal relations between IDs inside and outside of vehicles. Also, the computational complexity was reduced by performing a hyperparameter optimisation. Besides, the method is limited due to the need for retraining of CNN when a new arbitrary ID appears in the CAN due to some software updates. It leads to high complexity in time and model. The other disadvantage of this approach is that it can only identify fewer typical intrusions. Nevertheless, the method was limited to addressing the attacks that alter the CAN's data without changing the arbitrary ID.

Alferaidi et al. [12] developed an IDS model using a combined DL model implemented on a spark framework. As CNN is a reliable model that works on high dimensional data features, and long-short-term memory (LSTM) is suitable for handling time-series data, the authors fused these two methods to develop a final model. The advantage of the Apache Spark framework is the capacity to process diverse and large datasets. The proposed method was validated on the NSL-KDD and UNSW GNB15 datasets. Nevertheless, this method requires more data to train the model to achieve state-of-the-art performance.

The authors in [14] demonstrated an IDS model CANintelliIDS to detect IV intrusion. The proposed CANintellilDS is a fusion of CNN and attention-based gated recurrent unit (GRU). The proposed model was examined for single intruders and multi-intruder environments. The system is validated on real-time collected data. The system performs better than many machine learning models and a neural net with five hidden layers. However, the performance is limited to relational aspects and contextual information. They relied on other features without GRU to improve the method's efficacy.

A ConvLSTM-based IDS was proposed in [50]. In the training phase, a federated learning (FL) framework is employed in the client-server mode. Intelligent connected vehicles (ICVs) are the local clients and mobile edge computing is the servers. The authors have also added a proximal policy optimisation (PPO)-based federated client selection (FCS) scheme to minimise the system overhead and improve the framework's accuracy. The experiments are validated on the existing Internet of Vehicles (IoV) and real datasets. The proposed work mainly focuses on IDS in the client-server FL framework. However, to use this model in real time, the model must be tested in a multi-agent system. The authors in [51] proposed an IDS system using CNN and the mosaic pattern-based coding (MPBC) method. As CAN provides time-series data, processing such data for DL models is difficult. Therefore, they have developed a 2D MPBC to convert the 1D data to 2D grid data without losing the temporal characteristics of CAN information. The authors used the data from the Hacking and Countermeasure research lab in South Korea. The data is examined on three types of attacks: Fuzzy, Dos, and Spoofing. On the other hand, the models were trained on each attack type individually. Therefore, the validation of each model must be separate. Such models can only identify the attacks with which they are trained. Also, the proposed method must be trained with the versatility of other crucial/vulnerable attacks.

The authors in [6] designed an IDS system for roadside units (RSUs) in the IoV to fight against the attacks. For this purpose, they have used the attributes extracted from the RSUs to train the CNN model. The proposed model was implemented on the testbed. The main difference between this work and others is that the model was analysed via the link loads of RSUs rather than network nodes. This approach saves many network resources like network bandwidth and IoV memory. However, the problem with this method is that if the length of the attack is large, then CNN's performance may decrease.

A hybrid-DL (HDL) based IDS was proposed in [21]. The authors have clubbed the LSTM and GRU to exploit their advantages as better training time of the LSTM and better performance of GRU, thereby mitigating their adverse results. Before training the model, the authors used a few preprocessing techniques: cleaning, shuffling, data and attribute normalisation. The proposed methods were validated on two datasets: Combined DDoS and car hacking. The main advantage of this method is its lower response time and the shortcoming is its complexity due to the fusion of two schemes (LSTM and GRU).

The authors in [24] have proposed a temporal CNN-based IDS system. First, the 19-bit length arbitrary ID is transformed into the images. Later, temporal and spatial features of these images are fed to CNN for training the model. Because of the global attention mechanism, the residual convolution component assigns more weight to these features. However, the proposed method is a binary classification method. Hence, it cannot address the various types of attacks. Also, if the length of the arbitrary ID increased due to attacks, it would be another problem.

In autonomous vehicles, automotive Ethernet is the next-generation network that replaces CANs for higher throughputs. Jeong et al. [52] proposed an IDS model for the audio-video protocol (AVP) in IoV using a CNN model. A total of six different attack cases have been tested using the proposed model. Though the model performs well, slightly degraded results were observed when the environment changed from indoor to driving. It is one of the frequent issues with most DL models.

The authors in [16] have proposed an IDS system using VGG16 DL model. They have utilised the Hacking and Countermeasure Research Lab (HCRL) dataset for validation and examined various network attacks: denial of service (DoS), Fuzzy, and spoofing gear. The results were compared with the ensemble machine learning (ML) models.

In a recent study [53], an IDS system was developed using ML and DL algorithms. The authors utilised various DL algorithms (recurrent neural networks (RNNs), LSTM, and GRU) to build the models individually. Later, an XGBoost-based feature selection algorithm was used for the feature selection. The proposed model was examined using two datasets, the NSL-KDD and UNSW-NB15. In the case of binary classification, the LSTM-XGBoost combination yielded the best results on the prior dataset (NSL-KDD). Simple-RNN-XGBoost achieved better performance on the later dataset (UNSW-NB15). Similarly, in the case of multiclass classification, the LSTM-XGBoost is the best fit for the NSL-KDD, and GRU-XGBoost was the best model for the UNSW-NB15 dataset. Despite the better performance, the algorithm has to be tested with various cyber-attacks.

The literature shows that DL approaches outperformed the ML methods in designing IDS systems. However, a large quantity of training data is required to implement robust DL methods. Also, almost all the DL models include many layers for performing feature engineering. It needs a lot of resources because of having several parameters. Moreover, many IDS based on DL-proposed hybrid or fused DL algorithms increase computational and timing complexity. One possible solution is employing lightweight DL models or exploiting the transfer-learning-based DL methods.

DEEP TRANSFER LEARNING TECHNIQUES. The existing ML approaches achieved a good performance level for developing IDS systems for the IoV. However, these methods fail to predict new cyber-attacks since the pre-trained model has limited/no knowledge of this attack. The DL models succeeded to some extent in addressing this issue. However, the success of these models depends on the amount and versatility of data used for training the model and the organisation of the different layers.

Transfer learning (TL) is a better alternative to the abovementioned problems. TL is an ML approach where a pre-trained network (trained using different data) is reused for solving other related issues. The main advantage of TL is saving a lot of resources and time in training a model with massive data. The already trained model's knowledge will be shared with a new model for better prediction accuracy of the current task. It is also known as an inductive transfer.

In [11], the authors developed an IDS model for IoV by fusing various existing CNN models: VGG16, VGG19, Xception, Inception, and InceptionResnet. The concatenation and confidence averaging methods were used for this fusion. Also, the hyper-parameter strategies of particle swarm optimisation (PSO) and hyper-parameter optimisation (HPO) were included for tuning the selected CNN models. The developed model is tested on two publicly available datasets, car-hacking, and CICIDS2017. The advantage of this proposed method is that it can handle both intra-vehicle and inter-vehicle cyber-attacks.

Fine-tuning methods utilisation allows learning higher-order features of the data by unveiling the top few layers of the pre-trained models. Besides, the authors have chunked the data samples based on feature size and time stamps. Later, these huge chunks were converted into lots of data to images for training and labelling purposes, which may lead to some data loss [54].

A novel wide and deep TL-based stacked GRU called the WideDeep is proposed for the IDS [55]. The model can be applied for regression and classification based on the input data. Moreover, it has the memorisation capacity of the regression (linear) model and the generalisation strength of the GRU. The hyper-tuned pre-trained networks are tested on the datasets KDDCup and UNSW-NB15. The other feature of this proposed model is employing a novel pre-processing method for converting numerical to categorical pf multi-dimensional data for classification and multivariate time series data for regression. In [56], the authors have built an IDS system based on the TL mechanism. First, the authors considered a pre-trained CNN model and did some fine-tuning in the early layers. Later, the model is trained and validated on the Bot-IoT dataset. Later, they applied another dataset, TON-IoT, to test the model, which was built on another dataset with different attacks. Based on the results, the model was again re-trained by fine-tuning the parameters above the frozen CNN base. This re-training ensures the minimal influence of the new attacks on the prior trained model. Finally, the new model was tested using the attacks from both datasets, which were kept aside from training. The authors mentioned their future work to deploy the proposed model in a real IoT environment.

A dependable IDS system based on TL was proposed in [57]. This model aims to detect any malware attack within any diversified IoT network. The success of the dependable IDS systems relied on the scalability of the features. Therefore, the authors developed a TL-based proposed residual network (P-ResNet) for training the data. The model can classify the attacks: DoS, DDoS, password cracking attack, and scanning. The data was collected from various IoT sensors from different locations. Another significant contribution of the authors is applying a redundancy and correlation analysis to remove redundant data that affects the results. In the future, the authors would like to add optimisation techniques for fine-tuning the network parameters and adding more diverse data for designing a robust model.

An in-vehicle IDS model was proposed using a TL method, namely, LeCun Network (LeNet) in [19]. The data was collected from various resources that contain three types of cyber-attacks. The attacks are flooding, fuzzing, and spoofing. The proposed method was compared with the other ML and DL methods using statistical methods and they proved that the TL approaches outperform all other methods. Though the method is performing well on the considered datasets, there is a need to test the model with more diversified data from intra-vehicles and new cyber-attacks.

In [38], the authors have proposed a novel IDS scheme using the TL approach. The approach has two model updates one online-based cloud and one offline. In the prior update method, the cloud will provide small labelled data for the unlabelled attacks using the pre-classifiers. In the later update, there is partial assistance from the cloud. Hence a local update will be done. Therefore, the proposed model guarantees that the model can independently and locally learn new attacks. The model was verified on the two datasets of the AWID public database.

An IDS scheme was recently proposed to identify zero-day attacks [58]. The proposed approach was based on a TL approach using pre-trained CNN. Besides, the authors also proposed three new datasets derived from the UNSW-NB15 to evaluate the proposed method. The first dataset, the UNSW-NB15-Basic, has normal and four known attacks. The second dataset, the UNSW-NB15-Test+, has normal and five zero-day attacks, and the third dataset, the UNSW-NB15-Test, has normal, known, and zero-day attacks. Albeit the proposed model tested on various attacks, all these were derived from a single source. Therefore, the model's efficiency is limited. Hence, the authors mentioned in their future work that they want to add more diversified data from IoT networks.

An open-source software called IDS-ML was developed for detecting cyber-attacks in IoT communications [59,60]. The authors have developed this model with the help of ensemble learning, TL, and HPO. They used various pre-trained networks like VGG16, 19, Inception, and Xception. The unique contribution of the authors is that the developed software is made open to the public. Hence, others can use it, and new modifications are also possible. Despite the advantages of the TL method, it has some limitations, like negative knowledge transfer. If the utilised pre-trained network has a different input data source when compared with the current task's data, then there is massive scope for negative results.

3 Discussion

This section discusses studies done in the field of IoV, methods used, contributions, limitations, and plans for future studies. The most commonly discussed attacks in previous studies are related to the security mechanism of IoV, and the most often-used algorithm is CNN. The details of some of the related studies considered from the past are discussed below and summarised in Table 3.

Table 3: Details of some of the attacks in IoV

Ref.	Problem	Contribution	Attacks type	Techniques used	Future work
[61]	Attacks IoV	Resolving attacks	Sybil, Masquerading, Wormhole, GPS deception	Digital signatures, Group signatures, Identity-based cryptography	Safe and secure vehicular communication infrastructure
[62]	Security challenges in IoV	Authentication mechanism	Sybil, Masquerading, Wormhole	RSU-based authentication, Pseudonym based authentication	N/A

(Continued)

Table 3 (continued)

Ref.	Problem	Contribution	Attacks type	Techniques used	Future work
[63]	Malicious attacks and limitations of local & weak feature mapping	Spatial-temporal correlation features of in-vehicle communication traffic (STC-IDS)	Intrusion detection	LSTM, CNN	Express realistic unknown attack messages
[64]	Cyber attacks	IVN design	Intrusion detection	Classification, Deep learning and Sequential Techniques	In-Vehicles Networks
[11]	Vulnerabilities and cyber threats	IDS for IoV systems	Cyber	CNN, Learning	An online adaptive model capable of online learning
[1]	Security threats	AI-based IoV IDSs	Denial of Service, DDoS, Sniffing	Federated Learning (FL)	Feature extraction, identification and classification
[10]	Security is-sues for cyber attacks	IDS system Rec-CNN	Denial of Service, Fuzzy, Spoofing-gear, Spoofing-RPM	CNN	Extending the promising results to an IDS
[65]	Intrusion issues in engineering vehicles	Method of motion target	Intrusion detection	CNN	Higher accuracy of classification
[12]	Security issues of IoV	Distributed deep CNN-LSTM	Intrusion detection	CNN-LSTM	Performance and reduction of detection time

Samad et al. [61] have conducted a systematic literature review focused on the security requirements of the IoV, potential attacks, and how to counter them. They consider four types of attacks: Attacks on authentication (Sybil attack, GPS deception attack, Wormhole attack), Availability attacks (Channel Interference Attack, Denial of Service, Distributed Denial of Service Attack), Privacy attacks, and Routing attacks. The authors present some possible countermeasures of the Sybil attack (digital signatures combined with anonymous certificates, group signatures, identity-based cryptography, tamper-proof devices, one-time identity-based aggregate signature, multiple secret sharing), Wormhole attack (digital signature), Channel Interference Attack (hardware-related side channels, visual light, and ultrasonic audio to verify identity and location of the vehicle), Distributed Denial of Service Attack (digital signature, user authentication methods, defining the trustworthiness of a node using group communication and predicting the possible attacks), Privacy attack (Encryption), Routing attacks (IDS, Routing Protocol for Low-Power and Lossy Networks in IoV). The authors highlight the security requirements of IoV, some possible attacks on it, and countermeasures to overcome some of these attacks. Authors do not make deep analyses based on which a reader selects a specific countermeasure for dealing with such attacks and provides a safe and secure vehicular communication infrastructure.

A novel coupled map car-following model in [66] considers cyber-attacks on continuous delay effects. It facilitates improved traffic stability by maintaining traffic flow stability and reducing emissions in the model. As an extension of this, the same authors in [67] incorporated cyber-attacks and continuous delay effects under stable conditions through control theory. The numerical simulations of the model confirm its efficacy for maintaining traffic flow stability and reducing emissions in the model.

Sharma et al. [62] focused on security issues and have presented a model of the IoV system. They discuss security issues, various security attacks, and their countermeasures from an IoV standpoint. In addition, they propose an authentication mechanism for vehicle-to-infrastructure (V2I) communication and an authentication scheme based on RSU-based authentication, Pseudonym authentication and Group-based authentication. This scheme ensures secure communication between two nodes in IoV and prevents malicious nodes from infiltrating the system. In their method, base stations and newly connected vehicles to the IoV network can authenticate each other using public key infrastructure cryptography.

Cheng et al. [63] have discussed security concerns. They propose a novel deep transfer learning-based dependable IDS model for detecting automotive intrusions using in-vehicle communication traffic spatial-temporal correlation features (STC-IDS) based on LSTM and CNN. The model makes use of encoding-detection architecture. Spatial and temporal relations are encoded concurrently in the encoder part. The encoded data is sent to the detector, which generates powerful spatial-temporal attention features and enables anomaly classification. Single-frame and multi-frame models, in particular, are built to provide distinct advantages. The model has been trained to get the best performance using automatic hyper-parameter selection based on Bayesian optimisation. The model outperforms several existing approaches. The authors include effective attribute selection, best suited to identify normal and attack scenarios for a small amount of labelled data, designing a dependable deep transfer learning-based ResNet model, and evaluating real-world data. The authors have done an extensive analysis and performance evaluation that show that their model is robust, more efficient, and has demonstrated better performance, ensuring dependability. There is still much room for improvement, particularly in detecting unknown attacks. In the future, the authors plan to study how to express realistic unknown attack messages to improve model robustness and generalisation capabilities.

Wu et al. [68] investigated the security risks of in-vehicle networks (IVNs) and state that all previous IVN designs lack cybersecurity considerations. They used classification, deep learning, and sequential techniques to introduce an IVN environment and present the constraints and characteristics of an IDS design for IVNs. The external interface for vehicle attacks was creatively analysed on three layers, and the vulnerabilities of each layer were discussed. The characteristic parameters available for IVN IDS design at each level (bus, message, data flow, and functional) were examined. Based on implementation techniques, cutting-edge intrusion detection methods for IVNs were classified into four types. Furthermore, advanced intrusion detection solutions for IVNs were thoroughly studied and proposed for future work.

The paper in [69] investigated the intrusion detection in IoVs problem and proposes an intrusion detection strategy based on Road Side Unit (RSU) anomalous traffic. The authors considered

OnBoard Unit (OBU) network resources and designed an intrusion detection mechanism based on RSU link loads. CNN-based architecture is developed to extract the spatiotemporal feature of link loads. It uses a traditional CNN architecture and a redundant error term in the output layer to achieve the convergence of the deep architecture for intrusion detection. The proposed method provides a theoretical analysis of the proposed deep architecture in convergence using a Bayesian hierarchical model. Finally, the proposed method was tested and evaluated for accuracy by implementing it on the test bed.

Yang et al. focused on cyber threats to IoV systems [11]. They proposed a transfer learning and ensemble learning-based intrusion detection framework (IDS) that detects various at-tack types in IoV systems to protect connected vehicles from cyber-attacks. Authors use CNN, transfer learning, ensemble learning models, and hyper-parameter optimisation techniques to build the framework. The experimental results show that the proposed IDS framework can effectively identify attack types with higher F1-scores of 100% and 99.925% on the two benchmark datasets than other compared state-of-the-art methods. The higher performance of the proposed models when compared with other state-of-the-art IDSs supports the reasons for using CNN, transfer learning, and hyper-parameter optimisation techniques. Also, the results from model testing on a vehicle-level machine demonstrate the feasibility of the proposed IDS in real-time vehicle networks. The authors plan to expand the framework in future work by creating an online adaptive model capable of online learning and addressing concept drift in time-series vehicle network data. Karie et al. [1] have focused on AI-based IoV IDSs, security threats, and attacks the IoV network has faced. They concentrate on the current anomaly-based IDS for IoV and discuss the use of AI technology in IDS, unresolved issues, and future research directions. Among the discussed machine learning techniques (KNN, SVM, RF, DT, ET, XGBoost, ANN, DNN, CNN, RNN, DBN & GAN, Federated Learning), Federated Learning is supposed to be one of the best techniques to be considered for designing IoV IDS. Desta et al. [10] focused on security measures for Controller Area Network (CAN) protocol that provides no authentication or encryption to prevent the consequences of cyberattacks. They use CNN-based IDS, where Rec-CNN is a CNN trained on recurrence images generated from encoded labels of CAN frame arbitration IDs. The proposed method is tested on a publicly available dataset and public passenger vehicles with DoS, fuzzy, spoofing-gear, and spoofing-RPM attacks, resulting in an accuracy of 0.999. In addition, we have tested the method on our target vehicle. When the attack frequency is once every 10 milliseconds, this method can classify simulated attacks with an accuracy of 0.999. The proposed method does not outperform the Inception-ResNet-based method in all cases.

The comparison of the performance of the two methods shows that the Inception-ResNet-based method works best when the attack frequency is high, and the proposed method outperforms the Inception-ResNet-based significantly when there are only a few attacks in a window. The proposed method has some disadvantages. Firstly, model retraining is required when the data used for training is significantly different from the data collected for inference. Another shortcoming of the proposed method is that it can only detect attacks that disturb the CAN packet flow's normal sequence and leave undetected attacks like impersonation, which manipulate the CAN frame's data without affecting the arbitration ID. The method could be extended to an IDS that can detect such attacks.

Lampe et al. [65] have proposed a two-step deep-learning method to detect engineering vehicles operating under high-power transmission lines. The intrusion detection algorithm is used in the first step to identify the potential target area. Then, the output is fed into a trained deep convolution neural network classifier. By combining the intrusion detection method with CNN, the invasion of engineering vehicles under high-power transmission lines can be detected with 97.2% accuracy.

Alferaidi et al. [12] focused on the practical application of emerging technologies in IoV. Because of its uniqueness, the car does not value network security highly enough. IoVs' security has increasingly become a barrier to their adoption. Due to the rapid changes in the structure of the IoV, the large data flow, and the complex and diverse forms of intrusion, traditional detection methods cannot ensure their accuracy and real-time requirements and cannot be applied directly to the IoV. To solve these problems, Alferaidi and his team [14] proposed a new AA-distributed combined deep-learning intrusion detection method. Their method combines deep-learning convolutional neural network (CNN) and extended short-term memory (LSTM) networks to extract features and data for detecting car network intrusion and irregular behaviour from large-scale car network data traffic. The experimental results show that compared to other existing models (CNNGLSTM, SVM, RNN, CNN, and LSTM algorithm), the CNN-LSTM algorithm using the Spark framework can reach 20 in the shortest time possible, with an accuracy rate of up to 99.7%. Among the advantages of the proposed solution are the reduced training and test time, improved detection rate, and the fact that it meets the real-time requirements of intrusion detection and satisfies the actual needs of the IoV for intrusion detection. This study also has some limitations. The method could be improved in terms of reduction of detection time, conducting intrusion detection on distributed platforms, and exploring suitable distributed deep learning algorithms to meet the needs of intrusion detection for car network information security.

As can be seen from Table 3, in which the studies discussed in this section are presented in a systematised form, most of them are focused on Intrusion detection attacks [12,63,65]. The conducted study shows that the most suitable techniques for dealing with this attack type are CNN [63,65], LSTM [63] and the combined CNN-LSTM [12], followed by the Classification Technique, Deep learning Technique and Sequential Technique [64]. Four studies focus on Denial-of-Service attacks [2,10,61,62] as all of them use different techniques-Federated Learning [1], CNN [10], RSU-based authentication [62], Pseudonym-based authentication [62], Group-based authentication [62]. The Sybil attack is considered in two studies [64,67], and for dealing with them are used digital signatures and group signatures, Identity-based cryptography, Tamper-proof devices, One-time identity-based aggregate signature, and multiple secret sharing [61], RSU based authentication, Pseudonym based authentication, Group based authentication [62].

Two studies focused on Channel interference attacks [61,62] and proposed solutions based on hardware-related side channels [61], RSU-based authentication [62], Pseudonym-based authentication [62], Group based authentication [62]. Digital signature [61], user authentication methods [61], and Federated Learning [1] are used for dealing with Distributed Denial of Service attacks in two studies [2,64]. Wormhole attacks are considered in two studies [61,62], and to overcome them different methods are used-digital signature [64], RSU-based authentication [62], Pseudonym based authentication [62], Group-based authentication [62]. For dealing with Fuzzy Attacks [2,10] researchers proposed Federated Learning [1] and CNN [10] to be used. Each one of the remaining attack types discussed is the subject of a study. Researchers propose several methods to deal with some of them-Privacy attacks (Encryption [61]), Routing attacks (Intrusion Detection Systems and Routing Protocol for Low-Power and Lossy Networks in IoV [61]), Data authenticity attacks (RSU based authentication, Pseudonym based authentication and Group based authentication [62]), Cyber-attacks (CNN, Transfer Learning, Ensemble Learning Models and Hyper-Parameter Optimization techniques [11]), Sniffing Attack (Federated Learning [1]), Brute Force Attack (Federated Learning [1]), Integrity Attack (Federated Learning [1]), Web Attack (Federated Learning [1]), Malware Attack (Federated Learning [1]), Spoofing-gear (CNN [12]), Spoofing-RPM attacks (CNN [10]).

Most of the discussed techniques are suitable for dealing with more than one attack type. The most widely used is the CNN method, suitable for dealing with 6 attack types- Intrusion detection attacks [63,65,69], Denial-of-Service attacks [10], Fuzzy attacks [10], Cyber-attacks [11], Spoofing-gear [10], Spoofing-RPM attacks [10]. Federated Learning is also applied to deal with a large number of attacks, among which Denial-of-Service attacks [1], Distributed Denial-of-Service attacks [1], Fuzzy attacks [1], Sniffing attacks [1], Brute Force attacks [1], Integrity attack [1], Web attack [1], Malware attack [1]. Different types of authentications (RSU-based authentication, Pseudonym-based authentication, Group-based authentication) are suitable for dealing with Denial-of-Service attacks, Sybil attacks, Channel interference attacks, Wormhole attacks, and Data authenticity attacks [61]. Studies have shown that Digital signatures can handle Sybil attacks [61], Distributed Denial-of-Service attacks [61], and Worm- hole attacks [61]. The rest of the methods discussed are indicated as being suitable for dealing with only one type of attack-Identity-based cryptography (Sybil attack [61]), Tamper-proof devices (Sybil attack [44]), One-time identity- based aggregate signature (Sybil attack [61]), Multiple secret sharing (Sybil attack [61]), Hardware-related side channels (Channel interference attack [61]), User authentication methods (Distributed Denial-of-Service attack [61]), Encryption (Privacy attacks [61]), IDS (Routing attack [64]), Routing Protocol for Low-Power and Lossy Networks in IoV (Routing attacks [61], Transfer Learning (Cyber-attacks [11]), Ensemble Learning Models (Cyber-attacks [11]), Hyper-Parameter Optimization techniques (Cyber-attacks [11]), LSTM (Intrusion detection attacks [68]), CNN-LSTM (Intrusion detection attacks [12]), Classification Technique (Intrusion detection attacks [64]), Deep learning Technique (Intrusion detection attacks [64]) and Sequential Technique (Intrusion detection attacks ([64]).

4 Open Research Challenges

4.1 How to Reduce the Deployment Cost of IDS-IoV

As a large-scale commodity, how to reduce its production cost is a significant factor for automobile manufacturers to consider. Therefore, one of the challenges faced at present and for a long time to come is how to reduce the deployment cost of IDS-IoV systems. Therefore, for intrusion detection technology based on deep transfer learning, how to further reduce its consumption of computing performance and storage resources is one of the key research directions in the future.

To reduce costs, some current work is based on statistical methods and deployed at the vehicle network data link layer. For example, Wu et al. proposed a sliding window method based on information entropy [68]. In the reference [69], Jin et al. proposed a method based on multi-feature recognition to achieve lightweight and low-cost intrusion detection in-vehicle networks through multi-feature recognition. In general, deploying intrusion detection at the data link layer or even the physical layer to provide a native security mechanism for the in-vehicle network is the overall path to achieve low-cost and real-time security enhancement.

4.2 How to Reduce the Response Time of Intrusion Detection

Considering that cyber-attacks against intelligent vehicles will not only bring threats to information fields, such as information leakage and data theft but also may cause serious personal injury to passengers and roadside personnel due to malicious control of vehicles. Therefore, the IDS-IoV based on deep transfer learning should consider not only the detection accuracy, and false alarm rate but also focus on the detection response time of attacks. In this way, cyber-security protection actions can be taken after the intrusion attack as soon as possible. Therefore, it is a research direction in the future to implement intrusion detection algorithms by using hardware methods such as deep learning processing units (DPU), application-specific integrated circuits (ASIC), FPGA, etc.

The time consumption caused by the computational complexity of classic machine learning methods is one of the factors affecting the reduction of intrusion detection response time. Therefore, the existing work in this area mainly focuses on three aspects-lightweight DTL model design, combining statistics and machine learning, and sinking the intrusion detection technology to the physical layer to achieve a more real-time detection response.

4.3 The Security Requirements of Next-Generation in-Vehicle Networks

The requirements for in-vehicle network bandwidth of intelligent network-connected vehicles are constantly improving. The existing in-vehicle network standard CAN network is increasingly unable to meet the needs of intelligent network-connected vehicles. Ethernet TSN is expected to become the next-generation vehicle network standard. Therefore, the research on intrusion detection will be increasingly vital for designing the network security enhancement mechanisms of vehicle Ethernet TSN. Meanwhile, for the heterogeneous in-vehicle network environment, how to take full advantage of the characteristics of the deep transfer learning model to extract network data is one of the research challenges in the future.

To ensure network security, TSN defines the 802.1Qci protocol to block malicious devices or attacks like DDoS. Currently, there is little research on TSN security, and the enhancement of protocols, algorithms, and encryption mechanisms to ensure network security. As a potential standard for a new generation of in-vehicle networks, TSN can consider functional safety and network security issues during the design and completion processes. In the current research, for the functional safety and network security of TSN, reference [70] discussed the key management, frame replication and elimination, and virtual local area network (VLAN) segmentation); To achieve end-to-end security in TSN, reference [71] proposed a centrally configured network mechanism that combines TSN flow configuration with Security Group Tags (SGT).

5 Future Directions

5.1 Intrusion Detection Technology for Automotive Ethernet

With the development of information and communication technology and the improvement of intelligent driving technology, in-vehicle networks and automotive electronic systems are becoming increasingly complex and often handle large data loads to meet their multi-clock intelligence requirements [72,73]. Automotive Ethernet is expected to meet the requirements of next-generation in-vehicle networks. Automotive Ethernet has better security measurements than CAN networks, e.g., it can be protected using encryption technologies such as IPsec and MACsec. However, these security mechanisms only prevent spoofed messages and man-in-the-middle attacks against unauthenticated devices. However, we believe that it is not enough to protect the communication channels of the in-vehicle network because the risk of authenticated ECUs being exploited throughout the vehicle life cycle remains. Therefore, we believe automotive Ethernet still requires other security mechanisms, such as intrusion detection and firewall policies. Although there are a lot of studies on CAN network intrusion detection technology, the research on vehicle Ethernet intrusion detection technology is still relatively lacking. However, it has been conducted on attacks that can be executed on automotive Ethernet. For example, in [74], Nie et al. demonstrated the use of automotive Ethernet to control vehicles, which shows that attacks against automotive Ethernet exist. There are also a few reports of attacks on SOME/IP, a standard protocol in automotive Ethernet. Similarly, there is very little research on automotive Ethernet IDS. Therefore, this part will become the key research direction in the field of vehicle network security in the future. Considering the increased performance and network bandwidth of automotive ECUs, Deep Transfer Learning techniques will play a more significant role in IDS development [74–76].

5.2 Automotive Operating Systems Will Provide More Support for In-Vehicle Cybersecurity

The cybersecurity of IoV is becoming more systematic due to the development of networked and automated vehicles. Automotive operating systems are a significant part of the automotive software ecosystem. In the field of safe vehicle control operating systems, due to the high requirements of automotive functional safety levels, MCU-based high-real-time and high-deterministic operating systems (such as OSEK/VDX OS) are still widely used, and these systems are usually bundled with the AUTOSAR CP platform. Today, the microkernel-based RTOS real-time system has products that support the ASIL-D functional safety level and will play an increasingly important role in safe vehicle control. In terms of vehicle network intrusion detection, the vehicle operating system will play greater key support, such as providing partition isolation, therefore, the integration of vehicle network intrusion detection technology into the mainstream automotive operating system in the form of middleware will become the focus of research in the future, of which AUTOSAR is currently the most common and commonly used middleware solution.

AUTOSAR already incorporates various IT security applications, e.g., to secure in-vehicle communication or protect confidential data. However, Classic and Adaptive AUTOSAR offer partly identical and partly different security applications due to their different architectures. Therefore, the security enhancement of AUTOSAR will also be a long-term dynamic development process.

5.3 Development of In-Vehicle Network Security Simulation Test Platform

In-vehicle cybersecurity enhancement technology needs extensive testing to meet commercial requirements before it can be truly commercialised. Using a real intrusion attack environment to optimise intrusion detection algorithms is too time-consuming and costly. Open road testing is still restricted by regulations, making it difficult to reproduce extreme attack conditions and scenarios, and there are hidden dangers in test security. Therefore, the simulation test platform suitable for vehicle network security will be more widely valued by the industry, similar to the autonomous driving simulation platform (Udacity, Car-Sim, etc.), about 90% of the future intrusion detection algorithm test will be completed by the simulation platform, 9% will be completed in the test field, and 1% will be completed through the actual environment. The vehicle network security simulation test platform must have several core capabilities: realistic restoration of attack scenarios, efficient use of road acquisition data to generate simulation attack scenarios, restoration of vehicle network data flow, etc., so that the simulation test meets the closed-loop conditions for verification of vehicle network intrusion detection algorithms. Today, technology companies, car companies, autonomous driving solution providers, simulation software companies, universities scientific research institutions, etc., are actively engaged in the virtual simulation platforms construction.

The current udacity vehicle simulator is a simulation platform to simulate the autonomous driving environment. Although its dynamic model is poor, its configuration requirements are low, and it is convenient for experiments. Therefore, it can be used as a potential vehicle network security verification simulation platform. Considering the complexity of the vehicle network IDS, the current focus is more on the design of the data set. Lampe, from the Technical University of Denmark, has been working on the development of open-source data sets for in-vehicle network IDS testing [65].

In [77], a state-of-the-art dataset for intrusion detection called the Car-Hacking dataset is proposed. Another widely used intrusion detection dataset is provided by vehicular network security researchers from South Korea in [78].

6 Conclusion

The landscape of automobile security in the era of 5 G/B5 G presents a complex interplay of design metrics such as cost, performance, safety, and reliability. The IoV stands out as a technology with immense potential, offering a range of functionalities from online communication services to accident prevention. However, with these benefits come significant cybersecurity challenges, necessitating robust IDS tailored for IoV environments. This article has provided a thorough survey of IDS-IoV, outlining its features, concepts, and the array of security attacks and threats facing IoV systems. Through an extensive review of research, we have explored various machine learning, deep learning, and transfer learning strategies employed in IDS-IoV, focusing on the recent advancements in DTL models for anomaly detection. Our evaluation criteria encompassed the ability to transfer knowledge, detection rate, accurate analysis of complex data, and stability, offering insights into the strengths and limitations of DTL models. Moreover, we have discussed the advantages and open challenges for future research in this domain, emphasising the need for cost-effective solutions and efficient intrusion response mechanisms. The key findings of this work serve as a foundational resource for researchers aiming to delve deeper into IDS-IoV, guiding them toward innovative approaches for enhancing the security and resilience of IoV systems. By leveraging state-of-the-art deep learning techniques and addressing emerging threats, we can pave the way for a safer and more reliable IoV ecosystem, ensuring the seamless integration of technology and transportation.

The obtained results allow for studying the applicability of IoV for real-time monitoring and operation of vehicles to enhance cost-effectiveness in various organisations, incl. higher education institutions. In addition, the study of the advantages and limitations of machine learning and Deep Transfer Learning techniques is beneficial for the planned future studies of their application in other fields, such as smart education, smart learning, and learning analytics, in particular and in general, in creating intelligent educational environments.

Acknowledgement: No specific acknowledgement.

Funding Statement: This paper is financed by the European Union-NextGenerationEU, through the National Recovery and Resilience Plan of the Republic of Bulgaria, Project No. BG-RRP-2.004-0001-C01.

Author Contributions: The authors confirm their contribution to the paper as follows: study conception and design: Wufei Wu, Javad Hassannataj Joloudari; data collection: Senthil Kumar Jagatheesaperumal, Kandala N. V. P. S. Rajesh; analysis and interpretation of results: Silvia Gaftandzhieva, Sadiq Hussain, Rahimullah Rabih; draft manuscript preparation: Najibullah Haqjoo, Mobeen Nazar, Hamed Vahdat-Nejad, Rositsa Doneva. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: All data generated or analysed during this study are included in this published article.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] N. M. Karie, N. M. Sahri, and P. Haskell-Dowland, “IoT threat detection advances, challenges and future directions,” in *2020 Workshop on Emerg. Technol. Secur. in IoT (ETSecIoT)*, IEEE, 2020, pp. 22–29.

[2] D. Man, F. Zeng, J. Lv, S. Xuan, W. Yang and M. Guizani, “AI-based intrusion detection for intelligence internet of vehicles,” *IEEE Consum. Electron. Mag.*, vol. 12, no. 1, pp. 109–116, 2021. doi: 10.1109/MCE.2021.3137790.

[3] F. Jin, M. Chen, W. Zhang, Y. Yuan, and S. Wang, “Intrusion detection on internet of vehicles via combining log-ratio oversampling, outlier detection and metric learning,” *Inf. Sci.*, vol. 579, pp. 814–831, 2021. doi: 10.1016/j.ins.2021.08.010.

[4] Y. Otoum, Y. Wan, and A. Nayak, “Transfer learning-driven intrusion detection for Internet of Vehicles (IoV),” in *2022 Int. Wireless Commun. Mobile Comput. (IWCMC)*, IEEE, 2022, pp. 342–347.

[5] M. Jeihani *et al.*, “Investigating the effect of Connected Vehicles (CV) route guidance on mobility and equity,” 2023. Accessed: Jan. 25, 2024 [Online]. Available: https://rosap.ntl.bts.gov/view/dot/60931

[6] L. Nie, Z. Ning, X. Wang, X. Hu, J. Cheng and Y. Li, “Data-driven intrusion detection for intelligent internet of vehicles: A deep convolutional neural network-based method,” *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2219–2230, 2020. doi: 10.1109/TNSE.2020.2990984.

[7] D. Wang *et al.*, “Stop-and-Wait: Discover aggregation effect based on private car trajectory data,” *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 10, pp. 3623–3633, 2018. doi: 10.1109/TITS.2018.2878253.

[8] S. Xu, Y. Qian, and R. Q. Hu, “Data-driven edge intelligence for robust network anomaly detection,” *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 3, pp. 1481–1492, 2019. doi: 10.1109/TNSE.2019.2936466.

[9] C. Zhai and W. Wu, “Designing continuous delay feedback control for lattice hydrodynamic model under cyber-attacks and connected vehicle environment,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 95, no. 7, pp. 105667, 2021. doi: 10.1016/j.cnsns.2020.105667.

[10] A. K. Desta, S. Ohira, I. Arai, and K. Fujikawa, “Rec-CNN: In-vehicle networks intrusion detection using convolutional neural networks trained on recurrence plots,” *Veh. Commun.*, vol. 35, pp. 100470, 2022. doi: 10.1016/j.vehcom.2022.100470.

[11] L. Yang and A. Shami, “A transfer learning and optimized CNN based intrusion detection system for internet of vehicles,” in *ICC 2022-IEEE Int. Conf. Commun.*, Seoul, Republic of Korea, 2022, pp. 2774–2779.

[12] A. Alferaidi *et al.*, “Distributed deep CNN-LSTM model for intrusion detection method in IoT-based vehicles,” *Math. Probl. Eng.*, vol. 2022, no. 1, pp. 3424819, 2022. doi: 10.1155/2022/3424819.

[13] A. Oseni *et al.*, “An explainable deep learning framework for resilient intrusion detection in IoT-enabled transportation networks,” *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 1, pp. 1000–1014, 2022. doi: 10.1109/TITS.2022.3188671.

[14] A. R. Javed, S. Ur Rehman, M. U. Khan, M. Alazab, and T. Reddy, “CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU,” *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1456–1466, 2021. doi: 10.1109/TNSE.2021.3059881.

[15] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon and D. Gan, “Cloud-based cyber-physical intrusion detection for vehicles using deep learning,” *IEEE Access*, vol. 6, pp. 3491–3508, 2017. doi: 10.1109/ACCESS.2017.2782159.

[16] H. -C. Lin, P. Wang, K. -M. Chao, W. -H. Lin, and J. -H. Chen, “Using deep learning networks to identify cyber attacks on intrusion detection for in-vehicle networks,” *Electronics*, vol. 11, no. 14, pp. 2180, 2022. doi: 10.3390/electronics11142180.

[17] B. Lampe and W. Meng, “A survey of deep learning-based intrusion detection in automotive applications,” *Expert. Syst. Appl.*, vol. 221, pp. 119771, 2023. doi: 10.1016/j.eswa.2023.119771.

[18] F. Liu, Z. Ye, and L. Wang, "Deep transfer learning-based vehicle classification by asphalt pavement vibration," *Constr. Build. Mater.*, vol. 342, no. 2, pp. 127997, 2022. doi: 10.1016/j.conbuildmat.2022.127997.

[19] S. T. Mehedi, A. Anwar, Z. Rahman, and K. Ahmed, "Deep transfer learning based intrusion detection system for electric vehicular networks," *Sensors*, vol. 21, no. 14, pp. 4736, 2021. doi: 10.3390/s21144736.

[20] T. H. H. Aldhyani and H. Alkahtani, "Attacks to automatous vehicles: A deep learning algorithm for cybersecurity," *Sensors*, vol. 22, no. 1, pp. 360, 2022. doi: 10.3390/s22010360.

[21] S. Ullah *et al.*, "HDL-IDS: A hybrid deep learning architecture for intrusion detection in the Internet of Vehicles," *Sensors*, vol. 22, no. 4, pp. 1340, 2022. doi: 10.3390/s22041340.

[22] S. Wang, J. Wu, S. Zhang, and K. Wang, "SSDS: A smart software-defined security mechanism for vehicle-to-grid using transfer learning," *IEEE Access*, vol. 6, pp. 63967–63975, 2018. doi: 10.1109/ACCESS.2018.2870955.

[23] P. Cheng, K. Xu, S. Li, and M. Han, "TCAN-IDS: Intrusion detection system for internet of vehicle using temporal convolutional attention network," *Symmetry*, vol. 14, no. 2, pp. 310, 2022. doi: 10.3390/sym14020310.

[24] C. Foreman, M. Keen, M. Petrella, and S. Plotnick, *FHWA research and technology evaluation TechBrief: Truck platooning*. USA: Federal Highway Administration, Research and Technology, 2021.

[25] M. J. N. Mahi *et al.*, "A review on VANET research: Perspective of recent emerging technologies," *IEEE Access*, vol. 10, no. 2, pp. 65760–65783, 2022. doi: 10.1109/ACCESS.2022.3183605.

[26] C. R. Storck and F. Duarte-Figueiredo, "A survey of 5G technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by internet of vehicles," *IEEE Access*, vol. 8, pp. 117593–117614, 2020. doi: 10.1109/ACCESS.2020.3004779.

[27] E. S. Torres, S. Sriramula, D. Celeita, and G. Ramos, "Reliability model and sensitivity analysis for electrical/electronic/programmable electronic safety-related systems," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 3422–3430, 2020.

[28] R. Changalvala and H. Malik, "LiDAR data integrity verification for autonomous vehicle," *IEEE Access*, vol. 7, pp. 138018–138031, 2019. doi: 10.1109/ACCESS.2019.2943207.

[29] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, "Attacks on self-driving cars and their countermeasures: A survey," *IEEE Access*, vol. 8, pp. 207308–207342, 2020. doi: 10.1109/ACCESS.2020.3037705.

[30] W. Wu, R. Kurachi, G. Zeng, Y. Wang, H. Takada and K. Li, "Intelligent connected vehicles," in *Cybersecurity and High-Performance Computing Environments*, 1st edition. New York: Chapman and Hall/CRC, 2022, pp. 285–308.

[31] Z. Khan, M. Chowdhury, M. Islam, C. -Y. Huang, and M. Rahman, "In-vehicle false information attack detection and mitigation framework using machine learning and software defined networking," arXiv preprint arXiv:1906.10203, 2019.

[32] J. M. Qurashi, K. Jambi, F. Alsolami, F. E. Eassa, M. Khemakhem and A. Basuhail, "Resilient countermeasures against Cyber-Attacks on Self-Driving car architecture," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 11, pp. 11514–11543, 2023. doi: 10.1109/TITS.2023.3288192.

[33] T. Alladi, V. Kohli, V. Chamola, F. R. Yu, and M. Guizani, "Artificial intelligence (AI)-empowered intrusion detection architecture for the internet of vehicles," *IEEE Wirel. Commun.*, vol. 28, no. 3, pp. 144–149, 2021. doi: 10.1109/MWC.001.2000428.

[34] A. Anzer and M. Elhadef, "A multilayer perceptron-based distributed intrusion detection system for Internet of Vehicles," in *2018 IEEE 4th Int. Conf. Collaborat. and Int. Comput. (CIC)*, Philadelphia, PA, USA, 2018, pp. 438–445.

[35] X. Wang *et al.*, "Deep learning-based network traffic prediction for secure backbone networks in internet of vehicles," *ACM Trans. Internet Technol.*, vol. 22, no. 4, pp. 1–20, 2022. doi: 10.1145/3433548.

[36] I. Ahmed, G. Jeon, and A. Ahmad, "Deep learning-based intrusion detection system for internet of vehicles," *IEEE Consum. Electron. Mag.*, vol. 12, no. 1, pp. 117–123, 2021. doi: 10.1109/MCE.2021.3139170.

[37] L. Yang, A. Moubayed, and A. Shami, "MTH-IDS: A multitiered hybrid intrusion detection system for internet of vehicles," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 616–632, 2021. doi: 10.1109/JIOT.2021.3084796.

[38] X. Li, Z. Hu, M. Xu, Y. Wang, and J. Ma, "Transfer learning based intrusion detection scheme for Internet of Vehicles," *Inf. Sci.*, vol. 547, no. 14, pp. 119–135, 2021. doi: 10.1016/j.ins.2020.05.130.

[39] L. Yang, A. Shami, G. Stevens, and S. de Rusett, "LCCDE: A decision-based ensemble framework for intrusion detection in the Internet of Vehicles," in *GLOBECOM, 2022-2022 IEEE Global Commun. Conf.*, Rio de Janeiro, Brazil, 2022, pp. 3545–3550.

[40] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, and N. Kumar, "P2SF-IoV: A privacy-preservation-based secured framework for Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 11, pp. 22571–22582, 2021. doi: 10.1109/TITS.2021.3102581.

[41] J. Zhang, F. Li, H. Zhang, R. Li, and Y. Li, "Intrusion detection system using deep learning for in-vehicle security," *Ad Hoc Netw.*, vol. 95, no. 11, pp. 101974, 2019. doi: 10.1016/j.adhoc.2019.101974.

[42] M. S. Botla, J. B. S. Melam, R. S. P. Pedapati, S. Mookherji, V. Odelu and R. Prasath, "Comparative study of HDL algorithms for intrusion detection system in Internet of Vehicles," *Crypt. EPrint Archive*, vol. 2022, Article 7000, 2022.

[43] A. Alshammari, M. A. Zohdy, D. Debnath, and G. Corser, "Classification approach for intrusion detection in vehicle systems," *Wirel. Eng. Technol.*, vol. 9, no. 4, pp. 79–94, 2018. doi: 10.4236/wet.2018.94007.

[44] L. Yang, A. Moubayed, I. Hamieh, and A. Shami, "Tree-based intelligent intrusion detection system in internet of vehicles," in *2019 IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, 2019, pp. 1–6.

[45] M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, "Multi-stage optimized machine learning framework for network intrusion detection," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 2, pp. 1803–1816, 2020. doi: 10.1109/TNSM.2020.3014929.

[46] Z. Chen, M. Simsek, B. Kantarci, and P. Djukic, "All predict wisest decides: A novel ensemble method to detect intrusive traffic in iot networks," in *2021 IEEE Global Commun. Conf. (GLOBECOM)*, Madrid, Spain, 2021, pp. 1–6.

[47] S. Garg, K. Kaur, S. Batra, G. Kaddoum, N. Kumar and A. Boukerche, "A multi-stage anomaly detection scheme for augmenting the security in IoT-enabled applications," *Future Gener. Comput. Syst.*, vol. 104, no. 5, pp. 105–118, 2020. doi: 10.1016/j.future.2019.09.038.

[48] D. Kosmanos *et al.*, "A novel intrusion detection system against spoofing attacks in connected electric vehicles," *Array*, vol. 5, no. 1, pp. 100013, 2020. doi: 10.1016/j.array.2019.100013.

[49] P. Sharma and H. Liu, "A machine-learning-based data-centric misbehavior detection model for internet of vehicles," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4991–4999, 2020. doi: 10.1109/JIOT.2020.3035035.

[50] J. Yang, J. Hu, and T. Yu, "Federated AI-enabled in-vehicle network intrusion detection for internet of vehicles," *Electronics*, vol. 11, no. 22, pp. 3658, 2022. doi: 10.3390/electronics11223658.

[51] R. Hu, Z. Wu, Y. Xu, and T. Lai, "Vehicular-network-intrusion detection based on a mosaic-coded convolutional neural network," *Mathematics*, vol. 10, no. 12, pp. 2030, 2022. doi: 10.3390/math10122030.

[52] S. Jeong, B. Jeon, B. Chung, and H. K. Kim, "Convolutional neural network-based intrusion detection system for AVTP streams in automotive Ethernet-based networks," *Veh. Commun.*, vol. 29, no. 3, pp. 100338, 2021. doi: 10.1016/j.vehcom.2021.100338.

[53] S. M. Kasongo, "A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework," *Comput. Commun.*, vol. 199, no. 1, pp. 113–125, 2023. doi: 10.1016/j.comcom.2022.12.010.

[54] M. H. Modirrousta, P. F. Arani, and M. A. Shoorehdeli, "Analysis of anomalous behavior in network systems using deep reinforcement learning with CNN architecture," arXiv preprint arXiv:2211.16304, 2022.

[55] N. B. Singh, M. M. Singh, A. Sarkar, and J. K. Mandal, "A novel wide & deep transfer learning stacked GRU framework for network intrusion detection," *J. Inf. Secur. Appl.*, vol. 61, no. 1, pp. 102899, 2021. doi: 10.1016/j.jisa.2021.102899.

[56] I. Idrissi, M. Azizi, and O. Moussaoui, “Accelerating the update of a DL-based IDS for IoT using deep transfer learning,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 23, no. 2, pp. 1059–1067, 2021. doi: 10.11591/ijeecs.v23.i2.pp1059-1067.

[57] S. T. Mehedi, A. Anwar, Z. Rahman, K. Ahmed, and R. Islam, “Dependable intrusion detection system for IoT: A deep transfer learning based approach,” *IEEE Trans. Industr. Inform.*, vol. 19, no. 1, pp. 1006–1017, 2022. doi: 10.1109/TII.2022.3164770.

[58] E. Rodríguez *et al.*, “Transfer-learning-based intrusion detection framework in IoT networks,” *Sensors*, vol. 22, no. 15, pp. 5621, 2022. doi: 10.3390/s22155621.

[59] L. Yang and A. Shami, “IDS-ML: An open source code for intrusion detection system development using machine learning,” *Softw. Impacts*, vol. 14, pp. 100446, 2022. doi: 10.1016/j.simpa.2022.100446.

[60] J. S. Kumar, G. Sivasankar, and S. S. Nidhyananthan, “An artificial intelligence approach for enhancing trust between social IoT devices in a network,” *Toward Soc. Internet of Things (SIoT): Enabl. Technol., Architect. and Appl.: Emerg. Technol. Connect. Smart Social Objects*, vol. 846, pp. 183–196, 2020.

[61] A. Samad, S. Alam, S. Mohammed, and M. Bhukhari, “Internet of vehicles (IoV) requirements, attacks and countermeasures,” in *Proc. 12th INDIACom; INDIACom-2018; 5th Int. Conf. Comput. Sustain. Global Develop. IEEE Conf.*, New Delhi, 2018, pp. 1–4.

[62] N. Sharma, N. Chauhan, and N. Chand, “Security challenges in Internet of Vehicles (IoV) environment,” in *First Int. Conf. Secure Cyber Comput. Commun. (ICSCCC)*, Jalandhar, India, 2018, pp. 203–207.

[63] P. Cheng, M. Han, A. Li, and F. Zhang, “STC-IDS: Spatial-temporal correlation feature analyzing based intrusion detection system for intelligent connected vehicles,” *Int. J. Intell. Syst.*, vol. 37, no. 11, pp. 9532–9561, 2022. doi: 10.1002/int.23012.

[64] W. Wu *et al.*, “A survey of intrusion detection for in-vehicle networks,” *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 919–933, 2019. doi: 10.1109/TITS.2019.2908074.

[65] B. Lampe and W. Meng, “Can-train-and-test: A curated CAN dataset for automotive intrusion detection,” *Comput. Secur.*, vol. 140, pp. 103777, 2024.

[66] G. Peng, K. Wang, H. Zhao, and H. Tan, “Integrating cyber-attacks on the continuous delay effect in coupled map car-following model under connected vehicles environment,” *Nonlinear Dyn.*, vol. 111, no. 14, pp. 13089–13110, 2023. doi: 10.1007/s11071-023-08508-5.

[67] G. Peng, X. Li, and H. Tan, “Integrating the safety control against cyber-attacks on the global information in coupled map car-following model under connected vehicles platoon environment,” *IEEE Trans. Intell. Transp. Syst.*, pp. 1–12, 2024. doi: 10.1109/TITS.2024.3391372.

[68] W. Wu *et al.*, “Sliding window optimized information entropy analysis method for intrusion detection on in-vehicle networks,” *IEEE Access*, vol. 6, pp. 45233–45245, 2018. doi: 10.1109/ACCESS.2018.2865169.

[69] Z. Jin, Y. Xun, J. Qin, and J. Li, “MIDS: A new vehicle intrusion detection system based on multiple features,” in *GLOBECOM, 2023-2023 IEEE Global Commun. Conf.*, Kuala Lumpur, Malaysia, 2023, pp. 6717–6722.

[70] W. Wei, F. Gao, R. Scherer, R. Damasevicius, and D. Połap, “Design and implementation of autonomous path planning for intelligent vehicle,” *J. Int. Technol.*, vol. 22, no. 5, pp. 957–965, 2021. doi: 10.53106/160792642021092205002.

[71] Q. Wu, X. Fan, W. Wei, and M. Wozniak, “Dynamic scheduling algorithm for delay-sensitive vehicular safety applications in cellular network,” *Inf. Technol. Control*, vol. 49, no. 1, pp. 161–178, 2020. doi: 10.5755/j01.itc.49.1.24113.

[72] S. E. Bibri and S. K. Jagatheesaperumal, “Harnessing the potential of the metaverse and artificial intelligence for the internet of city things: Cost-effective XReality and synergistic AIoT technologies,” *Smart Cities*, vol. 6, no. 5, pp. 2397–2429, 2023. doi: 10.3390/smartcities6050109.

[73] S. K. Jagatheesaperumal, S. E. Bibri, J. Huang, J. Rajapandian, and B. Parthiban, “Artificial intelligence of things for smart cities: Advanced solutions for enhancing transportation safety,” *Comput. Urban Sci.*, vol. 4, no. 1, pp. 10, 2024. doi: 10.1007/s43762-024-00120-6.

[74] S. Nie, L. Liu, and Y. Du, “Free-fall: Hacking tesla from wireless to can bus,” *Briefing Black Hat. USA*, vol. 25, no. 1, pp. 16, 2017.

[75] M. H. Ali *et al.*, "Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT)," *Electronics*, vol. 11, no. 3, pp. 494, 2022. doi: 10.3390/electronics11030494.

[76] C. -J. Huang, K. -W. Hu, H. -Y. Ho, and H. -W. Chuang, "Congestion-preventing routing and charging scheduling mechanism for electric vehicles in dense urban areas," *Inf. Technol. Control*, vol. 50, no. 2, pp. 284–307, 2021. doi: 10.5755/j01.itc.50.2.27780.

[77] E. Seo, H. M. Song, and H. K. Kim, "GIDS: GAN based intrusion detection system for in-vehicle network," in *2018 16th Annual Conf. Privacy, Secur. and Trust (PST)*, IEEE, 2018, pp. 1–6.

[78] H. Lee, S. H. Jeong, and H. K. Kim, "OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame," in *15th Annual Conf. Priv., Secur. and Trust (PST)*, Calgary, AB, Canada, 2017, pp. 5709.