Hindawi
Security and Communication Networks
Volume 2021, Article ID 8868355, 23 pages
https://doi.org/10.1155/2021/8868355

*Review Article*

# Machine Learning Technologies for Secure Vehicular Communication in Internet of Vehicles: Recent Advances and Applications

**Elmustafa Sayed Ali**,[1,2] **Mohammad Kamrul Hasan**,[3] **Rosilah Hassan**,[3] **Rashid A. Saeed**,[4] **Mona Bakri Hassan**,[1] **Shayla Islam**,[5] **Nazmus Shaker Nafi**,[6] **and Savitri Bevinakoppa**[6]

[1]*Department of Electronics Engineering, Sudan University of Science and Technology, Khartoum, Sudan*
[2]*Department of Electrical and Electronics Engineering, Red Sea University, Port Sudan, Sudan*
[3]*Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), 43600 Bangi, Selangor, Malaysia*
[4]*Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*
[5]*Department of Computer Science, Institute of Computer Science and Digital Innovation, UCSI University Malaysia, 56000 Kuala Lumpur, Malaysia*
[6]*Schools of IT and Telecommunication Engineering, Melbourne Institute of Technology, Melbourne, Australia*

Correspondence should be addressed to Mohammad Kamrul Hasan; hasankamrul@ieee.org

Received 21 July 2020; Revised 30 January 2021; Accepted 24 February 2021; Published 13 March 2021

Academic Editor: Fawad Ahmed



Recently, interest in Internet of Vehicles' (IoV) technologies has significantly emerged due to the substantial development in the smart automobile industries. Internet of Vehicles' technology enables vehicles to communicate with public networks and interact with the surrounding environment. It also allows vehicles to exchange and collect information about other vehicles and roads. IoV is introduced to enhance road users' experience by reducing road congestion, improving traffic management, and ensuring the road safety. The promised applications of smart vehicles and IoV systems face many challenges, such as big data collection in IoV and distribution to attractive vehicles and humans. Another challenge is achieving fast and efficient communication between many different vehicles and smart devices called Vehicle-to-Everything (V2X). One of the vital questions that the researchers need to address is how to effectively handle the privacy of large groups of data and vehicles in IoV systems. Artificial Intelligence technology offers many smart solutions that may help IoV networks address all these questions and issues. Machine learning (ML) is one of the highest efficient AI tools that have been extensively used to resolve all mentioned problematic issues. For example, ML can be used to avoid road accidents by analyzing the driving behavior and environment by sensing data of the surrounding environment. Machine learning mechanisms are characterized by the time change and are critical to channel modeling in-vehicle network scenarios. This paper aims to provide theoretical foundations for machine learning and the leading models and algorithms to resolve IoV applications' challenges. This paper has conducted a critical review with analytical modeling for offloading mobile edge-computing decisions based on machine learning and Deep Reinforcement Learning (DRL) approaches for the Internet of Vehicles (IoV). The paper has assumed a Secure IoV edge-computing offloading model with various data processing and traffic flow. The proposed analytical model considers the Markov decision process (MDP) and ML in offloading the decision process of different task flows of the IoV network control cycle. In the paper, we focused on buffer and energy aware in ML-enabled Quality of Experience (QoE) optimization, where many recent related research and methods were analyzed, compared, and discussed. The IoV edge computing and fog-based identity authentication and security mechanism were presented as well. Finally, future directions and potential solutions for secure ML IoV and V2X were highlighted.

## 1. Introduction

Intelligent Transportation Systems (ITS) and computational systems' rapid development opened new scientific research in smart traffic safety with comfort and efficient solutions. Artificial Intelligence (AI) has been widely used to optimize traditional data-driven approaches in different research areas [1]. AI-based on the Vehicle-to-Everything (V2X) system obtains information from various sources, i.e., car, train, bus, etc., and enables to increase the realization of drivers and forecast to avoid accidents. This progression has directed to the opportunity to understand smart driving, which was built on the idea of copying real driving comportment, while avoiding human mistakes and bringing comfortable safety to drivers. Many services have been invented from crowd and light road traffic to adapting traffic, a legacy from self-based vehicle systems to the IoV [2]. IoV is addressed to change the interaction between the vehicles, roadside stations, on-board stations, and environments to communicate data and multimedia between various networks. The motivation of IoV is to be adopted and build the human-vehicle-roadside onboard IoT Connected services within the various vehicle and different networks.

Machine Learning (ML) is responsible for a wide range of AI applications. The ML techniques are unsupervised, supervised, and reinforcement learning. In the unsupervised ML scheme, training depends on untagged data. It tries to find an adequate representation of untagged data. While, in supervised learning, it learns from a group of labeled data. In supervised learning, regression and classification schemes train the discrete and continuous data for prediction and decision-making. Reinforcement learning (RL) studies from the learning agent's activities from the consistent reward to capitalize on the notion of cumulative rewards. The Markov Decision Process (MDP) is a sample of RL [2]. This scheme is a perfect technique for taking many issues' research problems in vehicular networks, such as in collaborative optimization of oil consumption for a specific area and optimum path forecasting of electric vehicles and minimizing traffic congestions.

Given the importance of the use of Artificial Intelligence (AI) in IoV, as it provides smart models in most of its applications, this paper contributes a brief concept on one of the AI methods known as machine learning and the possibility of its use in several specific aspects related to the IoV network. In IoV networks, edge computing and caching problems are the most considered challenges requiring an intelligent optimization method. Edge computing and caching challenges are related to many factors, i.e., channel condition, dynamic communication topology, and resource allocation management. In the IoV network architecture, artificial intelligence is in a separated layer responsible for virtual cloud infrastructure. The AI layer act as an information management brain. Deep neural networks are ML algorithms developed to make decisions according to learned IoV resource actions [3].

This paper has conducted a critical review with analytical simulation for offloading mobile edge computing decisions based on learning and Deep Reinforcement Learning (DRL) technologies for vehicular communication in (IoV). We have considered a typical IoV network architecture with one IoV Edge-Computing (IoVEC) and one mobile user. The tasks of the device arrive as a flow in time. Our analytical model performs the offloading decision process of the task flow as a Markov Decision Process (MDP). The optimization object minimizes the weighted sum of offloading latency and power consumption, which is decomposed into the reward of each time slot.

The rest of the paper is organized as follows; the study background and motivation are presented in Section 2, where systematic technical knowledge and motivation of secure ML in the IoV field were discussed. A brief concept of AI in IoV is reviewed in Section 3 by considering using AI in multimedia and IoV edge-based and Vehicle-to-Everything's Internet communications. Section 4 provides a clear concept about the contribution of AI to enabling QoS and QoE optimization, where QoS manages and controls resources of the IoV network by setting various priorities for each data type, while QoE discusses the measurement of the overall system homogeneity and stability of service. Section 5 provides a detailed description of using machine learning algorithms with IoV in different aspects. The most common use cases of ML in IoV applications are presented in Section 6. Section 7 gives a brief review of the possible future research directions and potential ML solutions in IoV. Finally, the conclusion is presented in Section 8.

## 2. Background and Motivation

Due to the significant research and technology development in wireless communication, the traditional ITS has to care about the vehicular communication field. Recently, the numbers of vehicles have increased due to transporting huge numbers of people from region to region. This increment in the number of vehicles would create issues such as crowding and accidents on the roads. This issue could be considered as one of the main problems in daily life. Most of the general form of vehicular networking is known as the vehicular ad hoc network (VANET) [4]. VANET consists of Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (V2R) communications to transfer the vehicles' information. The VANETs' communication depends on the Roadside Unit (RSU) to support Wireless Access in Vehicular Environments (WAVE).

The Roadside Unit (RSU) along the roadwork acts as wireless access points' support communication to the vehicles inside its coverage area [5]. The hybrid vehicular network architecture, interacted with the cellular communication architectures, will operate the cellular communication services, i.e., voice, in collaborations. Due to the current trend to connect vehicular networks to information centers and the need to exchange data, IoV allows enabling Internet access among on-road vehicles. One of the essential IoV applications is to improve the features of VANETs to reduce various issues in urban traffic and accident environments [6]. IoV enables the vehicular road networks to interconnect with different wireless network technologies i.e., Wi-Fi and 4G/LTE for V2I, IEEE WAVE for V2V and

V2R, MOST/Wi-Fi for V2S, and CarPlay NCF for V2P. It is useful to provide a comprehensive presentation to ML's concepts in IoV and explain the areas that could contribute to these networks' development [7].

In recent years, the arising need to introduce artificial intelligence technologies in IoV applications has been facing some challenges. These challenges are related to making particular decisions and forecasting different aspects of IoV, such as traffic monitoring and management, big data processing, energy and resource management, and intelligent interaction with users to provide high-quality services [6, 7]. Several studies have been conducted on using artificial intelligence techniques such as machine learning to develop solutions to most of these challenges [8]. Due to the current developments in the field of AI, especially in using machine learning techniques to make intelligent decisions in several IoV applications, it is useful to provide a comprehensive presentation to study some concepts of using ML in IoV and explain the areas that could contribute to the development of these networks.

## 3. Artificial Intelligence Methods in the IoV Network

AI technology is more related to the layer responsible for presentation and functionalities in the IoV-layered architecture. A term of virtual cloud infrastructure can describe this layer and be responsible for storing, processing, analyzing the information received from the IoV network, and decision-making based on the analyzed information. In IoV, the computation and analysis are provided by Big Data Analysis (BDA) and Vehicular Cloud Computing (VCC) systems which are used as an information management center [9]. According to the IoV applications, many services can be provided by the IoT cloud environment, requiring intelligent service management. The smart cloud-computing servers provide many smart services, i.e., safety, traffic administration, entertaining, and subscription, which are the foundation of elegance in IoV. The cloud servers based on AI enable the procedure and develop AI in Real-Time (RT) massive data traffic to provide a smart decision for intelligent customer services. The Vehicular Cyber-Physical System (VCPS) is considered a vehicular network model that concerns disseminating information using next-generation Internet [10]. VCPS depends on AI technology to provide smart processing in huge data traffic utilizing fog and cloud computing for civilian and safety applications.

In IoV networks, edge computing and caching problems are the most considered challenges requiring an intelligent optimization method. Edge computing and caching challenges are related to many factors, i.e., channel condition, dynamic communication topology, and resource allocation management. AI in IoV provides an intelligent approach to solve most of these challenges. The use of ML offers a means of interaction to the IoV environment and enables the creation of an agent that learns challenging factors to optimize the overall IoV network utilization [11]. $Q$-learning and deep neural networks are ML algorithms developed to make decisions according to learned IoV resource actions. In the IoV network architecture, the presentation of artificial intelligence in a separated layer is responsible for virtual cloud infrastructure. The AI layer acts as an information management brain [10, 11]. The AI layer in IoT architecture consists of big data analysis, cloud computing, and expert systems. It plays an essential task in storing, processing, and analyzing the information received from the coordination layer and takes decisions according to the network status.

*3.1. Artificial Intelligence Methods for IoV Multimedia Communication.* The deployment of IoV in multimedia communications requires a device that allows data exchange and communication with other surrounded devices. This can be achieved by any technology such as Personal Area Networks (PAN), the Internet of Things (IoT), and Wireless Sensor Network (WSN). Data exchange's scalability and flexibility are quite important for IoV by integrating sensors, vehicles, humans, actuators, machines, etc. The sensor in intelligent IoV enhances vehicle and traffic systems' safety, while harmonized traffic data transfer in the IoV system network enhances vehicular system efficiency. However, the amount of energy consumption, required capacity, green buffer-awareness, and message exchange through IoVs may compromise severe data transfer risk [12]. AI based on self-driven vehicles encourages several types of applications with many benefits of intelligence. Especially for the increase in the amount of data and complexity, which the algorithms will be processing, it is precise and effective for future directions. As growing, the high traffic information in IoVs required a smart utility, followed to efficiently monitor and manage the demand for intelligent IT technologies [13]. With the rapid evolution in digital technologies, the development of multimedia depends on the IoV system, and it needs a portable device to collect a voluminous amount of information for aiding and guiding the specific trend for analyzing the transportation industry by IoT-based platforms.

Figure 1 shows the structure of multimedia communication through sensor nodes in the IoV system. Its structure consists of three main parts for IoV data and information network techniques and models. The data and information network techniques and models are redeveloped with the central server. The inter and intravehicle network connections among various sections are executed by transferring urgent and sensitive data throughout the vehicle via adaptive and smart wireless communication. The vehicle's client enables QoS monitoring [13, 14]. In this structure, the IoV traffic can be arranged based on the category containing sensitive/standard, prestored, real-time, or high-definition resolution, respectively. To accomplish the real-time and jitter-tolerant data and information exchange with low buffer storage and scarce power supply, it should be fortified to tolerate the raw unprocessed data and information into

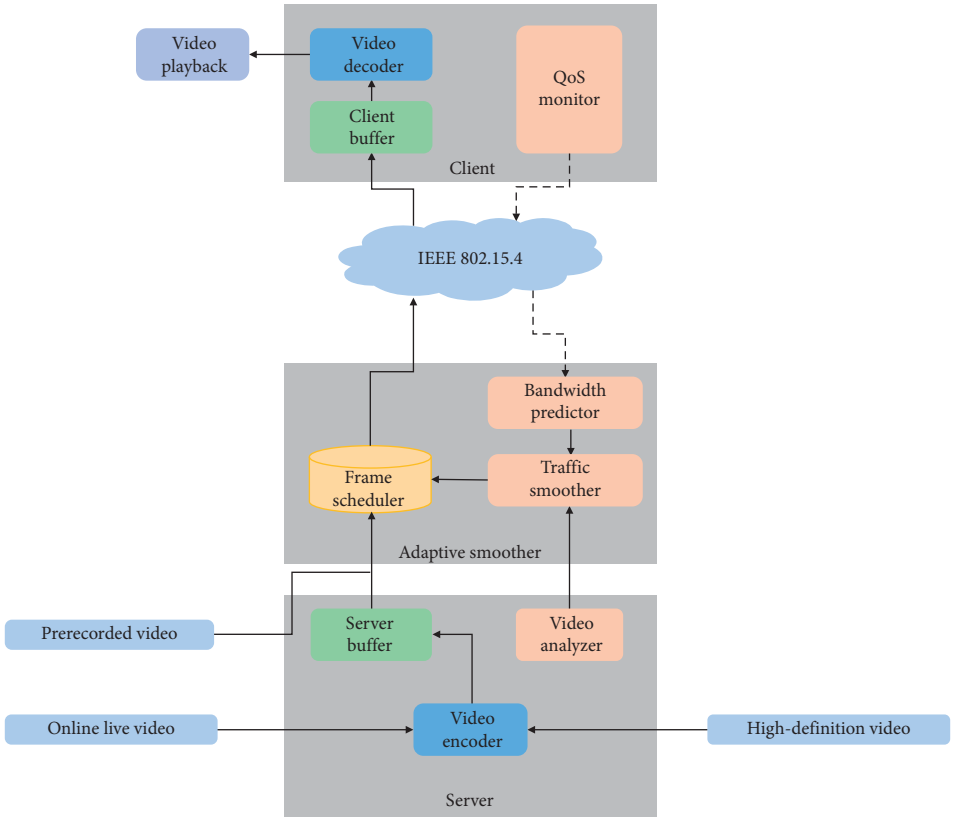


Figure 1: IoV data and information network techniques and models [14].

the regular and synchronized format with good and clean visibility.

*3.2. Intelligent IoV Edge-Based Algorithm.* IoV Edge Computing (IoVEC) is a new technology that enables vehicles to communicate with cloud computing to directly deliver cloud services from the network edge and support delay-critical IoV applications. It could be achieved by placing computer servers at radio access points or base stations. In edge caching and computing platforms, AI trains and deploys powerful ML models at the edge servers and mobile devices. Edge AI techniques changed the structure of the semiconductor industry [15]. In IoV, the Edge Information System (EIS) plays a vital and unique role. It is able to help the key functionalities of intelligent vehicles, from data acquisition and data processing to actuation. Data processing in the network edge can satisfy the low-latency requirement for mission-critical tasks and save an amount of communication bandwidth. The AI edge-based IoV typically has high spatial locality for road conditions, map information, and temporal locality for traffic conditions. On the contrary, with big sensing data, intelligent vehicles are facing tremendous computation burdens [12, 15].

Offloading computation and load balancing are the most critical factors that determine the maximum system utility in IoV. Cooperative edge caching and edge computing can serve to improve the performance of these factors. But indeed, the edge computing and caching policies are limited in dynamic systems' applications such in IoV networks. AI cognitive capability helps develop edge cognitive computing architecture to provide dynamic computing service [16]. AI cognitive capability will improve energy efficiency and user experience since it is able to interact with other IoV components to perform efficient resource management, as shown in Figure 2. IoV architecture-based AI algorithms enable the perception of vehicular environment information's real-time behavior by interacting with the environment according to the current state related to offloading, cooperative caching, and edge computing [15, 16].

The IoV edge-based AI architecture can efficiently drive the edge computing resources depending on cooperative caching to manage edge computing policies. Such edge-based AI architectures can use deep ML algorithms for efficient IoV resource management. Other considerations related to system utility are IoV network mobility and vehicles'/RSUs' handover mechanisms. These considerations are significant factors that significantly affect temporary storage resources [15]. Therefore, it is necessary to the trade-off between the accuracy of the prediction, the temporary storage of content on the move, and the handoff implementation. AI enables the prediction of handover and intelligent sharing of allocated bandwidth and edge caching.

*3.3. Artificial Intelligence Methods for Vehicle-to-Everything.* In vehicular applications, AI enables executing tasks intelligently, such as enhancing the Plug-in Electric Vehicle

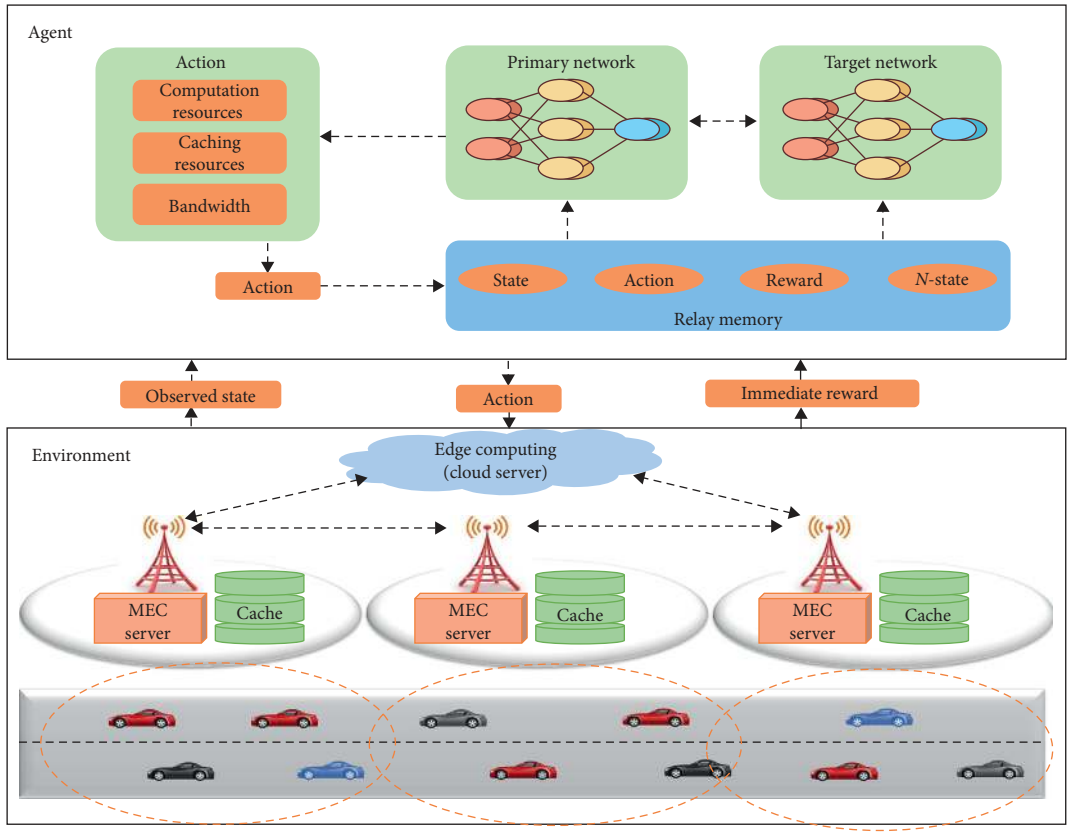


Figure 2: IoV edge-based AI architecture.

(PEV) charge, minimizing fuel consumption, enhancing location-based services, and traffic congestion rectification. The traffic flow information can be obtained from multiple sources such as induction loops, crowd sourcing-based information services and vehicles, and Closed-Circuit Television (CCTV) cameras [17]. Modeling precise and accurate traffic exchange prediction procedures utilizing legacy traffic flow prediction mechanisms is a vital problematic issue. AI techniques have been extensively used for modeling estimation mechanisms in research areas such as robotics, data science, computer vision, natural language processing, and medicine. AI used the data-driven method that facilitates it more efficiently to tackle little and multimedia data. The aims of V2X technology to transportation systems are to enhance safety and efficiency by sharing data among vehicles, infrastructures, and walkers. V2X schemes received a tremendous amount of use in academia, industry, and governments.

There are three fundamental aspects of a V2X communication system: road safety, energy efficiency, and traffic efficiency [18]. The V2X scheme is based on sharing information among Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V), Vehicle-to-Self (V2S), Vehicle-to-Pedestrian (V2P), and Vehicle-to-Road side units (V2R). V2X is an evaluation technology for vehicular networks. AI with V2X can enable new approaches to applications such as traffic flow prediction and management for real-time data, location-based applications, vehicular platoons, data storage in vehicles, autonomous transport facilities, and congestion control. The most widely utilized AI techniques are Heuristic Techniques, Robotics, Game-Theoretic Learning, Expert Systems, Evolutionary Algorithms, Turning Test, Logical AI, Planning, Schedule and Optimization, Natural Language Processing, Swarm Intelligence, Inference, Fuzzy Logic, and Machine Learning [19]. One of the ML-based V2X is autonomous driving where AI is used to enable essential features of human driving. ML in V2X can play a critical role in enhancing safety and efficiency of in-vehicle networks [18]. Modern machines have widely applied it for applications such as competing at the highest level in strategic games, autonomous vehicles, understanding human speech, and intelligent network routing in content delivery networks.

Other considerations are related to security in V2X applications. AI provides many security mechanisms for routing protection against threats and attacks. In addition, the AI swarm intelligent algorithms protect against malicious vehicle attacks. A DL-based technique for anomaly detection in V2X vehicles provides a means of security against different kinds of attacks, i.e., Denial of Service (DOS), rushing attacks, gray hole, and Sybil attacks. The research work presented by Abdallah Moubayed (2020) reviews the concept of using machine learning in fifth generation (5G) IoV for security issues, in addition to discussing various challenges faced by V2X communications [20]. The study presents the considerations related to V2X security and privacy and illustrates different kinds of attacks

related to authentication, confidentiality, data integrity, and accountability. Zeinab El-Rewini (2020) provided a three-layer automotive security framework considering the issues of control, communication, and sensing [21]. The framework enables eavesdropping, jamming, and spoofing attacks.

Moreover, it has the ability to detect different communication layer attacks in the V2X network such as spoofing, man-in-the-middle, and Sybil attack; the research is also providing a survey on using the machine and deep learning for cybersecurity solutions and V2X network security. Haji M. Furqan (2019) had introduced an intelligent security framework for V2X communication based on the AI radio brain model to enable learning information from higher network layers and radio environment [22]. The security framework detects the vehicle condition and considers the channel information to decide the best-suited security level. In this scheme, decision-making depends on vehicle conditions related to location, environment, utility, time, and application. In automotive V2X, traffic safety is an important issue that needs to make data classification and enable secure permitting of the autonomous vehicle. The defensible decision to pass another vehicle is a critical issue according to its dynamic behavior. Jean-Philippe Monteuuis provided a misbehavior classifier related to data classification for multiple road users using machine learning algorithms [23].

Another V2X traffic issue is location spoofing, which can cause traffic congestion. So (2019) reviewed practical spoofing attacks that can pay to pass the security checks in the V2X application layer [24]. The study proposed three physical layer checks to ensure the detection rate and decrease false positives, in addition to enabling comprehensive evaluation of the performance of the security for several types of attacks. The misbehavior detection is depending on machine learning to security checks at the application layer using the VeReMi datasets which are enhanced datasets for several types of attacks. Kang (2016) used the Intrusion Detection System (IDS) based on Deep Neural Network (DNN) for V2V and V2I networks [27]. The proposed study uses unsupervised Deep Belief Network (DBN) pretraining schemes to train the parameters of the DNN to optimize the learning efficiency. The IDS-based DNN enables to train high-dimensional CAN packet data afterwards, in order to extract the statistical properties of normal and attack packets to identify the attack. This method provides security features against hacking packets and identifies any malicious attack to V2X networks. Table 1 presents a brief summary of different research works considering the use of AI technology in Vehicle-to-Everything's security issues.

## 4. Artificial Intelligence-Enabled Quality of Experience Optimization (QoE)

In IoV, QoE provides measurement deals with network performance and perception, in addition to IoV application experience. The QoE considers the IoV experience to ensure high quality of data transmission by continuously measuring the QoE of the network and updating. For IoV end users and due to the rapid change of IoV communication topology, the user's quality of experience is considered as one of the main challenges in IoV networks [28]. The flexible and scalable connection between integrated components of the IoV system i.e., vehicles, sensors, actuators, humans, and machines, is vital for IoV, which must fit with the requirement of user perception enhancement to decrease the power consumption. Moreover, to improve transportation systems' safety and traffic data exchanging in vehicular networks, power and buffer-aware QoE/QoS via IoV came with a high risk of quality compromise during sensitive IoV applications i.e., in the medical field. For such reason, cost-effective power and buffer-aware QoE optimization solutions for designing and deploying the IoV are required. Quality of Service (QoS) in IoV is related to the routing path quality, impact of velocity, position of vehicles, and network topology. These aspects mainly affect IoVs' energy efficiency [29]. The QoS optimization with energy efficiency regarding the IoV network efficiency is about developing a solution to the multiattribute decision-making and being able to optimize many IoV network operations.

AI techniques have changed the landscape of the IoV through multimedia communication. It improves the overall IoV network by efficiently optimizing the route selection to obtain stable transmitting multimedia content in the IoV system [14, 29]. AI can also help develop energy and buffer-aware optimization mechanisms to optimize the QoE and QoS during multimedia communication in the IoV system. Machine Learning (ML) techniques can provide a framework to analyze the QoE services with the high level of optimization. ML will help in assessing and examining the faults and quality degrading factors prospected from important collected information by IoV systems to enhance the IoV user's satisfaction, in addition to evaluating the QoS by considering several impacts to the IoV network related to communication, energy, and resource management operations [14].

*4.1. Buffer-Aware QoE/QoS Optimization.* Due to the high demand for video traffic in IoV networks, the development of intelligent solutions must fulfill the expectations and ensure maximum Quality of Experience (QoE). The optimization of QoE during multimedia communication in the IoV system can be obtained by deploying a novel algorithm based on the buffer allocation mechanism, which enables controlling the high peak variable rate of multimedia by allocating the proper buffer size in IoV. The buffer aware QoE optimization must consider the requirements related to energy and video rate adaptation. In IoV applications based on video transmission, the dynamic adapting coding rate of the requested videos can ensure that optimizing the QoE by the encoding rate depends on the video content itself. Machine learning algorithms provide automatic video processing with the additional complexity given by the data's temporal dimension [30]. ML can achieve different video processing schemes in pixel level or higher-level

Table 1: Summary of artificial intelligence methods in secure Vehicle-to-Everything networks.

| Year | Source | Security approaches | Features | Advantages | Challenges | Citations |
|---|---|---|---|---|---|---|
| 2020 | ArXiv | NSL-KDD data mining; Cloud Security Alliance (CSA) | Machine learning in fifth generation (5G) IoV | Security issues related to softwarization, software-defined perimeter, and virtualization | QoS performance and scalability and cost in secure V2X dynamic networks | Abdallah [20] |
| 2020 | Elsevier | Controller Area Network (CAN); IDS; Security-Aware FlexRay Scheduling Engine (SAFE); Hardware Security Module (HSM) | AI-based V2X automotive security framework | Detects sensing and communication layers' attacks | Cybersecurity in fully autonomous V2X | El-Rewini [21] |
| 2019 | arXiv | Intelligent V2X security (IV2XS); physical layer security (PLS) | Cognitive security based on context-aware proactive security | Security decision-making according to vehicles' channel conditions | Identify the best-suited level of security. | Furqan [22] |
| 2019 | WiSec'19 | Basic safety messages (BSMs). | Misbehavior detection based on ML for secure V2X traffic | Detects spoofing attacks in the V2X application layer | Identify and detect the V2X location spoofing | So [24] |
| 2018 | IEEE | MinMax, MLP, Adaboost, and Random Forest misbehaving classifiers | V2X traffic safety-based ML algorithms | A misbehavior classifier for vehicle data classification | Secure decision for V2X traffic safety | Monteuuis [26] |
| 2016 | PLoS ONE | Controller Area Network (CAN) and IDS | Intrusion detection system (IDS) based on deep neural network (DNN) | Extract the statistical properties of normal and attack CAN data packets | Identify malicious attack to V2X networks | Kang [27] |

representations obtained after additional preprocessing of raw images. The ML schemes enable the optimization of the process of buffer allocation and dynamic video-rate adaption.

In IoV networks, it is challenging to achieve QoS and efficiency for multimedia streaming, especially in high-mobility features. The buffer-aware streaming approach will allow users to play multimedia streaming over the IoV network. AI-based buffer-aware QoS adopted for vehicle streaming services to evaluate multimedia content preloaded by IoV servers according to the user's mobility information. A buffer-aware QoS streaming approach over the IoV network can provide various priority levels of streaming service [31]. ML will evaluate vehicle mobility's direction and speed, the strength of IoV signals, and the size of media content stored in the buffer to optimize the quality of streaming service on the IoV network.

*4.2. Energy-Aware QoE/QoS Optimization.* Energy management in IoV systems is considered one of the main challenges faced in IoV applications. It is very important to effectively manage the power resources during communication in the IoV system. In most IoV applications, the Electric Vehicles' (EVs) charging and discharging time negatively impact the QoE. Power-aware QoE Optimization in Vehicle-to-Grid (V2G) networks expresses the degree of satisfaction with the State of Charge (SOC) and charging the cost of using an EV [32]. In the charging schedule, the service of enough CSs is an important QoE metric, especially in the peak charging hours. AI-based charging scheduling schemes must consider the QoE optimization. The QoE of vehicles in the IoV network with a higher vehicle's mobility and limited coverage area of RSU can be degraded and can significantly affect communication quality by decreasing flow satisfaction. In addition, any growth in energy consumption in RSU leads to inefficient IoV energy network management [33]. Moreover, due to the limited IEEE 802.11p-based vehicular communication bandwidth, providing a fair share of network resources among vehicles will face a crucial problem related to flow management [34]. AI-based energy management schemes provide an intelligent decisions' controller to overcome energy operation's complexity by providing efficient solutions. Table 2 presents the key points of most related works in AI technologies that use the IOV QoS/QoE optimizations.

## 5. Machine Learning Algorithms in the IoV Network

Machine learning has different models, classifications, and training methods widely used for prediction problems and intelligent managing. In IoV applications, Reinforcement Learning (RL) will provide guidance behavior to promote resilience and scalability. It can give path selection or route optimization in IoV networks. The use of ML with the Software Defined Network (SDN) in IoV can ensure delay of minimization and throughput maximization as the operation and maintenance strategy. Together, ML and SDN will improve the IoV network performance with stable and superior routing services [35]. They can ensure optimal routing policy adaptation according to sensing and learning from the IoV environment to achieve better utilization. Figure 3 shows the functions of ML that can be deployed in the IoV networks. In the domain of IoV network security,

Table 2: Artificial intelligence methods in IoV QoS/QoE optimization.

| Year | Source | Approaches | Features | Advantages | Challenges | Citations |
|---|---|---|---|---|---|---|
| 2020 | Sensors | Reinforcement learning; centralized Q-learning | Energy optimization with 5G vehicular social networks | Maximize the energy efficiency and optimization | Ensure communication quality and reduce delays | Park and Lim [33] |
| 2019 | IJEAT | SDN-based ML (BAT algorithm) | Prioritize the data packets in IoT cloud storage | Enhance traffic QoS | Traffic delay reduction in IoT multimedia applications | Hasan et al. [28] |
| 2019 | Elsevier | Fuzzy-enabled algorithms for buffer and power-aware QoE optimization. | AI-based multimedia communication mechanism and IoV-based QoE optimization framework | Improve multimedia streaming for end users | QOE optimization for multimedia communication in IoV | Sodhro [14] |
| 2018 | IEEE | QoE-based ML for video admission control and resource management | Extracting the quality-rate characteristics of unknown video sequences | Improve the service and quality level delivered to end user | Guarantee a minimum service quality level | Islam et al. [30] |
| 2017 | EAI | Many-to-one matching game; Stable Matching Algorithm (SMA); Pareto Optimal Matching Algorithm (POMA) | Traveling plan-aware scheduling scheme for EV charging in driving pattern | Improve the QoE in vehicle power grid networks | QoE enhancement in EV industry | Bozkaya and Canberk [34] |
| 2016 | Science PG | Fuzzy QoS | Enhance energy efficiency in IoV | Optimize energy QoS | Trade-off between QoS and energy efficiency | Hu [29] |

ML with the SDN brings some unique advantages to the deployments of security solutions. For security issues, the centralized control on the software layer with API access will be convenient to develop ML software interaction with the SDN data plane to provide statistical reports to the application layer upon vehicles' requests [36].

In Cognitive Internet of Vehicles' (CIoV) applications, i.e., automatic driving, automation and connectivity are very important in self-driving aspects which should be sufficient of intelligence to reduce road accidents. ML can take control of vehicles to enable error-free driving. CIoV allows cloud-based ML into a transportation system for security risks and privacy issues [37]. In CIoV cognition and control layer, ML provides strategic services for different function levels, i.e., driving behaviors, health monitoring, and pattern and emotion analysis, in addition to network resource allocation and optimization. To improve driving safety and efficiency in the IoV transportation system, deep learning (DL) schemes provide intelligent decision-making to evaluate the critical, influential collision probability factors and risk of possible accidents in the IoV [38]. Different DL techniques can be used for collision prediction and accident forecasting, i.e., Genetic Algorithms (GA), Neural Networks (NN), Fuzzy logic, and Support Vector Machine (SVM).

*5.1. ML-Based Edge Caching Mechanisms for IoV.* The operational excellence and cost efficiency in IoV depend on the caching and computing design. To efficiently improve the QoS for applications, edge caching placements and computing offloading at the vehicles and the RSUs can ensure efficient QoS. Machine learning provides schemes to tackle problems encountered in caching, computing, and communications for IoV. Many ML schemes can be used for edge caching in IoV [39]. It provides relatively right caching decisions, IoV traffic levels' classification prediction, and content demand in supervised learning. Unsupervised learning can be applied to the edge caching design by clustering numbers' vehicles into different groups according to their behavioral and data request history information [40]. The ML-based clustering scheme can predict the data demand depending on the entire vehicle group's interests or social relations.

The reinforcement learning scheme such as the $Q$-learning technique will enable distribution cache replacement strategy according to the content popularity. Moreover, it can estimate the unknown popularity of caching contents. Integrated Mobile Edge Computing (MEC) servers in the IoV network will help reduce the workload at roadside stations and make the vehicle requesting content perform data and computation offloading during its movements such as mobility-aware caching and computational scenario, as shown in Figure 4. The use of deep $Q$-learning will optimize the parameters of caching and computing for resource allocation. Deep $Q$-learning will determine the optimal actions from the collected status of MEC and RSU servers in addition to each vehicle's mobility, channel information, caching contents, and computing [39, 40]. These actions are forwarded to vehicles. Deep $Q$-learning will select the best set of caching activity for RSU, MEC, and vehicles to serve the requesting and compute the offloading tasks for the IoV.

Integration of ML with edge caching has challenges related to data processing and analysis. The diffusion and high density of data are challenges for the learning and training process. In addition, insufficient computing resources can manipulate the high-dimensional information

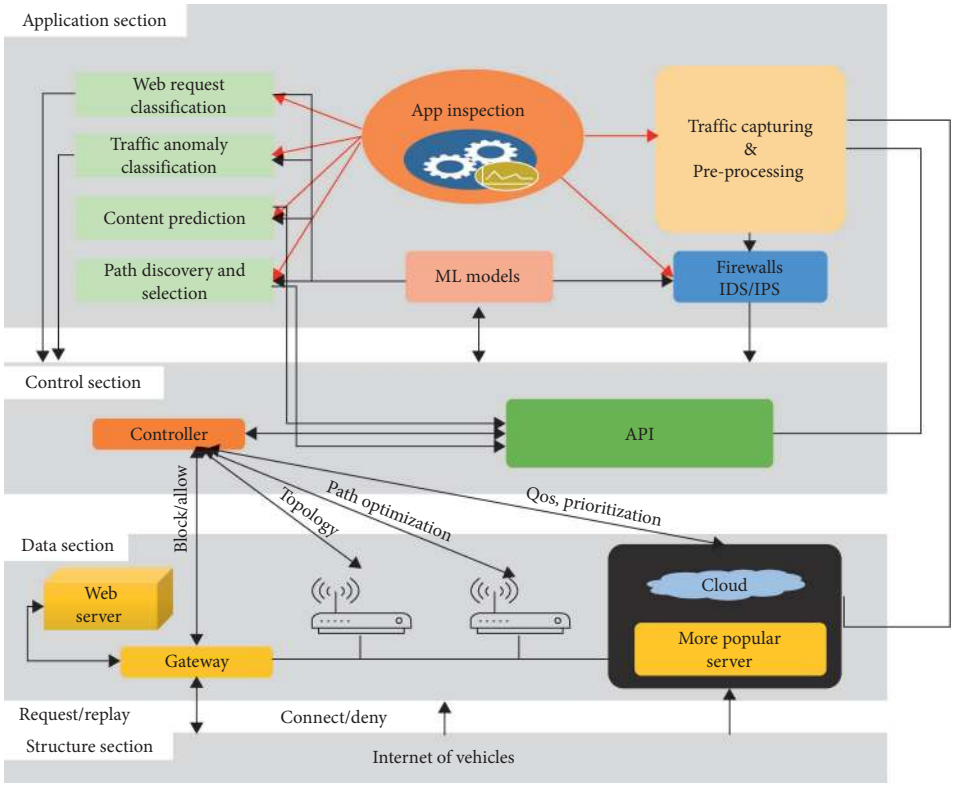


Figure 3: ML functions in the IoV network [36].

that cannot provide precise buffering decisions. To strongly cooperate ML at the IoV network edge to enhance the edge's smart duties, it requires an effective learning approach for massive high-dimensional information that is established to offer a precise estimation of the buffered information at the IoV network edge. Moreover, ML schemes' deployment in IoV applications will extract much sensitive and critical information, and if there is any leakage of information, it can cause serious confidentiality, security, and privacy concerns [40]. For these concerns, an edge-caching system must be secured by security and privacy-preserving schemes and should be developed in different system levels, i.e., transmission/collection, data processing, data access, and storage levels for both edge networks and vehicles.

*5.2. Deep Reinforcement Learning-Based Offloading Algorithm.* The execution of computing-intensive applications on resource-constrained vehicles still faces a challenge related to offloading the IoV system. Deep Reinforcement Learning (RL) will provide an intelligent offloading system for vehicular edge computing. Integration of Deep RL with vehicular edge computing helps to schedule offloading requests and allocate IoV network resources. Deep RL optimizes the scheduling and resource allocation in IoV to maximize the QoE. In IoV, vehicles calculate utility values related to their available RSUs and pass the offloading requests to the roadside stations. The stations perform task scheduling and resource allocation and inform the RSUs. RSUs are able to receive all vehicle offloading tasks to perform computation offloading. The deep RL algorithms help to optimize the offloading decision by intelligent task scheduling. Figure 5 shows the deep reinforcement learning-based task offloading framework. Offloading requests are scheduled in the task according to the action-value function Q. RSU is selected by vehicles from the available accessing list with probability $\varepsilon$ and largest $Q$-value of the current action-value function [41]. The use of deep RL in IoV offloading optimization will be guaranteeing their venue of network operators by ensuring cooperative offloading in the IoV network, which will maximize the QoE of vehicles.

In IoV offloading computing, optimization parameters are related to the offloading ratio  i for each task. The vehicle's utility value constraints are related to the limitations of vehicle's CPU and memory resources. Offloading optimization depends on how to minimize the function task latency and energy costs [42]. The cost function can be calculated as follows:

$$\text{Function} = \sum_{i=1}^{N} \left(L_i + w_i E_i\right), \tag{1}$$

where $N$ represents the number of tasks, $L_i$ is denoted for latency cost, and $E_i$ is denoted  for energy cost, and $w_i$ is denoted for the weight ratio between latency and energy cost. Each offloading decision is taken depending on the resource unit time slot. This means the flow of scheduling tasks is a sequence in time. For the sequence of $N$, tasks

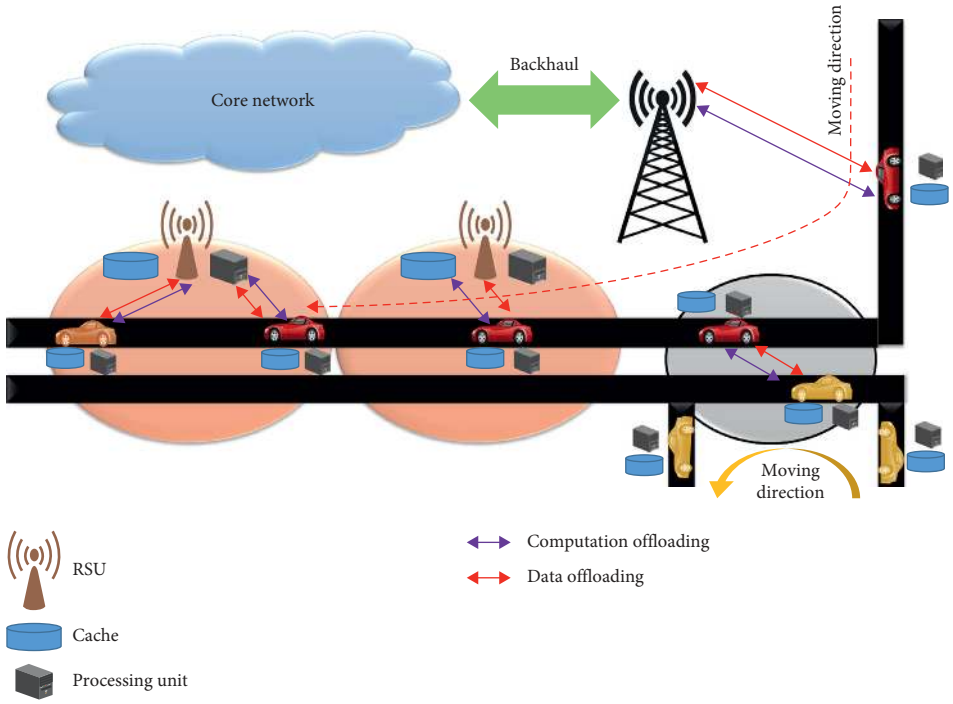


Figure 4: IoV mobility-aware caching and computational scenario [39].

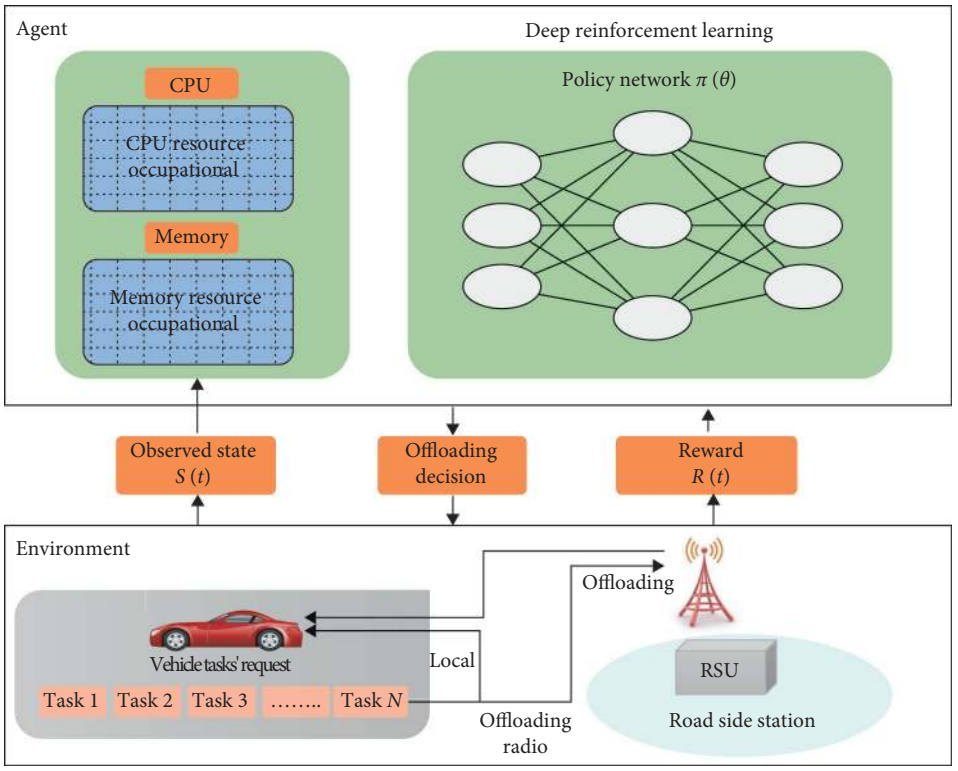


Figure 5: Offloading decision optimization-based deep reinforcement learning.

arrive during a limited observing time $L_{obs}$, and the cost function $F$ can be calculated depending on the reward function $R(t)$ by

$$\text{Function} = \sum_{t=1}^{L_{obs}} \left(\gamma^{t-1} R(t)\right), \tag{2}$$

where $R(t)$ is the reward of time slot $t$ and $\gamma$ denoted for the reward discount ratio to describe affection of rewards of the future time slot on the overall cost function. This total cost function can be used to make policy network training. Deep neural networks will provide a policy for mapping from perceived states of the IoV environment to the probabilities of actions to be taken. The policy network-based deep RL training will achieve optimized computing via each time slot [42]. This will minimize the weighted sum of offloading latency and power consumption cost and ensure offloading decision optimization. Figure 6 presents the average cost for power consumption versus probability of task arrival, and Figure 7 shows the average cost for task latency (in Seconds) for different ML for IoV architecture vs. task arrival probability.

The Markov Decision Process (MDP) method is compared with three various techniques i.e., Local, IoVEC, and Random. Local means the zero-offloading technique where all tasks are performed in the vehicle on-board device. IoVEC is known as an integrated IoV edge computing server where a full-offloading procedure has to be maintained and performed. Finally, a random technique selects offloading randomly.

In IoV-based edge computing, vehicles act like clients connecting over the edge-computing node on the roadside without accessing a remote cloud. In this scenario, the offloading decision for heterogeneous resources is considered a complex operation. This is because the environment of vehicular edge computing is changing each time and requires that offloading decisions be re-computed, which will delay providing services. In addition, for vehicular service, the task execution progress cannot guarantee fairness offloading queuing. Deep RL provides a unique decision algorithm to achieve intelligent vehicular-controlled services based on an edge computing model [43]. It helps to learn the service offloading knowledge and the observation functions related to environmental data of vehicular mobility and the edge computing nodes. The offloading decision model is trained at the powerful edge computing nodes and distributes the decision information to the vehicles for services offloading. During decision model training, vehicles transmit the parameters to the roadside station edge-computing node for updating the necessary offloading decision periodically.

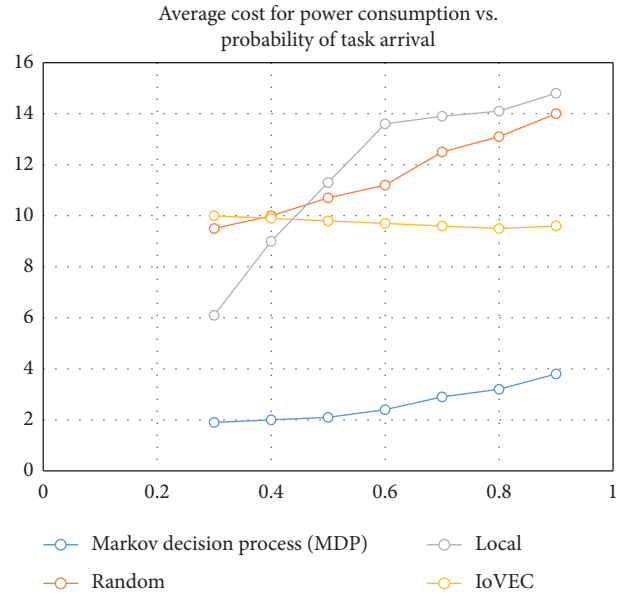


Figure 6: Average cost power consumption (KJ) for different ML for IoV architecture vs. task arrival probability.

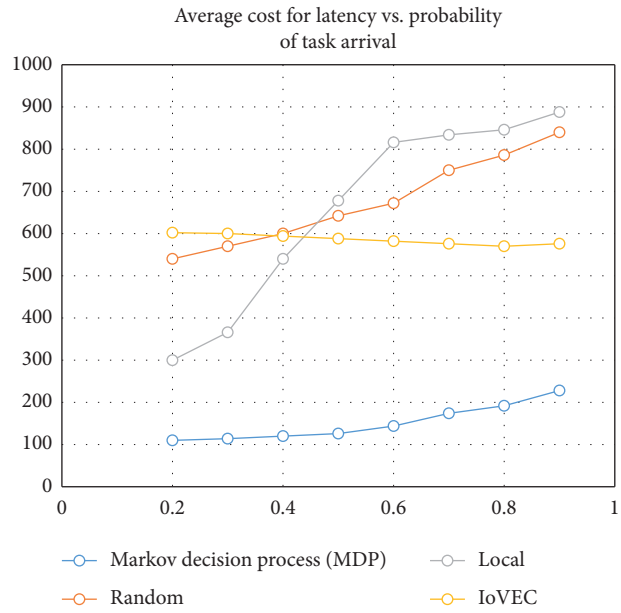


Figure 7: Average cost for task latency (Sec) for different ML for IoV architecture vs. task arrival probability.

*5.3. ML for Dynamic and High-Mobility IoV.* IoV networks may have dynamic features in many aspects, i.e., topology, traffic, and wireless propagation channels, due to their mobility. An efficient learning and dynamic prediction must provide a degree of optimization in routing, traffic load, and assisting the channel estimation module-tracking channel variations [44]. Machine learning (ML) methods lead to better results for modeling the dynamic changes of vehicular channels and optimizing vehicle routing and traffic flow. ML systems integrated into RSUs help to estimate traffic patterns by collecting information about vehicles. ML can provide intelligent IoV routing protocol with critical information for a highly dynamic environment. It was able to predict the network capability of paths to optimize vehicle route selection based on vehicle mobility and transmission capacity. In dynamic IoV, RSUs-based ML can predict the vehicle's moves and direction [45]. The prediction is depending on the information provided by the vehicle when it moves from RSU to another which will help RSUs to enable estimation of the traffic flows.

*5.4. ML-Based Decision-Making in IoV.* In recent years, Autonomous Vehicle (AV) growth generates a novel tendency to implement several intelligent approaches and methods to enhance adaptive decision-making efficiency

and quality. The combination of AI, ML, RI, and IoV offers high-efficient control systems that can be exploited in various applications to accommodate more adaptive, automatic, and robust embedded systems [46]. Decision-making in IoV networks requires intelligent algorithms to handle the processes related to driving environment perception, path planning, strategy network control, and resource management. For an intelligent driving vehicle system, a module that integrates the path, behavior, and motion planning is needed to operate in a highly optimized decision-making algorithm. In addition, the decision-making algorithm must take into account the operations of vehicle control. It must be able to predict and learn the information related to vehicle platform faults, trajectory, and energy [47]. These considerations deal with vehicles' platform, as shown in Figure 8. For cognitive driving, localization, semantic understanding, and sensor fusion contribute to the decision-making process.

Furthermore, the intelligent vehicles and IoV systems' applications face the decision-making challenges associated with collecting and distributing IoV big data to vehicles and interested users to enhance road intelligence experience, in addition, in making decisions related to traffic managing, road congestion, and safety. Huge volumes of big data require a more robust and intelligent mechanism in decision-making procedures to reduce road congestion and improve traffic operations in addition to challenges related to useful communication links between different types of vehicles and smart devices and security and privacy problems [48]. Many machine learning methods can be used to contribute to solving the above challenges where these methods enable to model channels in different IoV network scenarios. In addition, it provides intelligent solutions to avoid road accidents by smart learning and analysis of the driving environment using the data collected from the sensors since IoV networks are interested in exchanging messages everywhere and sharing content between smart vehicles [49]. ML-based smart resource management for IoV networks has become crucial to decide the policy of the connection method of power control, selection, and resource allocation and assignment.

*5.4.1. Network Control.* Higher IoV network performance demands efficient solutions for network operation and optimization. ML in the network domain will leverage ML abilities for new network management for IoV applications. The capabilities of ML will provide an efficient way for intrusion detection and performance prediction. Besides, ML enables the IoV network to make intelligent decisions for network scheduling, and adaptation depends on network characteristics and environment [50]. ML algorithms will facilitate the IoV network to classify and predict traffic patterns and network states. In general, the use of ML in communication networks promises to achieve many solutions for different networking aspects, i.e., data collection and analysis, clustering decision-making and prediction, and model construction validation, in addition to network deployment and interference, as shown in Figure 9 [51]. Because of the IoV characteristics, which depend on the Internet, data and traffic prediction, analysis, and classification are the most critical aspects related to IoV network control.

*(1) Traffic Prediction*. Data collection and analysis are related to collecting a large amount of representative network data and the ability to characterize the network factors. Based on the IoV application, data collection can be gathered from different network layers. According to the IoV network state, offline data collection with high quality is required for data analysis, while online data collection will enable learning network performance and adaptation [52]. For IoV critical applications, data analysis needs to find a proper network feature, i.e., to predict the best network traffic performance by analyzing the historical data. Data collection and analysis need to prepare network data by normalization, discretization, and missing value completion. ML is an excellent choice to help extract the network feature. For IoV networks, ML plays an essential role in traffic prediction and network management [53]. Accuracy in traffic volume estimation in IoV networks is considered as one of the main factors that impact the performance analysis of network operations, i.e., resource allocation, network routing, congestion, and data streaming control.

*(2) Traffic Classification*. Traffic classification represents the need for IoV network applications to be matched with the Internet traffic flow. In IoV, the Internet traffic classification is an essential aspect of efficient network quality of service and quality of experience. Moreover, in the network edge, accurate Internet traffic classification is a critical challenge and an essential component of the network security domain. In this case, network traffic classification's importance is to recognize the vehicle network applications and control the traffic flow as needed to balance value or prioritize each other. In the security issue, traffic classifications provide a means of intrusions and malicious attack detection [53]. ML-based statistical features will give a classification scenario to the more realistic situation for IoV network traffic for network control and security. Moreover, it achieves efficiency, adaptability, and performance enhancement.

*(3) Traffic Management*. Other considerations related to network control are network traffic monitoring and management. In the IoV network, to ensure efficient network optimization, ML enables to adapt the dynamic Internet traffic in IoV and maximize the QoS/QoE without compromising end user experiences. ML provides an adaptation of real-time network conditions and maximizes the user experience [53]. ML can help to overcome the shortcoming of classical TCP congestion control algorithms by classifying a packet loss due to congestion or link errors. ML approaches will be easy to customize best-suited congestion control schemes that can adapt to unique network requirements. ML can systematically prospect important information from data held by vehicles and automatically identify very complex links, allowing vehicles to monitor

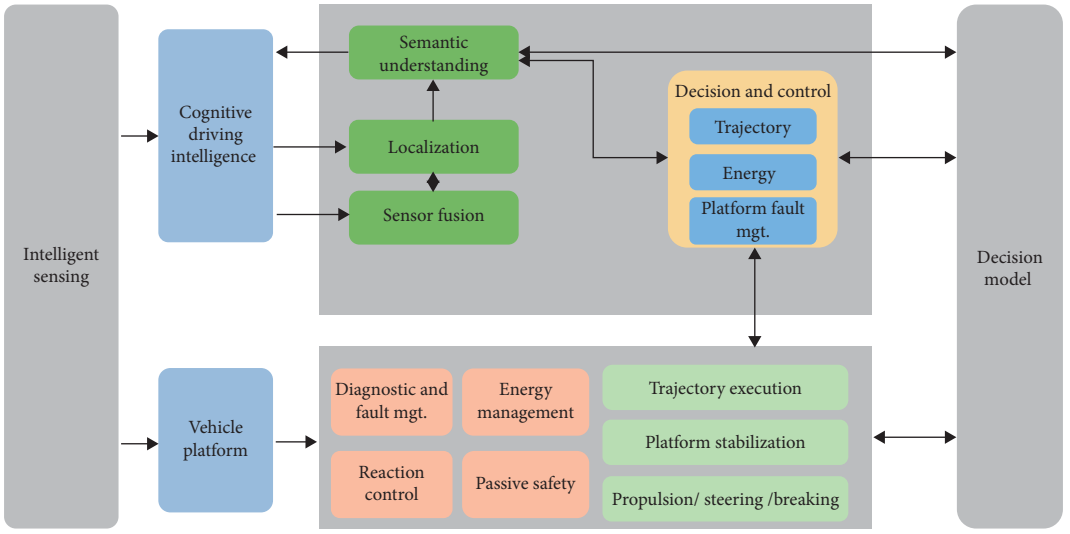


Figure 8: Intelligent driving vehicles' decision-making framework.

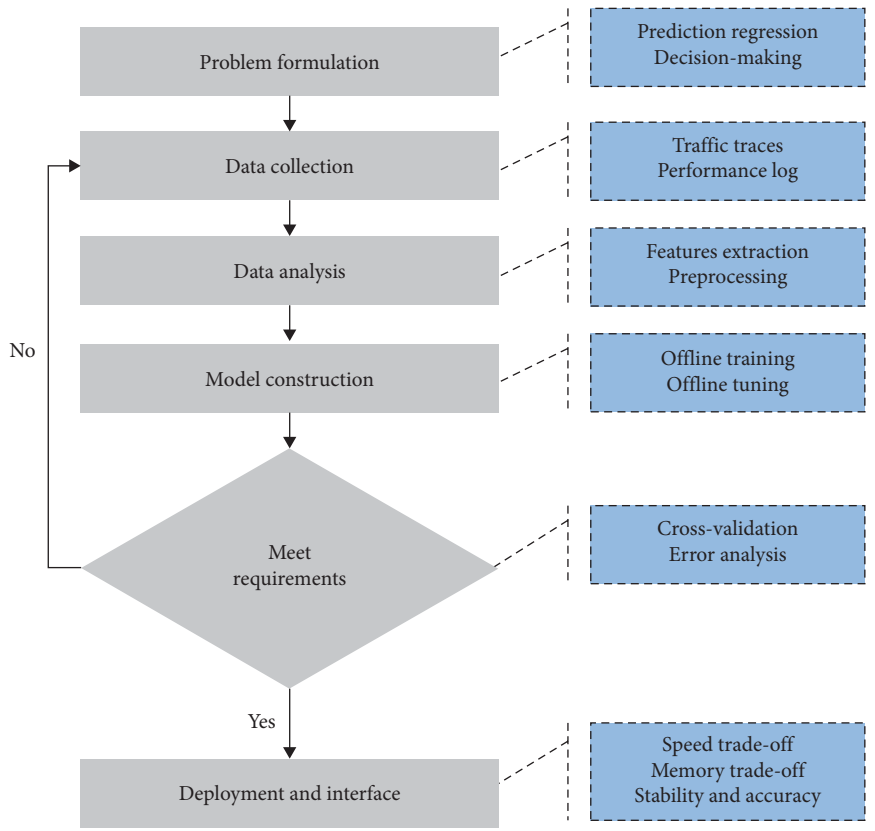


Figure 9: ML for the IoV network control cycle.

their environment intelligently and use data for training purposes [53, 54]. ML enables predicting and adapting to the evolution of environmental features, including wireless channel dynamics and traffic and mobility patterns, and configuring the network, which gives the high possibility to control and manage the network traffic.

Other ML solutions relate to developing accurate channel models in different environments and reducing path loss. These solutions lie in predicting IoV topology and treating severe interference from other IoVs using navigation data and vehicle connectivity. In IoV applications, Internet traffic may be impacted by the weakness of wireless communications [54]. ML technologies can assess wireless conditions without the need for a large number of datasets. Using ANNs' methods, an RSS prediction can be performed in an IoV environment.

*5.4.2. Location Prediction.* Automation is considered one of the essential advantages of the IoV network. The vehicles contain a perception system to be able to object detection and prediction. In most applications, vehicles' behavior depends on sensory data and the ability to classify the objects in the surrounding environment. These factors help develop autonomous vehicle applications using efficient vehicle behavior prediction and decision-making [55]. The intelligent prediction will help to optimize the decision-making of vehicle trajectories to avoid any risks. Self-driving and autonomous IoV depend on location prediction. The prediction requires information about the position of the vehicle itself and the behaviors of the surrounding vehicles, in addition to the road geometry and traffic rules. Different vehicle behavior prediction models are developed i.e., intention trajectory, maneuver-based, and interaction-aware models [56]. These kinds of models are categorized as input representation and output types' criterion, as shown in Figure 10. In recent years, researchers have tried to use the ML prediction methods to optimize location prediction precision.

ML uses recorded vehicle historical mobility patterns to predict the next location prediction according to mining trajectory patterns. This strategy is depending on the availability of enough historical trajectory data. To gain accurate prediction, ML provides an efficient method to get rid of the problem of suffering from the data sparsity and little historical trajectory and the impact of unknown dynamic contexts, traffic flows, and weather. ML enables the incorporation of this contextual information into the vehicle movement prediction. ML helps to model the contextual information characteristics between the trajectories and builds a learning model by integrating, for example, the neural network with the Long Short-Term Memory (LSTM) to predict the next location, as shown in Figure 11 [57]. The LSTM can easily incorporate heterogeneous features by integrating the trajectory variables to predict the following location effectively.

*5.4.3. Intelligent Resource Management.* Since IoV applications depend on the IoT, it is found that resource management in this technology is facing many challenges, especially in large-scale IoT networks. These challenges are related to massive channel access, power allocation, interference management, energy management, and coexistence between V2V or V2I and IoT traffic. Massive channel accessing causes overloads to networks and congestion [58]. For resource management, there is a need to develop proper load balancing and access management techniques. The crowded vehicles traveling over the roads make interference problems which requires efficient power allocation and interference management techniques. In the IoV, the IoT's nature is characterized by continuous data traffic, which leads to high energy consumption. Moreover, the harmonious coexistence between the V2V or V2I-existing networks and IoT traffic requires intelligent resource management [58, 59]. ML algorithms play an essential role in addressing the mentioned challenges related to resource management.

ML can make classification, regression, and density estimation for intelligent resource management to exploit data traffic and develop automated solutions for IoV services. ML provides the intelligent prediction for unknown IoV system parameters and system behavior, i.e., RL can control system actions from anonymous monitored system behavior during network activities. Moreover, ML provides suitable solutions for helping careful channel and power allocation and extracts the network parameters to make decisions for CSI, traffic characteristics, and demands of the vehicle's users [59]. Deep learning promises smart solutions to characterize the inherent relationships between the IoV system input and output to develop a traffic control system to optimize the network management and scheduling adaption [50]. This will help to optimize the IoV network QoE.

Another consideration related to the ML use in resource management is maximizing the overall network capacity and guaranteeing the best QoS. $Q$-learning can attain a substantial regulation and strategy by utilizing the network learning policy to accomplish smart resource control, assignment, and management with the continuous valued activities. It can be employed to obtain an optimal resource allocation approach in V2V communications to maximize the long-term expected accumulated discounted rewards, where the $Q$ function is approximated by a deep neural network [50]. The following equation can find the optimal policy with $Q$ values:

$$Q_{\text{new}}(s_t, a_t) = Q_{\text{old}}(s_t, a_t) \cdot + \alpha\left[r_{t+1} + \gamma \max_{s\varepsilon S} Q_{\text{old}}(s_t, a_t) - Q_{\text{old}}(s_t, a_t)\right]. \tag{3}$$

The observed state is represented by $s\varepsilon S$, where $S$ represents the state space, $t$ denoted for time, $s_t$ is an agent state, and $a_t$ represents action. The $Q$-learning can be deployed by what is known as Actor-Critic (AC) learning algorithm which is discussed in [50] by (Wang in 2017). The frame of AC learning consists of actor and critic parts which are responsible for control strategy adoption with action selections based on the tested network status and the entered policy of the environment parameter reward function, respectively, as shown in Figure 12. This mechanism enables the IoV vehicles to make decisions based on their learned policy strategy [60]. Each of IoV communication link will observe the current network state, i.e., resource block allocation, channel quality, and QoS requirements to enable selection of actions related to resource block assignment and power level according to the policy strategy to provide a new IoV network state.

## 6. Machine Learning Applications in IoV

ML contributes to many IoV applications related to emergent message transmission for road safety and dangerous activities. In addition, ML provides new smart solutions for IoV services and entertainment. To minimize the overall energy consumption of the computational facilities and vehicles, while satisfying the delay constraint for

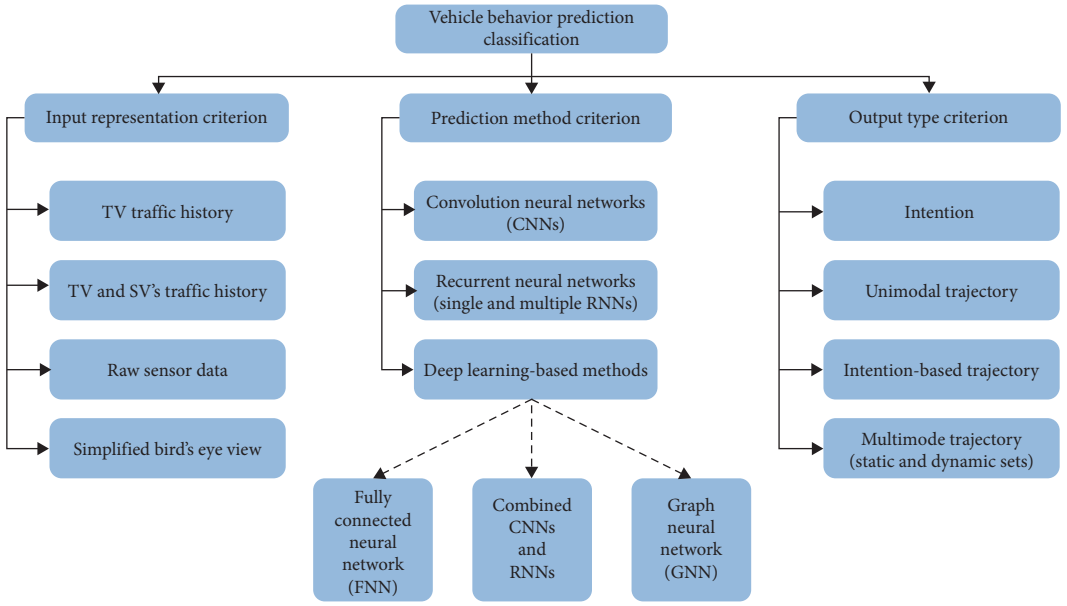


Figure 10: IoV behavior prediction models.

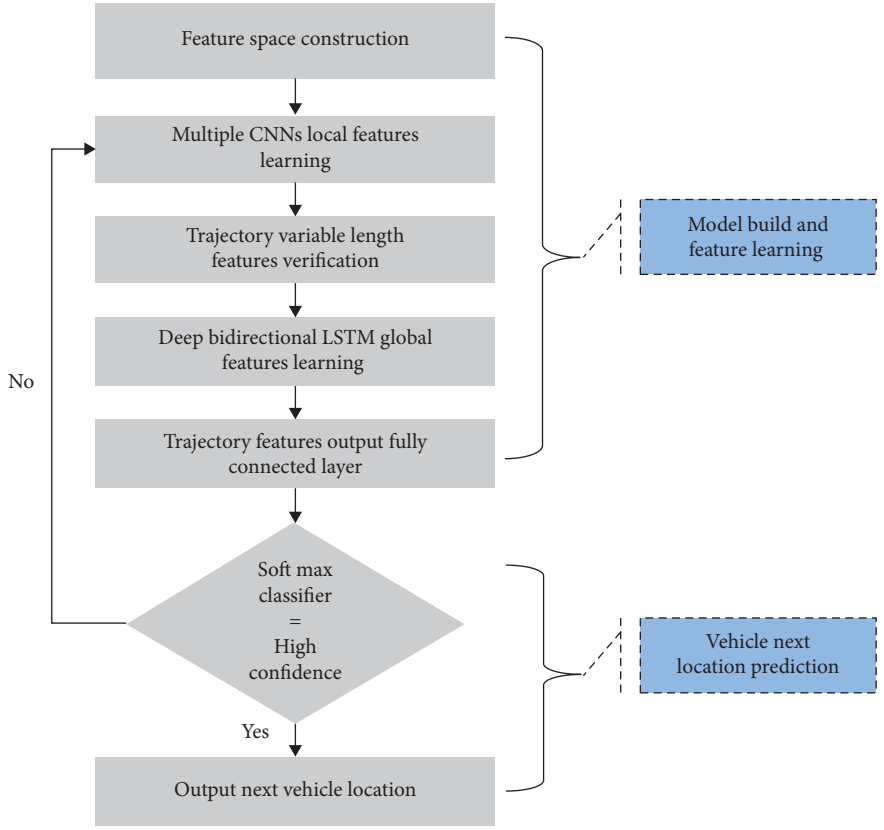


Figure 11: ML algorithm flowchart for IoV location prediction [56].

traffic offloading, ML technology in data mining, pattern recognition, processing, and cognitive computing is an alternative for decision making, which will open new opportunities for intelligent IoV networks, i.e., in driver safety, smart transportation, and autonomous driving applications.

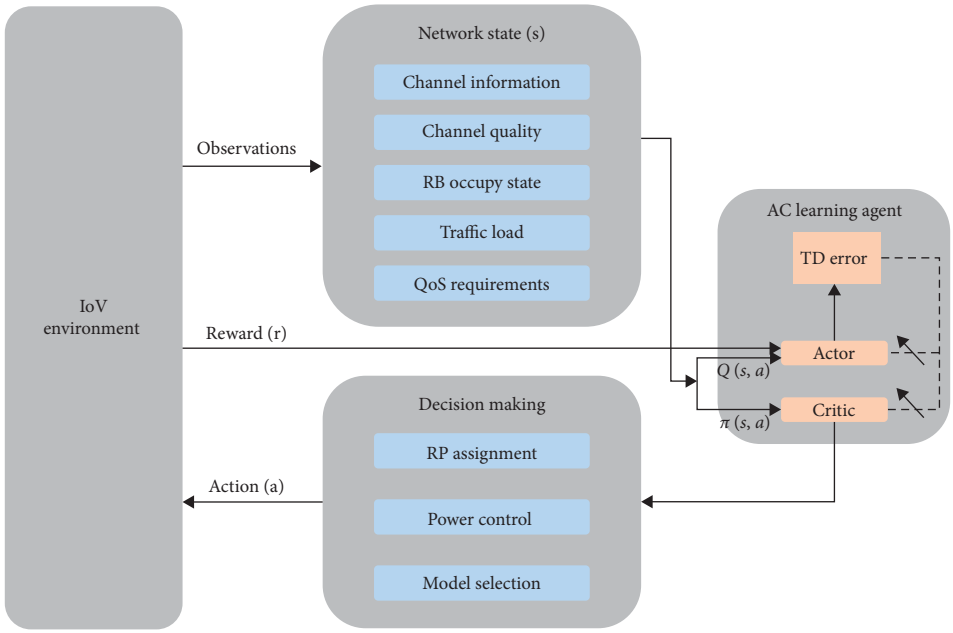


Figure 12: AC learning algorithm for IoV resource management [60].

*6.1. Intelligent Autonomous Driving.* Machine learning plays a vital role in vehicle intelligent driving applications, making vehicles perceive and estimate to manage the vehicle driving system efficiently. ML makes the vehicles self-automated which will improve the society by reducing road accidents. In general, self-driving vehicles are very closely associated with IoV. The combination of the IoT with ML and smart computing will provide an intelligent driving system. Machine learning algorithms in self-driving enable IoV to predict the possible changes in the surrounding driving environment and provide different tasks i.e., object detection and identification, in addition to prediction of another vehicle's localization and movement [61]. Many ML algorithms can be used to provide the mentioned tasks. Regression algorithms provide a localization scheme to develop prediction and feature selection models for self-driving vehicles. Clustering algorithms provide a way to model approaches such as centroid-based and hierarchical for intelligent localization [61, 62]. Decision matrix algorithms will help identify, analyze, and rate the performance of relationships between sets of values and information for intelligent decision-making.

To enable self-driving vehicles, intelligent decision-making must process streams of observations coming from different vehicle devices, such as cameras, radars, LiDAR's, ultrasonic sensors, GPS units, and sensors. The information gathered by these sources helps the vehicle's ML-based computer to make driving decisions, as presented in the study proposed by Hussain (2020) [58]. Decision-making can take place by the modular perception-planning-action or by the End2End learning fashion. The modular perception-planning-action uses the AI and deep learning methodologies to make various learning and nonlearning-based components. End2End learning is based on deep learning which performs the direct mapping from sensory data to control commands. End2End learning can also be formulated as a backpropagation algorithm scaled up to complex models [63]. Such deep learning-based algorithms will be able to find a route between the vehicle start position and the desired location, which represents path planning. It is able to consider all possible obstacles present in the surrounding environment and find out a trajectory free of the collision route.

*6.2. Deep Learning for Driver Safety and Assistance.* Due to the increasing number of accidents and the urgent need to reduce road accidents and improve traffic safety, modern vehicles are equipped with sensors and connected to high-speed mobile communication networks. The vehicle sensors allow collecting a large amount of data used in vehicle safety analysis procedures. The data are analyzed in real time by AI algorithms in the autonomous driving systems' applications to reach a high level of safety through several designs. It enables the designing of the road safety index and its prediction of parameters such as street engineering, human behavior, and traffic flow. The description of road safety by deep learning will predict the real-time road safety index based on the deep dense neural network. Moreover, ML helps to learn the association between visual entities and city characteristics to estimate road safety based on image processing [64]. The extraction of associations between captured pictures and estimated road safety with multiple cross-domain factors can achieve high prediction accuracy of the road safety index (SI). The real-time road safety index estimation will enhance vehicle safety. The road SI can be defined as a number used to inform the public about the area's safety, as published by Abdallah in 2018 [65]. The safety index can be calculated based on the traffic accident rate per 100,000 inhabitants Ra as follows:

$$SI = (1 - Ra) * 100. \quad (4)$$

Driver Assistance Systems (ADAS) are quickly being established for self-directed vehicles which are considered driver safety and assistance methods. ML and embedded computing are considered the main driving factors enabling the development [65]. ML will enable driver assistance systems to perceive obstacles, objects, lanes, pedestrians, and other cars and predict obstacle trajectories and targets. ML helps to detect and to track the obstacle to avoid collision and for path planning. Vehicle camera-based deep learning improves quality enhancement and cost reduction of blind spot prediction rather than radar [66], as proposed by Ball and Tang (2019). It uses a lightweight and computationally effective Neural Network (NN).

*6.3. ML in Smart Transportation.* Intelligent transport is one of the most important vehicle Internet applications, as it covers several applications including improving track, parking lots, avoiding and detecting accidents, and other applications related to infrastructure. ML technologies serve to develop advanced models of ITS. In general, traffic congestion is one of the most important problems faced by transportation systems in urban areas, especially in cities that contain high vehicle density [67]. The use of ML with smart transport systems provides optimization for traffic network configuration. Another smart transportation application in modern cities is parking. Smart cities try to find an intelligent parking method to provide reservation services and select parking for vehicles. IoT and ML technologies enable free parking methods. ML helps manage parking for different drivers. It can classify parking according to drivers' requirements, i.e., regular drivers or those with special needs. The IoT helps to exchange the mapping of parking information to the vehicles or for mobile users through cloud servers [68]. Moreover, IoT will improve traffic monitoring, live location streaming, and vehicle performance monitoring.

Since the IoV network consists of multiple types of smart vehicles, transport data processing of these numerous vehicles in real time requires an intelligent schedule and data processing mechanism [68]. Distributed systems provide an efficient and fast method for such a situation. This needs to deal with big transportation data collected from heterogeneous sources of database solutions. ML-based SQL database enables smart database queries and flow data processing. ML will allow the balance between the algorithms' accuracy and the size of the data and determine the circumstances in which it becomes useful to implement distributed systems. For transportation route optimization, ML provides reliable predictions to make routing decisions [69]. ML enables a clear understanding of available route options, associated energy, and environmental costs in real time. ML provides predictability of changes that can help convoy operators choose vehicles and methods that save fuel costs, while maximizing efficiency [70].

## 7. Secure Vehicular Network towards 6G

Cyber-physical security is one of the hot research areas in the Internet of Things, which is also a thoughtful subject in vehicular communication. The attack and malicious activities of vehicular networks cause thoughtful damage that threatens passengers' safety in vehicles and affects network performance. The vehicular systems usually need many severe strains in the ML-based security scheme. The precise restraints of the vehicular system can be presented as follows.

*7.1. Vehicle Speed.* One of the most critical parameters of the vehicular system is the high mobility of vehicle nodes and the network dynamics. Communications between nodes regularly go down, making the system security and authentication quite hard [71]. The system traffic is abruptly flapping with the rapid change and dynamic of the network topology which seriously disturbs the intrusion detection and security algorithm and schemes of the packets [72]. Additionally, the vehicle speed results in the random mobility of vehicles, which delays and disturbs the performance of the security and authentication data exchange.

*7.2. Diversity Framework.* The Vehicule-to-Vehicle (V2V) topology is structured with different nodes and a dynamic network, which is implanted with various network resources. The main challenge is to study the different resources among vehicles to guarantee security and authentication schemes. As an instance, in the storage-constrained, processing, and energy vehicular system, the challenge is to optimize and capitalize the security guarantee which can be resolved by neural network or fuzzy logic or game theory [73].

*7.3. Network Size.* The volume of the Internet of vehicular nodes grows rapidly. Thousands of nodes in vehicles are probable to be linked to the huge IoT network in near future [74]. Though, no present worldwide group or body offers security for such a huge rapidly changing network. Additionally, the growing volume of the Internet of Vehicular network grows both the processing and network protocol that lead the growing security protocol traffic, which grows the error detection and network latency.

*7.4. Confidentiality Obligation.* Always there is a compromise between privacy and security in the Internet network, especially in IoT and IoV. In IoV, vehicle nodes' authentication and confidentiality are usually designed and modeled by security algorithms. Without data privacy assurance, the security scheme is usually hungry for resources to distinguish and differentiate anomaly and error from flow data [75].

*7.5. Fast Response Prerequisite.* Unlike legacy networks, the Internet of vehicular networks needs an instantaneous handle to cope with the rapid and dynamic change network, i.e., news broadcasting, fast rescue, and avoidance of accidents. Such network needs fast response requirements for the Internet of vehicular network such as low-latency communication channels and real-time prevention of attack techniques [76]. To overcome these problematic issues, many solutions and mechanisms have been anticipated in the literature. Interfering and sniffing are two main vulnerabilities in IoV; Elliptic Curve Digital Signature Scheme (ECDSA) and vehicular Public Key Infrastructure (PKI) have been suggested to be the two primary intrusion techniques to guarantee privacy during communication from vexatious activities [46, 76].

Nevertheless, the vexatious activities include the pseudo spoofing, the wormhole attack, the packet drop attack, the Denial-of-Service (DoS) attack, the spurious data intrusions, and the reiteration intrusions that can counterfeit identity, broadcast junk packets, and kidnapping vehicle nodes to penetrate and stealth elliptic curve digital signature algorithm and public key infrastructure [77]. Many vexatious attitude recognition techniques have been invented [71, 73]. Some works suggest that infiltration and attacks can be drawn with machine learning techniques from rapid and high-diversity network traffic [75, 78]. The attack prevention mechanism for legacy networks is typically achieved by determining the normal state from flooding-emulated packets. In the highly rapid Internet of the vehicular network, the present emulated packets are not useful for innovative intrusions in such a dynamic environment. The legacy machine learning technologies, such as association rules, autoregressive, and classification, are widely used in the abovementioned works for intrusion detection. Recently, ML has proposed to be the promising machine learning and data mining utilities for enhancing the authentication, privacy, and attack prevention performance on the Internet of vehicular networks.

*7.6. Authentication Technology in the IoV.* Authentication algorithms for IoV networks are considered essential for network and communications' security purposes. Several studies dealt with the concept of certificates to determine the identity of vehicles. Other studies have used anonymous credentials and designated an unknown identity IoV area for the vehicle that allows access to it safely with the possibility of hiding the information. A hiding vehicle information mechanism is adopted by specifying the unknown identity to achieve safety against any attack by any malicious vehicle that tries to steal vehicle information in the IoV network [79]. Despite this mechanism's efficiency in maintaining the confidentiality of vehicle information, it is facing a delay issue in processing identity and is wasting a large amount of identity storage resources. Finding an effective anonymous authentication method in IoV, while reducing its computational cost is a big challenge. AI mechanisms can provide solutions to improve the anonymous authentication system by reducing account costs through a contextual tracking mechanism to manage IoV network vehicles and units on the roadside. Liu et al. (2018) proposed a mechanism based on the safe communication between vehicles and units on the side of the road using machine learning technology [80]. The study relies on creating a Certified Short Signature Model (CLSS) that works with the regional management strategy to design an anonymous and efficient anonymous authentication scheme for IoV. The study achieves a highly efficient model in terms of the interaction between vehicles and roadside units compared to traditional plans. The proposed CLSS scheme is secure under adaptively chosen message and ID attacks in the random oracle model.

On the contrary, issuing identity certificates to enable privacy protection is more efficient. Still, it is the responsibility of the RSU, which increases the operating cost and causes the greater consumption of network resources to operate and configure RSU. In addition, the resource management processes related to vehicle verification and requesting authentication take a lot of time [80]. Aggregated authentication technology can reduce time delay, but it also contains frequent authentication problems and requires a large amount of authentication information. An authentication protocol is known as Distributed Aggregate Privacy-Preserving Authentication (DAPPA), proposed by Zhang (2017), enables to authenticate the vehicles in the vehicular network by providing a multiple trusted authority based on an identity-based aggregate signature mechanism [81]. The aggregation of vehicle signatures in one of the verified messages reduces storage needs and resource management costs. A smart adaptive data aggregation study by Islam et al. (2016) presents a method to enable data communication between distributed mobile vehicles on vehicles unknown to other vehicles or IoV locations [82]. The adaptive data aggregation depends on machine learning to analyze data and extract information for the drivers, enabling fully automated switching of different vehicle sensors and data fusion processes' adaptation.

In general, the AI technologies in IoV develop secure management processes and achieve intelligent, fast authentication and progressive authorization. AI enables to provide a light authentication scheme in addition to a comprehensive authentication and authorization system. Machine and deep learning can enhance IoV security by investigating valuable information and providing self-adaptation for certification and authorization. In IoV channel communication, the Support Vector Machine (SVM) enables developing a lightweight authentication system to identify vehicles based on their pseudorandom arrival in the time domain or the frequency range via multiple sensors. Hasan et al. (2020) provided a fast authentication mechanism for large-scale IoV that depends on the identical unique Pseudo-Random Binary Sequence (PRBS) for vehicle access time slots or access frequencies [83]. This mechanism can be used to verify the authentication of vehicles to the IoV network base station access. Figure 13 shows the possible lightweight authentication scheme based on SVM for IoV secure authentication.

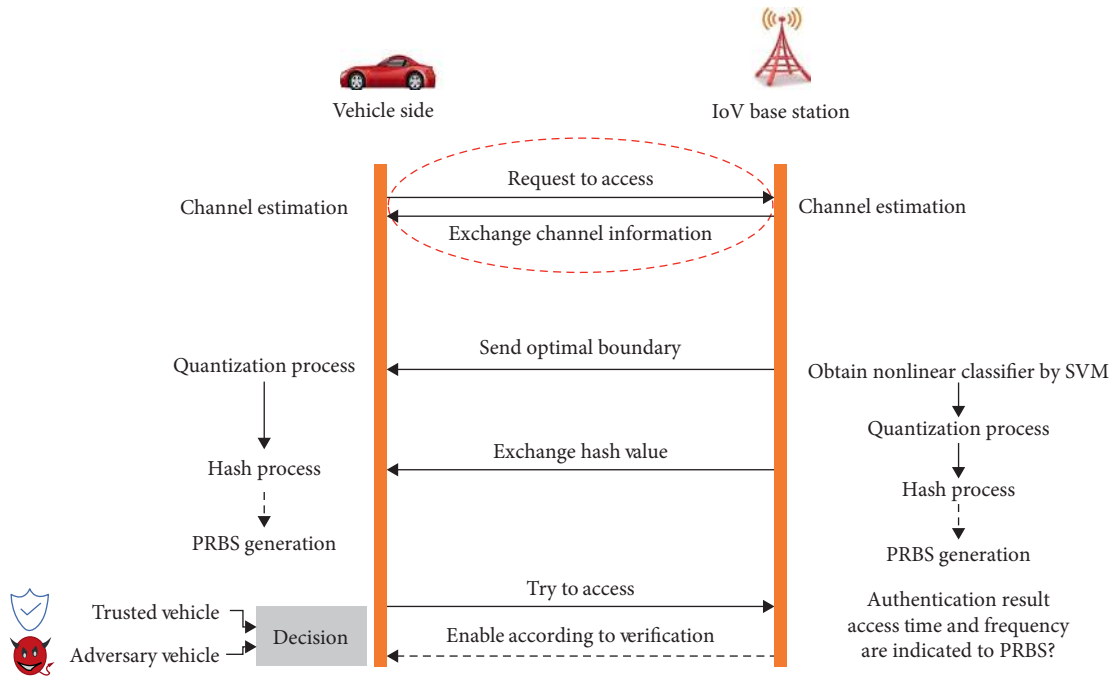


Figure 13: IoV authentication scheme based on the SVM.

The decisions taken by the SVM are a function of the support vector machine network. The output decision is according to several linear combinations of the middle layer nodes. The layer nodes correspond to the inner product between the input sample and support vector that enables the selection of the most suitable optimized communication mode [83]. This module provides a fast authentication scheme by directly specifying access times or frequencies and the progressive protection of trusted communications without the need for a complex account. The PRBS between each vehicle and the gateway can be obtained by utilizing their unique features by the SVM. The PRBS between each vehicle and the IoV base station can be obtained by utilizing their unique features based on the SVM. The selected features are measured by channel information estimation. The separation between the dense data and sparse data is enabled by an SVM-based quantization technique. This technique reduces the wrong decisions by diminishing the measurements near the boundary [84]. The lightweight authentication scheme based on the SVM ensures higher similar binary sequences acquired on both IoV base stations and vehicles because of the channel reciprocity.

*7.7. Fog-Based Identity Authentication.* In IoV applications, the fog-computing concept reduces the burden on the traffic control center. All computing components in IoV, i.e., the roadside and vehicle units, are well suited to the concept of fog computing and enable the communication and interaction between vehicles and clouds [85]. Due to several fogs' possibility, the vehicle identification certification system's security is essential to enhance the security issues related to the fog nodes. The fog-based identity authentication scheme presented by Song (2020) provides two authentication levels: vehicles outside the fog and the other for the security monitoring of the rest of the vehicles. The scheme uses deep learning for security monitoring to conduct real-time security in the IoV [86].

A reliable and secure IoV fog mechanism based on machine learning develops access security authentication and security timing detection for vehicles that need to join IoV. When using vehicle safety certification and timing detection mechanisms, it is very important to pay attention to the fog head replacement frequency to reduce resource consumption and time delay and detect the manufactured vehicles to access the fog legitimately [87]. AI-based coding algorithms provide intelligent solutions that ensure the exchange of information for vehicles that leave and join the IoV fogs. Machine learning technologies enable the detection of malicious vehicles that use legal personalities to join the fog. In general, most current fog-based IoV security mechanisms, such as authentication, encryption, and access control, are relatively weak solutions. AL and ML technologies provide a defensive scheme for the fog-IoV environment enabled to secure related operations such as activities monitoring, misuses identification, and threats and vulnerabilities detection in accessing processes [88–91].

Table 3 summarizes the key factors regarding secure IoV communications.

## 8. Future Directions and Potential Solutions

It is well known that artificial intelligence plays a vital role in most IoT applications that depend on perception and predictions of events. As one of these applications, IoV

Table 3: Summary for secure IoV communications.

| Year | Source | Approaches | Features | Advantages | Challenges | Citations |
|---|---|---|---|---|---|---|
| 2020 | IEEE | Fog-based identity authentication (FBIA) | Fog-based identity authentication scheme and deep learning | IoV real-time security monitoring | Dual authentication levels for access authentication and vehicles' timing detection | Song et al. [86] |
| 2020 | IEEE | SVM-based classifier | Authentication scheme based on SVM | Secure access frequencies and progressive protection of trusted communications | Fast authentication mechanism for large-scale IoV | Hasan et al. [83] |
| 2018 | IEEE | Certificateless Short Signature Scheme (CLSS) and ML | Anonymous authentication scheme-based ML | Secure communication between vehicles and roadside units | Security under adaptively chosen message and ID attacks | Liu et al. [80] |
| 2017 | IEEE | Aggregate privacy-preserving authentication protocol; Multiplicative Secret Sharing (MSS) technique | Distributed aggregate signature mechanism | Secure vehicular network authentication and trusted authority | Trade-off between security and storage resource management | Memon et al. [81] |
| 2016 | Elsevier | Smart Adaptive Data Aggregation (SADA); machine learning-based data fusion and analysis | Adaptive data aggregation-based ML | Secure data exchange between vehicles | Fully automated switching to unknown vehicle | Islam et al. [82] |

networks require the development of smart algorithms to manage intelligent technology, such as self-driving cars. Self-driving cars are a high-risk test for machine learning authorities, as well as a test case for social learning in technology management [92–96]. In IoV applications, the convergence between machine learning and the Internet of Things promises future progress in efficiency, accuracy, and improved resource management. The use of machine learning with IoV provides high performance in communication and computing to achieve efficient control, management, and decision-making processes [92, 97]. ML allows the extraction of big sensory data to get better insights into the range of problems associated with the IoV and the surrounding environment and the ability to make critical operational decisions. It also promises soon to upgrade vehicle networks' performance and make them more interactive with other things' Internet applications. Using ML in the IoV enables interaction between the cyber and physical components together and can significantly improve the efficiency and reliability of processes and systems [97]. Moreover, machine learning offers smart solutions to enhance decision-making in the event of cyber attacks.

ML provides solutions for many ITS applications, especially in 2D level realization and forecasting. However, it can develop AI techniques that can develop collaborative mobility applications based on the description of realistic 3D objects and 4D perception for autonomous driving [98]. For different IoV applications, such as driving managements, route, and localization prediction, smart ITS camera devices can create holograms to provide 3D object visualization. Due to the hybrid ITS context, the combination of data from different resources to improve 3D visualization accuracy is an exciting potential solution and critical future research direction. The 5G of the IoV network is expected to provide some AI technologies to provide network management completely smart and provide innovative services [89, 90]. However, the Sixth Generation (6G) is expected to pack machine learning techniques an essential role in its operation through self-reconfiguration on demand to ensure a doubling in network performance and service types [99]. ML techniques can provide the 6G network model that can rapidly respond to IoV management processes by learning in real-time the network's state.

## 9. Conclusion

Machine learning (ML) helps analyze big data in IoV networks, enabling intelligent forecasting and decision-making. Various potential applications have been indicated for the use of ML to improve the performance of IoV networks. ML technologies offer beneficial solutions in addressing congestion problems in high-density IoV networks to achieve quality services and experience. Moreover, the scope of employing machine-learning technology in network management and control, data flow, site forecasting, and resource tools across different layers of communication networks were discussed. In general, we find that, in most automated learning applications, performance depends on the amounts of data available and that must be large enough. Recently, parallel computing capabilities and machine learning methods have been developed to build smart integrated systems for IoV networks. This development can build intelligent systems with immense parallel processing capabilities and energy efficiency to prepare solutions for various operations associated with the IoV, such as multi-dimensional signal/image processing and wireless communications.

## Data Availability

Data used to support the findings of this study are already available in the manuscript.

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

## Acknowledgments

This work was supported by the research grant Universiti Kebangsaan Malaysia (UKM) under Grant nos. FRGS/1/2020/ICT03/UKM/02/6 and DIP-2018-040.

## References

[1] W. Tong, A. Hussain, W. X. Bo, and S. Maharjan, "Artificial intelligence for vehicle-to-everything: a survey," *IEEE Access*, vol. 7, pp. 10823–10843, 2019.

[2] H. Yang, A. Alphones, Z. Xiong, D. Niyato, J. Zhao, and K. Wu, "Artificial intelligence-enabled intelligent 6G networks," 2019, https://arxiv.org/abs/1912.05744.

[3] A. A. Eltahir, R. A. Saeed, A. Mukherjee, and M. K. Hasan, "Evaluation and analysis of an enhanced hybrid wireless mesh protocol for vehicular ad-hoc network," *EURASIP Journal on Wireless Communications and Networking*, vol. 1, pp. 1–11, 2016.

[4] Y. Dai, "Artificial intelligence empowered edge computing and caching for internet of vehicles," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 12–18, 2019.

[5] H. Ji, "Artificial intelligence-empowered edge of vehicles: architecture, enabling technologies, and applications," *IEEE Acces*, vol. 8, pp. 61020–61034, 2020.

[6] A. H. Sodhro, Z. Luo, G. H. Sodhro, M. Muzamal, J. J. P. C. Rodrigues, and V. H. C. de Albuquerque, "Artificial Intelligence based QoS optimization for multimedia communication in IoV systems," *Future Generation Computer Systems*, vol. 95, pp. 667–680, 2019.

[7] M. B. Hassan, E. S. Ali, R. A. Mokhtar, R. A. Saeed, and B. S. Chaudhari, "NB-IoT: concepts, applications, and deployment challenges, book chapter (ch 6)," in *LPWAN Technologies for IoT and M2MApplications*, B. S. Chaudhari and M. Zennaro, Eds., Elsevier, Berlin, Germany, 2020.

[8] Y. Dai, D. Xu, S. Maharjan, G. Qiao, and Y. Zhang, "Artificial intelligence empowered edge computing and caching for internet of vehicles," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 12–18, 2019.

[9] E. S. A. Ahmed and R. A. Saeed, "A survey of big data cloud computing security," *International Journal of Computer Science and Software Engineering (IJCSSE)*, vol. 3, no. 1, pp. 78–85, 2014.

[10] Z. K. A. Mohammed and E. S. A. Ahmed, "Internet of things applications, challenges and related future technologies," *WSN*, vol. 67, no. 2, pp. 126–148, 2017.

[11] H. Wu, "Developing vehicular data cloud services in the IoT environment," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1587–1595, 2014.

[12] Z. E. Ahmed, M. K. Hasan, R. A. Saeed et al., "Optimizing energy consumption for cloud internet of things," *Frontiers of Physics*, vol. 8, p. 358, 2020.

[13] M. K. Hasan, A. F. Ismail, A.-H. Abdalla, H. A. M. Ramli, W. Hashim, and S. Islam, "Throughput maximization for the cross-tier interference in heterogeneous network," *Advanced Science Letters*, vol. 22, no. 10, pp. 2785–2789, 2016.

[14] A. H. Sodhro, "Artificial Intelligence based QoS optimization for multimedia communication in IoV systems," *Future Generation Computer Systems*, vol. 95, pp. 667–680, 2019.

[15] Y. Mao, "A survey on mobile edge computing: the communication perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.

[16] J. Xu, "Joint service caching and task offloading for mobile edge computing in dense networks," in *Proceedings of the IEEE Conference on Computer Communications*, Honolulu, HI, USA, 2018.

[17] Y. Cao, "An EV charging management system concerning drivers' trip duration and mobility uncertainty," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 4, pp. 596–607, 2016.

[18] S. Islam, A.-H. A. Hashim, M. H. Habaebi, and M. K. Hasan, "Design and implementation of a multihoming-based scheme to support mobility management in NEMO," *Wireless Personal Communications*, vol. 5, no. 2, pp. 457–473, 2017.

[19] N. S. Nafi, M. K. Hasan, and A. H. Abdallah, "Traffic flow model for vehicular network," in *Proceedings of the 2012 International Conference on Computer and Communication Engineering (ICCCE)*, pp. 738–743, IEEE, Kuala Lumpur, Malaysia, 2012.

[20] M. Abdallah, "Softwarization, virtualization, and machine learning for intelligent and effective V2X communications," 2006, https://arxiv.org/abs/2006.04595.

[21] Z. El-Rewini, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, 2020.

[22] H. M. Furqan, "Intelligent physical layer security approach for V2X communication," 2019, https://arxiv.org/abs/1905.05075.

[23] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP—Sybil attacks detection in vehicular ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 582–594, 2011.

[24] S. So, "Physical layer plausibility checks for misbehavior detection in V2X networks," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, WiSec'19*, Miami, FL, USA, May 2019.

[25] W. Li and H. Song, "ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2016.

[26] J.-P. Monteuuis, "My autonomous car is an elephant": a machine learning based detector for implausible dimension," in *Proceedings of the Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)*, Shanghai, China, 2018.

[27] M.-J. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS ONE*, vol. 11, no. 6, Article ID e0155781, 2016.

[28] M. Akhtaruzzaman, M. K. Hasan, S. R. Kabir, S. N. H. S. Abdullah, M. J. Sadeq, and E. Hossain, "HSIC bottleneck based distributed deep learning model for load forecasting in smart grid with a comprehensive survey," *IEEE Access*, vol. 8, pp. 222977–223008, 2020.

[29] S. Hu, "A fuzzy QoS optimization method with energy efficiency for the internet of vehicles," *Advances in Networks*, vol. 4, no. 2, pp. 34–44, 2016.

[30] S. Islam, A. H. Aisha-Hassan, R. A. Saeed et al., "Mobility management schemes in NEMO to achieve seamless handoff: a qualitative and quantitative analysis," *Australian Journal of Basic and Applied Sciences*, vol. 5, no. 6, pp. 390–402, 2011.

[31] C.-F. Lai, "A buffer-aware QoS streaming approach for SDN-enabled 5G vehicular networks," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 68–73, 2017.

[32] R. A. Saeed, R. Mokhtar, and S. Khatun, "Spectrum sensing and sharing for cognitive radio and advanced spectrum management," *ICGST International Journal on Computer Networks and Internet Research (CNIR)*, vol. 9, no. 2, pp. 87–97, 2009.

[33] H. Park and Y. Lim, "Reinforcement learning for energy optimization with 5G communications in vehicular social networks," *Sensor*, vol. 20, no. 8, p. 2361, 2020.

[34] E. Bozkaya and B. Canberk, "Software-defined management model for energy-aware vehicular networks," *EAI Endorsed Transactions onWireless Spectrum*, vol. 3, no. 11, Article ID 152099, 2017.

[35] Y. Zhao, "A survey of networking applications applying the software defined networking concept based on machine learning," *IEEE Access*, vol. 7, pp. 95397–95417, 2019.

[36] T. n. Nguyen, "The challenges in ML-based security for SDN," in *Proceedings of the 2nd Cyber Security in Networking Conference (CSNet)*, Paris, France, 2018.

[37] K. F. Hasan, "Cognitive internet of vehicles: motivation, layered architecture and security issues," in *Proceedings of the International Conference on Sustainable Technologies for Industry 4.0 (STI)*, Bangladesh, India, 2019.

[38] C. Chen, "A rear-end collision prediction scheme based on deep learning in the internet of vehicles," *Journal of Parallel and Distributed Computing*, vol. 117, pp. 192–204, 2017.

[39] L. T. Tan and R. Q. Hu, "Mobility-aware edge caching and computing in vehicle networks: a deep reinforcement learning," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 10190–10203, 2018.

[40] Z. Chang, "Learn to cache: machine learning for network edge caching in the big data era," *IEEE Wireless Communications*, vol. 25, no. 3, pp. 28–35, 2018.

[41] Z. Ning, "Deep reinforcement learning for vehicular edge computing: an intelligent offloading system," *Transactions on Intelligent Systems and Technology*, vol. 10, no. 6, 2019.

[42] H. Zhang, "Deep reinforcement learning-based offloading decision optimization in mobile edge computing," in *Proceedings of the IEEE Wireless Communications and Networking Conference(WCNC)*, Marrakesh, Morocco, 2019.

[43] J. Wang, "Vehicular edge computing: a deep reinforcement learning approach," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4192–4203, 2018.

[44] H. Ye, "Machine learning for vehicular networks: recent advances and application examples," *IEEE Vehicular Technology Magazine*, vol. 13, no. 2, 2018.

[45] W. K. Lai, "A machine learning system for routing decision-making in Urban vehicular ad hoc networks," *International Journal of Distributed Sensor Networks*, vol. 11, no. 3, Article ID 374391, 2015.

[46] K. Hamid, "Artificial intelligence and internet of things for autonomous vehicles," *Nonlinear Approaches in Engineering Applications*, Springer, 2020.

[47] J. Li, *Survey on Artificial Intelligence for Vehicles; Automotive Innovation*, Springer, Berlin, Germany, 2018.

[48] C.-Y. Fana, "Using machine learning to forecast patent quality–take "vehicle networking" industry for example," *Transdisciplinary Engineering: A Paradigm Shift*, vol. 5, 2017.

[49] J. Gu, "Introduction to the special section on machine learning-based internet of vehicles: theory, methodology, and applications," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, 2019.

[50] M. Wang, "Machine learning for networking: workflow, advances and opportunities," *IEEE Network*, vol. 32, no. 2, pp. 92–99, 2017.

[51] J. de Hoog, "Improving machine learning-based decision-making through inclusion of data quality," in *Proceedings of the BNAIC/BENELEARN Computer Science*, Brussels, Belgium, 2019.

[52] J. Zerillil, "Algorithmic decision-making and the control problem," *Minds and Machines*, vol. 29, pp. 555–578, 2019.

[53] M. Usama, "Unsupervised machine learning for networking: techniques, applications and research challenges," *IEEE Access*, vol. 7, pp. 65579–65615, 2019.

[54] S. Petros, "A survey on machine-learning techniques for UAV-based communications; MDPI," *Sensors*, vol. 19, no. 23, p. 5170, 2019.

[55] S. Mozaffari, "Deep learning-based vehicle behavior prediction for autonomous driving applications: a review," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–15, 2019.

[56] X. Fan, "A deep learning approach for next location prediction," in *Proceedings of the 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design*, Nanjing, China, 2018.

[57] H. Jiang, "Trajectory prediction of vehicles based on deep learning," in *Proceedings of the 4th International Conference on Intelligent Transportation Engineering*, Singapore, 2019.

[58] F. Hussain, "Machine learning for resource management in cellular and IoT networks: potentials, current solutions, and open challenges," 2019, https://arxiv.org/abs/1907.08965.

[59] M. Chen, "Artificial neural networks-based machine learning for wireless networks: a tutorial," 2019, https://arxiv.org/abs/1710.02913.

[60] H. Yang, "Intelligent resource management based on reinforcement learning for ultra-reliable andLow-latency IoV communication networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4157–4169, 2019.

[61] R. Abduljabbar, "Applications of artificial intelligence in transport: an overview," *Sustainability*, vol. 11, no. 1, p. 189, 2019.

[62] Y. Xing, "Driver activity recognition for intelligent vehicles: a deep learning approach," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 5379–5390, 2019.

[63] S. Grigorescu, "A survey of deep learning techniques for autonomous driving," 2020, https://arxiv.org/abs/1910.07738.

[64] Z. Peng, "Vehicle safety improvement through deep learning and mobile sensing," *IEEE Network*, vol. 32, no. 4, pp. 28–33, 2018.

[65] M. Abdallah, "Machine learning techniques in ADAS: a review," in *Proceedings of the International Conference on Advances in Computing and Communication Engineering (ICACCE-2018)*, Paris, France, 2018.

[66] J. E. Ball and Bo Tang, "Machine learning and embedded computing in advanced driver assistance systems (ADAS)," *Electronics*, vol. 8, no. 7, p. 748, 2019.

[67] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and IoT in smart transportation," *Future Internet*, vol. 11, no. 4, p. 94, 2019.

[68] M. Veres and M. Moussa, "Deep learning for intelligent transportation systems: a survey of emerging trends," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 8, pp. 3152–3168, 2019.

[69] A. J. Howard, "Distributed data analytics framework for smart transportation," in *Proceedings of the IEEE 20th International Conference on High Performance Computing and Communications*, Exeter, UK, 2018.

[70] I. Lana, "From data to actions in intelligent transportation systems: a prescription of functional requirements for model actionability," 2020, https://arxiv.org/abs/2002.02210.

[71] H. Nakayama, A. Jamalipour, and N. Kato, "Network-based traitor-tracing technique using traffic pattern," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 300–313, 2010.

[72] R. van der Heijden, "Security architectures in V2Vand V2I communication," in *Proceedings of the 20th Student Conference IT*, pp. 1–10, Enschede, The Netherlands, 2010.

[73] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting black hole attack on AODV-based mobile ad hoc networks by dynamic learning method," *International Journal of Network Security*, vol. 5, no. 3, pp. 338–346, 2007.

[74] Y.-S. Shiu, S. Chang, H.-C. Wu, S. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[75] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: a survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[76] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 85–91, 2007.

[77] H. Nishiyama, D. Fomo, Z. M. Fadlullah, and N. Kato, "Traffic pattern-based content leakage detection for trusted content delivery networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 301–309, 2014.

[78] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 5, pp. 2471–2481, 2009.

[79] N. Nurelmadina, M. K. Hasan, I. Memon et al., "A systematic review on cognitive radio in low power wide area network for industrial IoT applications," *Sustainability*, vol. 13, no. 1, p. 338, 2021.

[80] J. Liu, Q. Li, R. Sun, X. Du, and M. Guizani, "An efficient anonymous authentication scheme for internet of vehicles," in *Proceedings of the IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, 2018.

[81] I. Memon, R. A. Shaikh, M. K. Hasan, R. Hassan, A. U. Haq, and K. A. Zainol, "Protect mobile travelers information in sensitive region based on fuzzy logic in IoT technology," *Security and Communication Networks*, vol. 2020, Article ID 8897098, , 2020.

[82] S. Islam, A.-H. Abdalla, and M. Kamrul Hasan, "Novel multihoming-based flow mobility scheme for proxy NEMO environment: a numerical approach to analyse handoff performance," *Scienceasia*, vol. 43S, no. 1, pp. 27–34, 2017.

[83] R. Hassan, F. Qamar, M. K. Hasan, A. H. M. Aman, and A. S. Ahmed, "Internet of things and its applications: a comprehensive survey," *Symmetry*, vol. 12, no. 10, p. 1674, 2020.

[84] C. Zhang, K. Chen, X. Zeng et al., "Misbehavior detection based on support vector machine and dempster-shafer theory of evidence in VANETs," *IEEE Access*, vol. 6, pp. 59860–59870, 2018.

[85] Z. Meng, "Security enhanced internet of vehicles with Cloud Fog Dew computing," *ZTE Communications*, vol. 15, no. S2, 2017.

[86] L. Song, G. Sun, H. Yu, X. Du, and M. Guizani, "FBIA: a fog-based identity authentication scheme for privacy preservation in internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5403–5415, 2020.

[87] J. Yakubu, "Security challenges in fog computing environment: a systematic appraisal of current developments," *Journal of Reliable Intelligent Environments*, vol. 27, pp. 467–483, 2019.

[88] J. Pan, "Key enabling technologies for secure and scalable future Fog-IoT architecture: a survey," 2018, https://arxiv.org/abs/1806.06188.

[89] M. K. Hasan, A. F. Ismail, S. Islam, W. Hashim, M. M. Ahmed, and I. Memon, "A novel HGBBDSA-CTI approach for subcarrier allocation in heterogeneous network," *Telecommunication Systems*, vol. 70, no. 2, pp. 245–262, 2019.

[90] S. Islam, O. O. Khalifa, A. A. Hashim et al., "Design and evaluation of a multihoming-based mobility management scheme to support inter technology handoff in PNEMO," *Wireless Personal Communications*, vol. 114, no. 2, pp. 1133–1153, 2020.

[91] M. K. Hasan, M. M. Ahmed, A. H. A. Hashim, A. Razzaque, S. Islam, and B. Pandey, "A novel artificial intelligence based timing synchronization scheme for smart grid applications," *Wireless Personal Communications*, vol. 114, no. 2, pp. 1067–1084, 2020.

[92] J. Stilgoe, "Machine learning, social learning and the governance of self-driving cars," *Social Studies of Science*, vol. 48, no. 1, pp. 25–56, 2018.

[93] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A comprehensive survey: benefits, services, recent works, challenges, security, and use cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, 2020.

[94] S. H. Alrubaee, M. Ismail, M. A. Altahrawi, and B. B. Burhan, "Filter bank multi-carrier modulation technique for vehicle-to-vehicle communication," *Journal of Communications*, vol. 15, no. 7, 2020.

[95] A. Ghazvini, S. N. H. S. Abdullah, M. Kamrul Hasan, and D. Z. A. Bin Kasim, "Crime spatiotemporal prediction with fused objective function in time delay neural network," *IEEE Access*, vol. 8, pp. 115167–115183, 2020.

[96] M. Z. Ibrahim and R. Hassan, "The implementation of internet of things using test bed in the UKMnet environment," *Asia-Pacific Journal of Information Technology & Multimedia*, vol. 8, no. 2, pp. 1–17, 2019.

[97] E. Adi, A. Anwar, Z. Baig, and S. Zeadally, "Machine learning and data analytics for the IoT," *Neural Computing and Applications*, vol. 32, no. 20, pp. 16205–16233, 2020.

[98] T. Yuan, "Harnessing machine learning for next-generation intelligent transportation systems: a survey," in *Proceedings of the Computational Intelligence, Communication Systems and Networks (CICSyN)*, Tetova, Macedonia, 2019.

[99] Syed Junaid Nawaz, "Quantum machine learning for 6G communication networks: state-of-the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46317–46350, 2019.