

Review

# A Comprehensive Survey on VANET–IoT Integration Toward the Internet of Vehicles: Architectures, Communications, and System Challenges

Khalid Kandali <sup>1,\*</sup> , Said Nouh <sup>1</sup> , Lamyae Bennis <sup>2</sup>  and Hamid Bennis <sup>3</sup>

<sup>1</sup> Laboratory of Information Technology and Modeling (LTIM), TCA Team, Faculty of Sciences Ben M'Sick, Hassan II University of Casablanca, Casablanca 20360, Morocco; said.nouh@univh2c.ma

<sup>2</sup> Laboratory of Sciences, Engineering and Management, High School of Technology, Sidi Mohamed Ben Abdellah University of Fez, Fes 30000, Morocco; lamyabennis@gmail.com

<sup>3</sup> IMACS Laboratory, SCIA2M Team, Graduate School of Technology, Moulay Ismail University of Meknes, Meknes 50040, Morocco; h.bennis@umi.ac.ma

\* Correspondence: kandali.khalid@gmail.com

## Abstract

The convergence of Vehicular Ad Hoc Networks (VANETs) and the Internet of Things (IoT) is giving rise to the Internet of Vehicles (IoV), a key enabler of next-generation intelligent transportation systems. This survey provides a comprehensive analysis of the architectural, communication, and computing foundations that support VANET–IoT integration. We examine the roles of cloud, edge, and in-vehicle computing, and compare major V2X and IoT communication technologies, including DSRC, C-V2X, MQTT, and CoAP. The survey highlights how sensing, communication, and distributed intelligence interact to support applications such as collision avoidance, cooperative perception, and smart traffic management. We identify four central challenges—security, scalability, interoperability, and energy constraints—and discuss how these issues shape system design across the network stack. In addition, we review emerging directions including 6G-enabled joint communication and sensing, reconfigurable surfaces, digital twins, and quantum-assisted optimization. The survey concludes by outlining open research questions and providing guidance for the development of reliable, efficient, and secure VANET–IoT systems capable of supporting future transportation networks.

**Keywords:** VANETs; IoT; IoV; V2X communication; edge computing; cooperative perception; ITS; scalability; security and privacy; 6G communication



Academic Editor: Luigi dell'Olio

Received: 29 November 2025

Revised: 4 January 2026

Accepted: 9 January 2026

Published: 31 January 2026

**Copyright:** © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

## 1. Introduction

In many parts of the world, cities have expanded faster than transport infrastructures could reasonably adapt. The increasing density of vehicles, combined with rising mobility expectations, has exposed long-standing issues related not only to congestion but also to road safety and environmental impact. These limitations have pushed researchers to rethink what a “modern transportation system” should look like. Today, the shift is no longer simply toward more vehicles on the road, but toward transport networks that communicate, coordinate, and react. Two technological domains play a central role in this transition: Vehicular Ad Hoc Networks (VANETs) and the Internet of Things (IoT). When brought together, they offer new ways for vehicles and infrastructure to share information, improve awareness, and support more advanced Intelligent Transportation Systems (ITSs) [1].

VANETs stem from the broader class of Mobile Ad Hoc Networks, but they present their own characteristics. Vehicles move at high speed, links appear and disappear rapidly, and many applications, especially those related to safety, require very low latency and reliable communication. Technologies such as IEEE 802.11p/DSRC and C-V2X were developed specifically to cope with these constraints by enabling fast exchanges of safety messages such as collision alerts or hazardous-road notifications [2,3]. In parallel, IoT systems have spread across cities and transportation infrastructures. Sensors embedded in traffic lights, weather stations, public equipment, or even carried by pedestrians generate a wide range of contextual data that can complement what vehicles detect on their own [4].

The combination of these two domains is commonly referred to as the Internet of Vehicles (IoV). In this integrated environment, VANETs provide the communication backbone, while IoT enriches the system with additional perception. The resulting network is more capable of identifying events, predicting risks, and coordinating decisions. Instead of relying only on local sensors, vehicles can benefit from the information coming from the surrounding infrastructure, which offers a broader perspective of road and environmental conditions [5].

Several advantages arise from this integration:

Safety, for example, can be improved when roadside sensors detect problems—like slippery surfaces or objects on the roadway—that a vehicle might not see in time. These alerts, once shared through VANET communication channels, help approaching drivers or automated systems react earlier, as highlighted in recent cooperative ITS studies [6].

Traffic efficiency also benefits from this synergy. VANETs offer local coordination between nearby vehicles, but IoT deployments allow city-level data collection, enabling better adjustments to traffic lights or dynamic rerouting during congestion [7].

From an environmental perspective, smoother traffic and better routing reduce emissions. Measurements based on IoT of air quality also contribute to environmental monitoring and policy planning [8,9].

Finally, the system opens the door to new services, ranging from predictive maintenance to customized on-the-go applications or usage-based insurance models [10].

In general, integrating VANETs with IoT forms a foundation for more adaptive and intelligent mobility systems. This evolution is a prerequisite for future transportation networks that must respond to increasing mobility demands while maintaining safety, efficiency, and sustainability.

### 1.1. Current Surveys and Research Gaps

Several surveys have explored different aspects of VANET–IoT integration. Some provide general overviews of network architectures or application categories [11,12]. Others focus more specifically on communication aspects, comparing DSRC to C-V2X or discussing the evolution of V2X connectivity in recent deployments [13,14]. Several surveys place emphasis on security and privacy, offering taxonomies of threats and reviewing common mitigation mechanisms [15,16]. Beyond communication and security, other works discuss enabling technologies such as Mobile Edge Computing (MEC) and task offloading [17], or they examine how AI and machine learning contribute to perception and decision-making processes [18,19]. More recent contributions have begun to consider additional paradigms, including blockchain-based trust management [20] and UAV-assisted networking [21].

Although literature covers many important topics, these surveys often treat them as separate issues. For instance, protocol comparisons may not consider the implications for security overhead, and security-focused analyses rarely discuss the interplay between computational load and edge-offloading constraints. Moreover, surveys published several years

ago naturally predate the broader adoption of C-V2X, the introduction of 5G-Advanced features, or the early development of 6G concepts. As a result, some analyses no longer reflect the current direction of research or industry deployment.

To better understand how these works relate to one another, and to emphasize their limitations more clearly, we provide in Table 1 a comparative summary of several representative surveys. The table highlights their main objectives, the technological layers they examine, and their level of coverage regarding emerging paradigms.

**Table 1.** Comparative overview of recent VANET-IoT surveys.

| Survey Reference   | Journal                                                 | Primary Focus                      | Architectural Scope                     | Protocol Analysis Depth                                                      | Security and Privacy Coverage                         | Treatment of AI/ML                                             | Emerging Paradigms                                           | Cross-Cutting Challenges                                                                                        |
|--------------------|---------------------------------------------------------|------------------------------------|-----------------------------------------|------------------------------------------------------------------------------|-------------------------------------------------------|----------------------------------------------------------------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Agbaje et al. [11] | IEEE Transactions on Intelligent Transportation Systems | Standards and Governance           | System-level overview                   | Limited to standards discussion                                              | Overview of security needs                            | Not a primary focus                                            | Pre-6G perspective                                           | Discusses interoperability as a key challenge                                                                   |
| Clancy et al. [13] | IEEE Communications Surveys and Tutorials               | DSRC vs. Cellular Interworking     | Focused on access network               | In-depth physical/link layer comparison                                      | Not covered                                           | Not covered                                                    | Not applicable                                               | Limited to network performance trade-offs                                                                       |
| Verma et al. [15]  | Applied Sciences                                        | Security Attacks and Solutions     | Not a focus                             | Not a focus                                                                  | Comprehensive threat taxonomy and solutions           | Discusses AI for threat detection                              | Lightweight cryptography                                     | Security–overhead trade-off analyzed                                                                            |
| Guo et al. [17]    | IEEE Wireless Communications                            | Computation Offloading             | Detailed edge architecture              | Medium (as an offloading factor)                                             | Not a primary focus                                   | Algorithm-focused                                              | Not a primary focus                                          | In-depth analysis of latency–energy trade-off                                                                   |
| Han et al. [19]    | IEEE Intelligent Transportation Systems Magazine        | AI for Vehicle Perception          | Focused on perception stack             | Not a focus                                                                  | Not a focus                                           | Comprehensive review of perception models                      | Not a primary focus                                          | Discusses computing complexity of models                                                                        |
| Wu et al. [21]     | IEEE Journal on Selected Areas in Communications        | UAV Communication                  | Aerial access layer architecture        | In-depth on aerial links and integration                                     | Limited discussion                                    | Not a primary focus                                            | UAVs as a core paradigm                                      | Analyzes UAV energy constraints                                                                                 |
| <b>Our Survey</b>  |                                                         | <b>Holistic System Integration</b> | <b>Full stack: Cloud, Edge, Vehicle</b> | <b>Comprehensive: Access (DSRC/C-V2X) and Application (MQTT/CoAP) layers</b> | <b>Dedicated section on mechanisms and trade-offs</b> | <b>Integrated throughout architectures, apps, and security</b> | <b>Dedicated section on 6G, Quantum, UAVs, Digital Twins</b> | <b>Core focus: A holistic treatment of trade-offs between scalability, latency, energy, and standardization</b> |

As shown in Table 1, many surveys remain confined to specific layers or technologies, which underlines the need for a more integrated perspective—one that considers architectural, protocol-level, and system-level issues in combination. This is the approach adopted in the present work.

### 1.2. Main Contributions

Taking into account the gaps identified above, this survey aims to provide an updated and more comprehensive view of VANET-IoT integration. The main contributions can be summarized as follows:

- 1 A multi-layer architectural perspective: We examine the interactions between the cloud, the edge, and vehicles, and we discuss how decisions at one layer may influence constraints or performance at another.
- 2 A protocol comparison across several layers of the communication stack: Rather than concentrating solely on access-layer technologies (DSRC, C-V2X), our review also

analyzes application-layer protocols such as MQTT and CoAP and their evolving roles in 5G-Advanced and prospective 6G systems.

- 3 A cross-analysis of system challenges: Latency, scalability, security, and energy consumption are discussed not as isolated issues but as elements that often interact and impose trade-offs within the system.
- 4 A forward-looking exploration of emerging paradigms: The survey highlights research directions likely to shape the next decade, including Joint Communication and Sensing (JCAS), digital-twin concepts, collaborative intelligence, and certain early ideas derived from quantum computing.

Together, these contributions provide a clearer picture of how VANET and IoT technologies intersect and where future efforts may be directed.

### 1.3. Organization of the Survey

The rest of the paper is organized as follows.

Section 2 presents background concepts related to VANETs and IoT.

Section 3 discusses enabling technologies and system models, including cloud computing, edge computing, and AI-based approaches.

Section 4 reviews representative applications such as smart-traffic control and emergency-response scenarios.

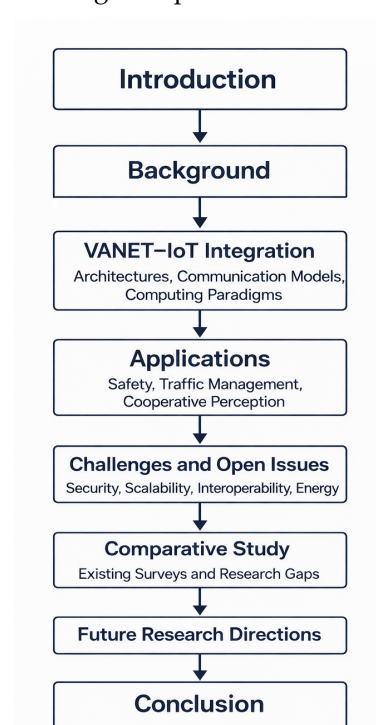
Section 5 outlines the main challenges associated with VANET–IoT integration.

Section 6 compares different communication protocols and architectural choices.

Section 7 highlights future research directions, including 6G-related developments and beyond.

Section 8 concludes the survey.

Figure 1 provides an overview of the structure of the paper.



**Figure 1.** Overview of the organization and structure of the survey paper.

## 2. Background

The integration of Vehicular Ad Hoc Networks (VANETs) with the Internet of Things (IoT) requires a clear understanding of the communication models, system architectures,

and enabling technologies that shape intelligent transportation ecosystems. This section provides an overview of these foundations, starting with the fundamentals of VANET communications, followed by the evolution toward the Internet of Vehicles (IoV) and ending with an examination of communication technologies and distributed computing models that support modern vehicular systems.

### 2.1. Vehicular Ad Hoc Networks (VANETs)

VANETs represent a specific class of Mobile Ad Hoc Networks (MANETs) in which vehicles act as mobile nodes that exchange information dynamically without relying entirely on fixed infrastructure [22]. Because of the inherent characteristics of vehicular mobility, high speeds, rapidly changing topology, and strict latency requirements, VANETs require dedicated communication mechanisms and optimized networking protocols. A central component of this ecosystem is Vehicle-to-Everything (V2X) communication, which includes interactions between vehicles, infrastructure, pedestrians, and network services.

Vehicle-to-Vehicle (V2V) communication enables the direct exchange of safety messages such as collision warnings or emergency braking information, allowing vehicles to react faster than with sensor perception alone [23]. Vehicle-to-Infrastructure (V2I) enhances situational awareness through communication with roadside units (RSUs), providing signal phase information, road status alerts, or cooperative traffic strategies [24]. Vehicle-to-Pedestrian (V2P) interactions rely on personal devices—such as smartphones or wearables—to improve the protection of vulnerable users, particularly in urban settings where visibility is limited [25]. Vehicle-to-Network (V2N) communication connects vehicles to cloud platforms through cellular infrastructure, enabling large-scale analytics, content distribution, and fleet coordination [26].

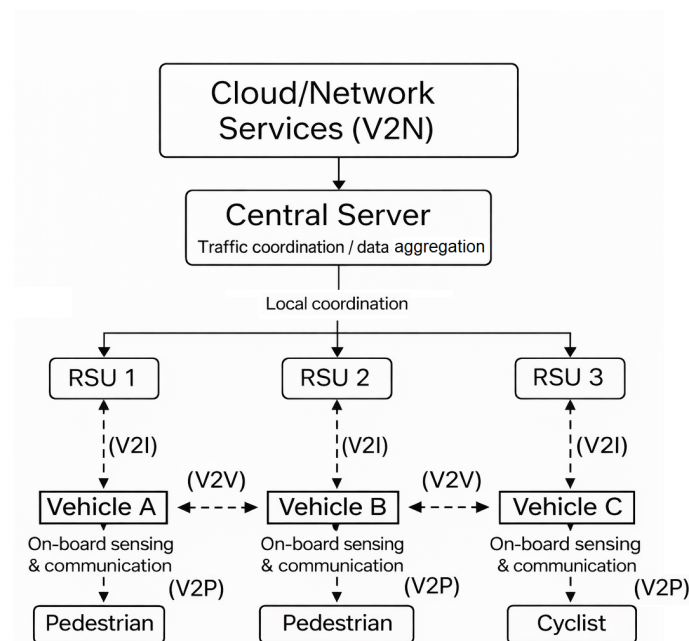
Recent studies on advanced V2X technologies have emphasized the transition toward 5G NR-V2X and its enhanced reliability, latency performance, and integrated sensing capabilities [13,14].

Figure 2 illustrates the main V2X communication modes in an intelligent transportation environment. It shows how vehicles interact with RSUs, edge servers, the cloud, vulnerable road users, and other vehicles through V2V, V2I, V2N, and V2P links. The architecture highlights the hierarchical flow of information from OBUs to MEC/Fog servers and cloud services.

Table 2 summarizes the four major V2X communication paradigms—V2V, V2I, V2N, and V2P. For each category, it lists the nodes involved, the underlying communication technologies, typical applications, and core challenges related to latency, reliability, coverage, and deployment constraints.

**Table 2.** Overview of V2X communication types, technologies, applications, and challenges.

| Type | Nodes Involved          | Communication Technology          | Primary Applications                 | Key Challenge                              |
|------|-------------------------|-----------------------------------|--------------------------------------|--------------------------------------------|
| V2V  | OBU ↔ OBU               | IEEE 802.11p, C-V2X PC5           | Collision avoidance, platooning      | Network fragmentation, high mobility       |
| V2I  | OBU ↔ RSU               | IEEE 802.11p, C-V2X PC5/Uu, Wi-Fi | Traffic management, internet access  | Infrastructure deployment cost             |
| V2N  | OBU ↔ Cloud/Server      | Cellular (4G/5G Uu)               | Infotainment, fleet management, SOTA | Network latency and coverage               |
| V2P  | OBU ↔ Pedestrian Device | LTE/5G Sidelink, Bluetooth LE     | Pedestrian safety, VRU protection    | Device penetration rate, power consumption |



**Figure 2.** Communication architecture of the Internet of Vehicles.

## 2.2. Role of RSUs in VANET–IoT Architectures

Roadside Units play a central role in VANET–IoT architectures by acting as intermediate nodes between vehicles, infrastructure, IoT devices, and cloud services. Beyond simple data relaying, RSUs support heterogeneous communication patterns, local coordination, edge processing, and interaction with external systems such as emergency services and unmanned aerial vehicles. Clarifying these communication types is essential to understanding the functional importance of RSUs in large-scale IoV deployments [14,27–29].

To clarify the functional role of Roadside Units in VANET–IoT systems, Table 3 categorizes the different RSU communication types and summarizes their respective functions within the IoV architecture.

**Table 3.** RSU communication types and their functional roles in VANET–IoT architectures.

| Communication Type        | Functional Role                                                                                                                             |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| V2I                       | Vehicles transmit status, sensor data, and alerts to RSUs for aggregation, local decision-making, and forwarding to edge or cloud systems.  |
| I2V                       | RSUs disseminate traffic updates, safety messages, signal phase and timing (SPaT), and control instructions to vehicles.                    |
| I2I                       | RSUs exchange information with neighboring RSUs to support coordinated traffic management and large-area situational awareness.             |
| RSU-to-Cloud              | RSUs forward aggregated data to cloud platforms for global traffic optimization, long-term analytics, and model training.                   |
| RSU-to-IoT Devices        | RSUs collect data from roadside sensors such as cameras, inductive loops, and environmental sensors to enrich vehicular perception.         |
| RSU-to-Emergency Services | RSUs relay incident reports and priority messages to emergency response systems, enabling faster reaction and coordinated intervention.     |
| RSU-to-UAV                | RSUs interact with UAVs to extend communication coverage, support aerial sensing, and assist in monitoring traffic and emergency scenarios. |

## 2.3. From IoT to the Internet of Vehicles (IoV)

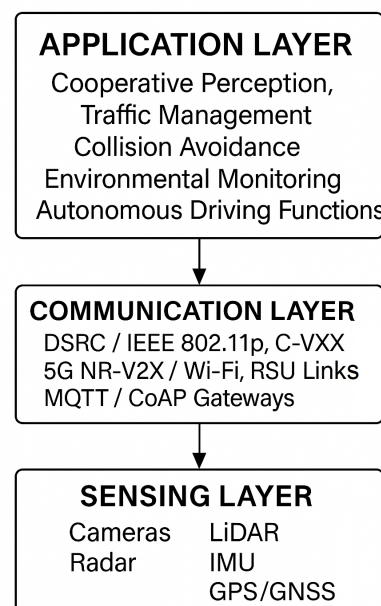
IoT technologies have increasingly influenced transportation environments through large-scale sensing, environmental monitoring, and distributed intelligence. Weather stations, traffic cameras, air-quality sensors, and smart parking systems provide contextual

data essential for vehicular decision-making [30]. The emergence of edge-AI modules—compact processors capable of local inference—has transformed many IoT devices into active computational nodes that can preprocess or analyze data before forwarding it [31]. The heterogeneous and multi-domain nature of IoV deployments builds upon foundational principles from heterogeneous ad hoc networking, particularly in environments where vehicles, IoT nodes, and RSUs dynamically form distributed topologies [32].

Building on the interaction between VANETs and IoT devices, the Internet of Vehicles (IoV) extends the vehicular ecosystem into a multi-layer cyber–physical–social system. IoV integrates sensing, networking, cloud services, and human participation to support more informed and efficient decision-making processes [33].

A typical IoV model includes three interconnected layers. The sensing layer collects raw information from vehicle-mounted LiDAR, radar, cameras, and IMUs, as well as from IoT-enabled roadside devices. The communication layer coordinates information exchange among vehicles, RSUs, and pedestrian devices using technologies such as DSRC, C-V2X, Wi-Fi, and cellular networks. The application layer supports tasks such as traffic prediction, cooperative perception, emergency response, and eco-routing [34]. Recent work emphasizes the importance of cross-layer optimization, showing that communication, sensing, and computing performance are tightly coupled [35].

Figure 3 illustrates the three-layer architecture commonly used in IoV systems. The sensing layer incorporates vehicle-mounted sensors such as cameras, LiDAR, radar, IMU, and GNSS, which generate raw environmental data. The communication layer enables data exchange through technologies such as DSRC, C-V2X, Wi-Fi, RSU links, and IoT protocols like MQTT and CoAP. The application layer supports higher-level intelligent services including cooperative perception, traffic management, collision avoidance, environmental monitoring, and autonomous driving.



**Figure 3.** Hierarchical IoV data processing architecture.

Modern IoV systems rely on a diverse set of sensing technologies deployed both on vehicles and in the environment. Cameras provide rich visual context for lane detection and semantic reasoning, whereas LiDAR offers precise depth estimation through 3D point clouds. Radar contributes robust velocity and distance measurements under

adverse weather conditions, and IMUs ensure short-term motion estimation. Roadside IoT devices complement vehicular sensing by monitoring weather, road surface conditions, and pedestrian movement.

Table 4 lists the principal sensor families used in IoV systems, including cameras, LiDAR, RADAR, GNSS, IMUs, OBD-II/CAN sensors, and V2X communication modules. For each sensor, the table summarizes its primary function, produced data type, and typical IoV applications.

**Table 4.** Overview of major IoV sensor types, their functions, data characteristics, and applications.

| Sensor Type                     | Primary Function                                              | Data Characteristics                                                     | IoV Application Example                                                                  | Representative References |
|---------------------------------|---------------------------------------------------------------|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------|---------------------------|
| Camera (Monocular/Stereo)       | Visual perception, object classification, scene understanding | High-volume 2D/3D image frames, video streams (RGB, thermal)             | Traffic sign recognition, pedestrian/cyclist detection, lane tracking, driver monitoring | [18,34]                   |
| LiDAR                           | High-precision 3D mapping, object detection and tracking      | 3D point clouds (x,y,z + intensity), very high data rate                 | High-definition mapping, precise obstacle detection, localization                        | [36,37]                   |
| RADAR                           | All-weather distance and velocity measurement                 | Object range, radial velocity, angle; lower resolution than LiDAR        | Adaptive Cruise Control (ACC), blind-spot monitoring, collision warning                  | [34,38]                   |
| GPS/GNSS                        | Global positioning and timing                                 | Latitude, longitude, altitude, velocity, timestamp; prone to signal loss | Navigation, location-based services, fleet tracking, geo-fencing                         | [37,39]                   |
| IMU (Inertial Measurement Unit) | Measures vehicle motion and orientation (dead reckoning)      | Acceleration, angular rate, yaw; high frequency but drifts over time     | Dead reckoning (GPS loss compensation), electronic stability control                     | [38,39]                   |
| OBD-II/CAN Bus Sensors          | Monitor internal vehicle status and diagnostics               | Engine RPM, fuel level, tire pressure, emissions, diagnostic fault codes | Predictive maintenance, eco-driving, usage-based insurance, remote diagnostics           | [10,40]                   |
| V2X Modems (OBU)                | Communication with other entities                             | Cooperative Awareness Messages (CAMs), DENM event messages               | Hazard sharing, intersection collision avoidance, platooning                             | [13,14]                   |

#### 2.4. Communication Technologies in IoV

Communication is essential to cooperative vehicular systems. IEEE 802.11p/DSRC offers low-latency broadcast communication over short ranges but suffers from performance degradation under high-density conditions due to channel contention [41].

Cellular-V2X (C-V2X), introduced in 3GPP Releases 14–15, provides both direct sidelink communication (PC5) and infrastructure-assisted communication (Uu). It has consistently demonstrated higher reliability, superior range, and better scalability compared to DSRC [34]. With the introduction of 5G NR-V2X (Releases 16–18), vehicular communication benefits from increased throughput, lower latency, improved spectrum allocation, and explicit support for cooperative perception and joint communication–sensing tasks. Research published between 2022 and 2025 shows that NR-V2X significantly enhances automated platooning, sensor fusion, and real-time coordination across multiple vehicles [42,43].

At the application layer, lightweight IoT protocols such as MQTT and CoAP play a growing role in vehicular data dissemination. MQTT is suitable for publish–subscribe communication between RSUs and cloud infrastructure, whereas CoAP is common in constrained IoT environments [44]. Autonomous driving systems increasingly rely on middleware frameworks such as DDS or gRPC to support low-latency, structured communication pipelines [45].

Table 5 compares DSRC (IEEE 802.11p/1609) and C-V2X (LTE-V2X and NR-V2X) across key dimensions such as standardization, radio access methods, latency, reliability, mobility support, and suitability for cooperative and automated driving scenarios.

**Table 5.** Comparison between DSRC and C-V2X for vehicular communications.

| Feature               | DSRC (IEEE 802.11p/1609)               | C-V2X (LTE-V2X & 5G NR-V2X)                            |
|-----------------------|----------------------------------------|--------------------------------------------------------|
| Standardization Body  | IEEE, ETSI                             | 3GPP (Releases 14, 15, 16+)                            |
| Underlying Technology | Wi-Fi variant (IEEE 802.11)            | Cellular (LTE, 5G NR)                                  |
| Communication Mode    | Only ad hoc (V2V, V2I)                 | Hybrid: direct sidelink (PC5) + cellular network (Uu)  |
| Multiple Access       | CSMA/CA (contention-based)             | Scheduled (network-managed or sensing-based)           |
| Latency & Reliability | Good, but degrades in dense scenarios  | Superior with 5G NR-V2X (URLLC support)                |
| Key Advantage         | Maturity; low cost for V2V deployments | Performance; scalability; clear evolution path (5G/6G) |
| Primary Use Case      | Basic Safety Messages (BSMs)           | Advanced V2X services and automated driving support    |

2.5. Distributed Computing: Cloud–Edge–Vehicle Continuum

The massive volume of data generated by connected vehicles and IoT systems requires flexible and distributed computational models. Cloud computing supports large-scale analytics, long-term storage, and centralized learning processes but is limited by communication delays that make it unsuitable for time-sensitive safety applications [46].

Mobile Edge Computing (MEC) reduces these delays by deploying computing resources closer to vehicles, typically at RSUs or cellular base stations. MEC servers can process data streams, perform multi-vehicle perception fusion, and execute offloaded tasks at low latency [47]. Recent studies (2022–2025) demonstrate that MEC-enhanced cooperative perception improves detection accuracy and reduces redundant onboard computation [48].

In-vehicle computing has also evolved significantly with the introduction of automotive-grade AI accelerators capable of running deep neural networks for perception, prediction, and planning tasks. Platforms released between 2023 and 2025, such as NVIDIA Orin or Qualcomm Ride, enable real-time processing of multi-sensor data directly within the vehicle [49].

3. VANET and IoT Integration

The convergence of VANET and IoT technologies is widely recognized as a key driver of next-generation intelligent transportation systems. While VANETs provide low-latency communication among vehicles and infrastructure, the IoT expands the sensing, contextual awareness, and computation capabilities of the environment. When combined, they form an extended Internet of Vehicles (IoV) ecosystem capable of supporting advanced mobility services, cooperative perception, predictive decision-making, and distributed intelligence.

Current research highlights that VANET–IoT integration does not follow a single architectural blueprint. Instead, several complementary models coexist, each designed to address specific challenges such as latency reduction, computational scalability, bandwidth optimization, and trust management. The following subsections summarize the primary integration paradigms reported in contemporary literature and outline their benefits and limitations.

### 3.1. Cloud-Based VANET–IoT Integration

Cloud-centric architectures remain foundational in large-scale data processing for transportation systems. Data generated by vehicles, RSUs, IoT sensors, and traffic monitoring devices is typically aggregated in remote cloud platforms with virtually unlimited computational and storage capabilities. Such architectures are effective for city-wide analytics, historical modeling, and large-scale AI training, particularly when the timing constraints are not strict [50].

Vehicles and IoT nodes forward data through RSUs or cellular networks (4G/5G) into cloud infrastructures such as AWS, Azure, or private clouds. These platforms use big-data engines (e.g., Hadoop, Spark) to process terabyte-scale datasets, enabling applications such as long-term traffic pattern analysis, anomaly detection, and predictive modeling. Typical cloud-based applications include:

**Predictive Traffic Modeling:** Long-horizon forecasting to anticipate congestion patterns and adapt traffic light programming across the city [51].

**Fleet and Logistics Management:** Real-time vehicle health monitoring, route optimization, and fuel usage analysis for large corporate fleets [40].

**High-Definition (HD) Map Creation:** Cloud servers consolidate sensor data from numerous vehicles to generate updated HD maps used by autonomous driving systems [52].

Despite their strengths, cloud-based models face two major limitations:

The first: the delay caused by long uplink/downlink transfers makes them unsuitable for safety-critical tasks requiring millisecond-level responses.

The second: continuous upload of raw sensor data (e.g., LiDAR or video) is bandwidth-intensive and costly.

Recent research emphasizes hybrid cloud-edge designs that keep high-level model training in the cloud while pushing latency-critical inference to the edge. Gu et al. [28] highlight that the cloud is increasingly used to train large-scale DRL models, which are later deployed at the edge for fast inference. Similar findings are reported by Zhang et al. [53] and Karimi et al. [54], who observe a shift toward transmitting processed metadata instead of raw sensor streams to reduce bandwidth pressure. Chougule et al. [55] extend this perspective to EV networks, suggesting the use of cloud-based digital twins to optimize large-scale charging and grid balancing scenarios.

In summary, the cloud excels in macro-level analytics, policy planning, and model training, while its limitations in latency and bandwidth make cloud-only solutions insufficient for real-time systems.

### 3.2. Edge/Fog-Based VANET–IoT Integration

Edge and Fog architectures aim to overcome the latency and bandwidth limitations of cloud-centric systems by distributing computation closer to vehicles. Processing tasks are moved to RSUs, base-station MEC servers, or clusters of nearby vehicles acting as fog nodes [56]. Several surveys on vehicular edge computing, including the study in [27], emphasize the crucial role of RSU-level processing for achieving low-latency and bandwidth-efficient VANET–IoT applications.

In this paradigm, local edge servers process sensor inputs, cooperative events, and safety messages in real time, avoiding the round-trip delays associated with cloud offloading. Typical edge-assisted applications include:

**Real-time Collision Avoidance:** Edge processors aggregate data from multiple vehicles approaching an intersection and predict collision risks within milliseconds [57].

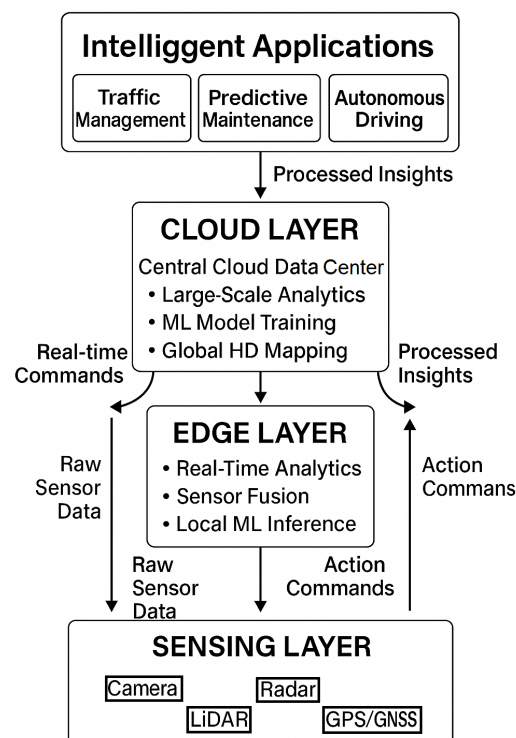
**Computational Offloading:** MEC servers execute heavy modules such as trajectory planning or multi-sensor fusion for autonomous vehicles, reducing onboard computing load [58].

**Low-Latency Caching:** Local distribution of frequently accessed content (e.g., map updates or software patches), enabling rapid delivery within specific road segments [59].

Although edge nodes improve latency, they have limited computing capacity compared to cloud servers. Their effectiveness depends on deployment density, mobility-aware service placement, and resource allocation strategies. The cost and operational complexity of deploying MEC infrastructure across cities also remain challenges.

Recent surveys emphasize the importance of intelligent task scheduling and resource management. Guo et al. [28] compare proactive and reactive offloading mechanisms and show that predictive, AI-driven strategies significantly reduce latency, albeit at the cost of possible misallocation when prediction errors occur. Habibi et al. [60] examine vehicular fog architectures and conclude that hybrid coordination schemes—combining centralized RSU-based orchestration with decentralized vehicle cooperation—offer the best compromise between reliability and flexibility.

Figure 4 illustrates the layered computation model used in IoV systems. The vehicle layer generates raw sensor data through on-board sensors such as cameras, LiDAR, radar, IMU, and GNSS. The edge layer, typically implemented through RSUs or MEC nodes, performs real-time analytics, sensor fusion, short-term prediction, and local decision support. The cloud layer provides large-scale processing for long-term learning, traffic forecasting, high-definition map updates, and global coordination. Processed insights flow back toward the edge and vehicle layers to support intelligent applications such as cooperative perception, collision avoidance, and traffic management.



**Figure 4.** Cloud-edge-vehicle continuum for VANET-IoT integration.

The literature suggests that while edge computing is indispensable for low-latency services, its performance depends heavily on predictive intelligence, topology dynamics, and the accuracy of mobility-aware orchestration. AI-driven resource management is therefore emerging as a critical research direction.

### 3.3. AI/ML for VANET–IoT Systems

Artificial Intelligence (AI) and Machine Learning (ML) play a central role in enabling perception, prediction, and decision-making across cloud, edge, and vehicle layers. Lightweight models deployed at the edge or inside the vehicle support real-time inference, while more complex models are trained in the cloud.

**Edge-based Inference:** Deep learning models such as YOLO and SqueezeNet can process camera streams to detect and classify objects in real time [61]. Other ML models perform anomaly detection to identify unsafe driving patterns, unusual traffic behavior, or road hazards [62].

**Cloud-based Training:** The cloud provides the large-scale computation required to train predictive analytics models capable of forecasting congestion, estimating travel times, and identifying accident-prone areas [63].

A significant trend is the rise of Federated Learning (FL), which keeps raw data local while sharing only model updates. Mo et al. [64] review FL frameworks for IoV and highlight challenges such as communication overhead, non-IID data, and vulnerability to model poisoning.

Another major research theme concerns model compression to support efficient edge inference. Gu et al. [28] compare pruning, quantization, and knowledge distillation techniques, emphasizing the trade-off between accuracy and computational load. Alqubaysi et al. [65] show that FL can match centralized learning accuracy while preserving privacy but often requires more communication rounds.

Overall, AI integration in VANET–IoT systems involves balancing privacy, latency, model accuracy, and communication efficiency. No approach is universally optimal; the most suitable solution depends on application constraints.

### 3.4. Security and Privacy

The open and wireless nature of VANET–IoT systems exposes them to multiple threats, making security and privacy core design requirements. Cryptographic primitives such as AES and ECDSA are fundamental for message confidentiality, integrity, and authentication. In parallel, blockchain technologies are increasingly explored for trust management and tamper-proof record keeping [66–68]. Pseudonymization is another widely used method, allowing vehicles to frequently change identifiers to prevent long-term tracking [69].

Recent research compares classical cryptographic solutions with emerging blockchain-based mechanisms. Mohammed et al. [70] analyze consensus protocols for vehicular fog systems and conclude that traditional Proof-of-Work is impractical due to energy and latency constraints, whereas lightweight schemes such as PBFT, PoS, or dPoS provide more suitable alternatives. Choi et al. [71] discuss limitations of PKI-based V2X authentication, particularly the delays in certificate revocation, and highlight that blockchain can enable faster CRL distribution. Boualouache et al. [72] survey pseudonym management schemes and observe that hybrid centralized–decentralized approaches—potentially combined with blockchain—achieve the best balance between privacy and performance.

In summary, blockchain is a promising complement to cryptographic mechanisms, particularly for transparent certificate management, but must be integrated carefully to avoid excessive overhead.

### 3.5. Comparative Summary of VANET–IoT Integration Models

Table 6 summarizes key contributions from recent VANET–IoT integration studies [28,40,51–64,66,67,69–74], highlighting the diversity of architectures, objectives, and technological enablers. This table compares representative works on VANET–IoT integration across four major categories: cloud-based architectures, edge/fog computing, AI/ML-

driven frameworks, and security/privacy solutions. For each category, it summarizes the main objectives, strengths, and remaining limitations identified in the literature. The comparison highlights the trade-offs between latency, scalability, security, and computational demands, helping identify research gaps addressed in subsequent sections.

**Table 6.** Comparison of integration approaches in IoV systems.

| Category                       | Representative Studies | Main Objectives                                                                  | Key Strengths                                                                               | Limitations                                                                  |
|--------------------------------|------------------------|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Cloud-based Integration        | [28,40,51–55,57]       | Large-scale analytics, HD map generation, fleet management, predictive modelling | High computing power; global view; long-term learning; digital twins                        | High latency; heavy data upload; unsuitable for safety-critical applications |
| Edge/Fog-based Integration     | [55,58–61]             | Low-latency inference, task offloading, real-time fusion at RSUs                 | Millisecond response time; cooperative perception; reduced bandwidth                        | Limited computing capacity; dependence on infrastructure density             |
| AI/ML-driven Integration       | [53,62–64,66,67]       | Object detection, traffic prediction, anomaly detection, FL-based learning       | High accuracy; autonomous and cooperative perception; privacy-preserving federated learning | High training cost; FL communication overhead; sensitivity to non-IID data   |
| Security and Privacy Solutions | [56,69–74]             | Authentication, integrity, blockchain-based trust, pseudonym management          | Strong authentication; transparent auditing; tamper-proof logs                              | Blockchain overhead; revocation delays; privacy–traceability trade-off       |

## 4. Applications of VANET–IoT Integration

The integration of VANET and IoT technologies has enabled a wide spectrum of applications that support safer, more efficient, and more sustainable mobility systems. By combining vehicular communication networks with large-scale sensing, distributed computation, and intelligent decision-making, emerging transportation infrastructures can optimize traffic, enable cooperative autonomous driving, improve emergency response, and enhance environmental monitoring. This section presents the major application domains structured around the most relevant categories observed in recent research.

### 4.1. Traffic Optimization and Intelligent Traffic Management

Traffic optimization is one of the most mature and widely studied application areas of VANET–IoT integration. By aggregating data from vehicles, roadside IoT sensors, cameras, and environmental monitoring devices, transportation authorities can generate situational awareness at both local and large scales. Intelligent intersections, adaptive signal control, and congestion-aware routing algorithms rely heavily on this integrated information flow.

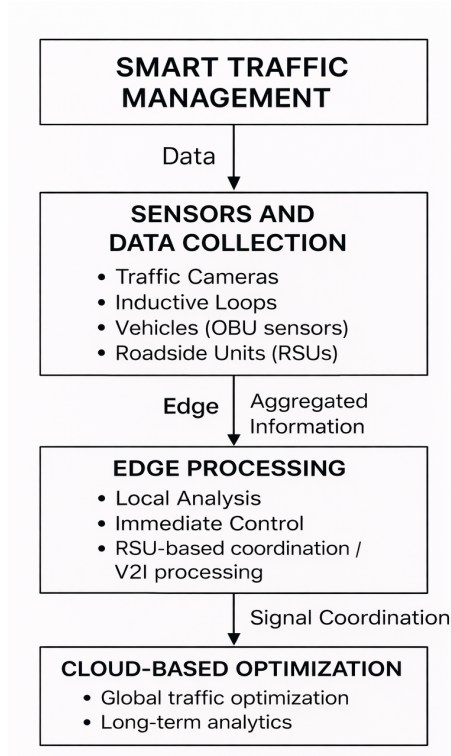
Real-time data collected from connected vehicles allow prediction of congestion build-up several minutes before it becomes critical [73]. IoT-enhanced RSUs equipped with traffic cameras, inductive loops, or radar sensors supplement this data by offering precise measurements of lane occupancy, queue length, and turning flows. Predictive models built on this multimodal dataset can adjust signal timings to minimize delays, prioritize public transport, or mitigate bottlenecks [74].

Several studies have demonstrated the benefits of cooperative routing strategies in which vehicles exchange local observations through V2V communication while RSUs provide regional traffic information via V2I links. These hybrid approaches improve traffic stability and reduce stop-and-go oscillations, especially in dense urban areas [75]. Cloud platforms play a complementary role by performing long-term analytics and identify-

ing recurring congestion hotspots, enabling strategic planning of infrastructure improvements [76].

Recent work has further explored decentralized and edge-assisted traffic management. MEC servers positioned at intersections perform local computations—such as real-time vehicle counting, trajectory clustering, or anomaly detection—allowing rapid responses under rapidly changing traffic conditions [77].

Figure 5 shows how sensing data from connected vehicles and roadside IoT devices flows to edge and cloud layers to enable adaptive traffic management. Vehicles report position, speed, and events through V2X links, while RSUs perform local analytics. Processed data is combined in the cloud to generate large-scale traffic predictions and optimization policies. Updated control strategies are then disseminated back to intersections and vehicles.



**Figure 5.** Example of VANET-IoT-enabled smart traffic management workflow.

#### 4.2. Connected and Autonomous Mobility (CAV Applications)

Connected and Autonomous Vehicles (CAVs) rely on continuous data exchange to enhance situational awareness and improve driving decisions. While onboard sensors provide high-resolution perception, their effectiveness remains limited by occlusions, adverse weather, and field-of-view constraints. Integrating VANET communication with IoT-based infrastructure significantly strengthens perception and decision-making for autonomous systems.

**Cooperative Perception (CP):** CP systems share object detections, trajectories, and free-space information among vehicles and roadside sensing units to remove blind spots and extend perception range. This cooperative data fusion drastically reduces collision risks in urban areas with heavy occlusions [78].

**Platooning and Cooperative Driving:** CAV platoons require stable low-latency communication to maintain tight inter-vehicle spacing. V2V links provide real-time updates on acceleration, braking, and trajectory adjustments, while IoT-enhanced RSUs monitor lane conditions and merging events [79].

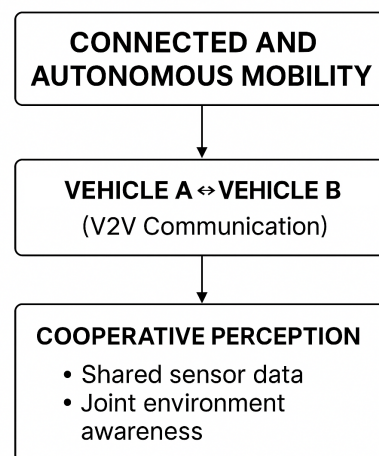
**HD Map Maintenance and Localization:** Cloud platforms aggregate perception data from multiple vehicles to generate near-real-time HD map updates. Edge servers simul-

taneously provide positioning corrections and lane-level localization cues using GNSS sensors, LiDAR landmarks, and IoT-based roadside beacons [39].

**Edge-Assisted Autonomy.** MEC nodes support compute-intensive tasks such as global path planning, image-based object recognition, and cross-vehicle sensor fusion while maintaining acceptable response times for safety-critical decisions [80].

These capabilities create a symbiotic relationship in which IoT infrastructure improves automated driving reliability, while connected vehicles enrich the collective knowledge base.

Figure 6 illustrates how connected autonomous vehicles share perception information through V2V communication. Vehicles exchange sensor data, hazard alerts, and situational context, enabling a broader and more reliable perception field than what a single vehicle can achieve independently.

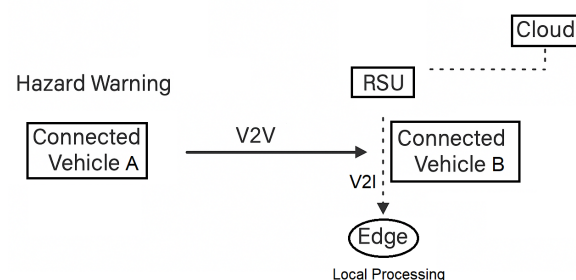


**Figure 6.** Cooperative perception in connected and autonomous mobility.

#### 4.3. Cooperative Safety and Emergency Response

Safety applications constitute one of the most critical motivations for integrating VANET and IoT technologies. By leveraging real-time sensing, low-latency communications, and distributed analytics, the network can rapidly detect hazardous situations and disseminate alerts to nearby vehicles.

Figure 7 illustrates how local vehicle sensors, roadside IoT devices, and edge servers collaborate to provide a unified perception view. Vehicles detect objects using onboard cameras, radar, and LiDAR, while RSUs supplement missing information. Edge servers fuse multi-vehicle data streams, support trajectory prediction, and assist autonomous driving modules with low-latency inference.



**Figure 7.** Cooperative hazard warning in VANET–IoT systems.

**Hazard and Incident Detection:** Vehicles can identify sudden braking, slippery surfaces, lane obstructions, or abnormal driving patterns using onboard sensors and V2V communication. IoT-enabled roadside sensors provide complementary data—such as

weather changes, smoke detection, or structural failures—leading to earlier hazard identification [81].

**Emergency Vehicle Coordination:** IoT-enhanced RSUs coordinate emergency vehicle routes by broadcasting lane-clearing instructions and signal preemption commands. V2X communication ensures that ambulances, fire trucks, and police vehicles receive right-of-way support through real-time traffic signal adjustments [82].

**Collision Avoidance:** Cooperative collision avoidance systems integrate V2V alerts, road friction data, and contextual information from IoT sensors to improve braking decisions and lane-change safety [38].

**Post-Incident Management:** Once an incident is detected, cloud-based systems generate rerouting instructions, notify emergency responders, and update long-term safety statistics for infrastructure planning [36].

Table 7 provides a structured comparison of major safety and emergency response applications supported by VANET–IoT integration, as identified in representative works [36,37,63,80,83–85]. For each safety challenge, it summarizes the enabling technologies, communication mechanisms, and main benefits, along with representative references from recent literature. The applications highlight the crucial role of cooperative sensing, real-time V2X communication, and IoT-enhanced analytics in improving road safety and emergency response efficiency.

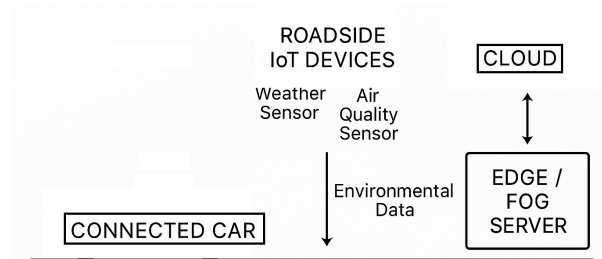
**Table 7.** Safety challenges in VANET–IoT systems and corresponding V2X mechanisms.

| Safety Challenge                                              | VANET–IoT Solution                               | V2X / IoT Mechanism                               | Key Benefit                                               | Representative References |
|---------------------------------------------------------------|--------------------------------------------------|---------------------------------------------------|-----------------------------------------------------------|---------------------------|
| Hazard Detection (slippery road, obstacles, abnormal braking) | Vehicle sensors + IoT roadside detection         | V2V alerts; RSU sensing; IoT environmental probes | Early hazard identification and warning distribution      | [36,83]                   |
| Cooperative Collision Avoidance                               | Multi-vehicle data fusion + predictive models    | V2V + V2I low-latency exchange                    | Reduced collision probability; faster reaction time       | [80,83]                   |
| Emergency Vehicle Priority                                    | IoT-enhanced signal preemption + dynamic routing | V2I communication with traffic signals            | Faster emergency response; optimized clearance paths      | [37]                      |
| Incident and Post-Accident Management                         | Cloud analytics + IoT road monitoring            | V2N uplink + RSU coordination                     | Rapid incident reporting, rerouting, and network recovery | [84]                      |
| Road Condition Awareness (ice, potholes, degradation)         | IMU data + roadside IoT weather stations         | V2V broadcast + V2I sensor aggregation            | Continuous and fine-grained road monitoring               | [36,85]                   |
| Abnormal Driving Detection (speeding, weaving, harsh braking) | In-vehicle sensors + IoT surveillance devices    | V2N reporting; local RSU analytics                | Improved driver safety and early risk identification      | [36,63]                   |

#### 4.4. Environmental Monitoring and Urban Sensing

Environmental monitoring has become an essential component of modern smart cities. The combination of vehicular sensors and stationery IoT nodes enables fine-grained assessment of environmental conditions across large areas.

Figure 8 illustrates how connected vehicles and roadside IoT sensors collect environmental data such as weather conditions and air quality. The data is forwarded to edge/fog servers for real-time processing and then to the cloud for large-scale analytics and long-term environmental insights.



**Figure 8.** Environmental monitoring in VANET-IoT systems.

**Air Quality Monitoring.** Vehicles equipped with low-cost gas sensors help monitor pollutants such as  $NO_2$ ,  $CO_2$ , and particulate matter (PM2.5). Their mobility allows dynamic mapping of pollution variations throughout the day [37].

**Weather and Microclimate Monitoring.** IoT stations measure temperature, humidity, rainfall, wind speed, and road surface conditions. This data supports route recommendations, road maintenance, and weather hazard prediction [83].

**Road Surface Condition Assessment.** Accelerometers, IMUs, and vibration sensors embedded in vehicles can detect potholes, cracks, or icy surfaces. RSUs collect these reports and notify maintenance teams or broadcast warnings [84].

**Noise Mapping and Urban Planning.** IoT microphones distributed in dense regions help build noise heatmaps, which support urban planning decisions and smart zoning policies [86].

The integration of IoT and vehicular sensing ensures wide spatial coverage without deploying a prohibitive number of stationary sensors.

Table 8 summarizes key environmental and urban sensing applications supported by VANET-IoT integration, derived from recent studies [85–88]. It highlights how mobile vehicle sensors and stationary IoT devices complement each other to provide high-resolution measurements of air quality, weather conditions, road-surface hazards, and urban noise. The table also identifies the underlying communication mechanisms and the main benefits associated with each application domain.

**Table 8.** Environmental applications enabled by VANET-IoT data fusion.

| Environmental Application            | Primary Data Sources                                                      | VANET-IoT Mechanism                                                                                                         | Key Benefit                                                         | Representative References |
|--------------------------------------|---------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|---------------------------|
| Air Quality Monitoring               | Gas sensors ( $NO_2$ , $CO_2$ , PM2.5) on vehicles; roadside IoT stations | Vehicles collect mobile air-quality samples; RSUs aggregate and transmit data; cloud performs large-scale pollution mapping | Fine-grained, dynamic pollution monitoring across large urban areas | [86]                      |
| Weather and Microclimate Observation | Roadside weather stations; vehicle-based humidity and temperature sensors | IoT nodes detect local weather patterns; edge servers trigger hazard alerts; cloud refines microclimate forecasts           | Early detection of severe weather; improved route safety            | [87]                      |
| Road Surface Condition Assessment    | IMU, accelerometer, wheel-slip sensors; roadside friction sensors         | Vehicles detect potholes, cracks, slippery surfaces via V2V/V2I; RSUs validate and broadcast roadway condition alerts       | Timely road hazard notification; supports maintenance planning      | [85]                      |
| Noise and Urban Sound Mapping        | IoT microphone arrays; vehicle-mounted acoustics sensors                  | Distributed IoT nodes measure noise levels; data aggregated at edge/cloud to produce environmental sound heatmaps           | Supports urban planning, zoning policies, and noise mitigation      | [88]                      |

#### 4.5. Representative VANET–IoT Integration Case Studies

Although this survey primarily focuses on architectures, communication technologies, and system challenges, it is important to illustrate how VANET–IoT integration is applied in representative real-world scenarios. This subsection presents typical VANET–IoT integration case studies reported in the literature to highlight practical deployment aspects and operational benefits.

**Case Study 1: Intelligent Intersection Management Using RSU-Assisted Cooperative Perception.**

In urban intersections, roadside units equipped with cameras, radar sensors, and IoT devices cooperate with connected vehicles to enable enhanced situational awareness. Vehicles share local perception data through Vehicle-to-Infrastructure links, while RSUs aggregate and fuse this information to detect occluded objects and predict potential collision risks [18]. The processed data are then disseminated back to vehicles using Infrastructure-to-Vehicle communication, enabling early warning and coordinated maneuvering. Such RSU-assisted cooperative perception systems have demonstrated improved detection accuracy and reduced reaction time compared to standalone on-board sensing, particularly in non-line-of-sight scenarios [7,36].

**Case Study 2: Emergency Vehicle Priority and Traffic Signal Control.**

Another representative application involves emergency vehicle prioritization in smart cities [77]. In this scenario, emergency vehicles broadcast priority messages through VANET communication, which are received by nearby RSUs and IoT-enabled traffic signal controllers. The RSUs locally coordinate signal phase adjustments and propagate priority information to neighboring intersections, while cloud platforms perform global traffic optimization when broader coordination is required [84]. This VANET–IoT integration enables faster emergency response times and reduces traffic disruption by dynamically adapting signal timing based on real-time vehicle and infrastructure data [80].

**Case Study 3: Cooperative Traffic Monitoring and Congestion Management.**

Large-scale traffic monitoring systems leverage IoT sensors such as inductive loops, traffic cameras, and environmental sensors deployed along road segments, combined with vehicular data collected from on-board units [51]. RSUs act as edge processing nodes that aggregate traffic density and speed information from both vehicles and roadside sensors. Edge-level analytics support rapid congestion detection, while cloud-based platforms perform long-term traffic pattern analysis and predictive modeling [73]. This hierarchical VANET–IoT architecture enables scalable traffic management with reduced communication overhead and improved responsiveness [78].

These representative case studies demonstrate how VANET–IoT integration enables practical intelligent transportation services by combining distributed sensing, edge-assisted coordination, and cloud-based optimization. While the specific implementation details vary across deployments, these examples highlight common architectural patterns and operational principles that guide real-world VANET–IoT system design.

#### 4.6. Discussion

VANET–IoT integration has demonstrated significant benefits across traffic management, autonomous mobility, safety, and environmental monitoring. However, the practical deployment of these applications depends on the reliability of V2X communication, the scalability of edge resources, the robustness of IoT sensors, and the development of secure and privacy-aware mechanisms. The next section discusses the remaining challenges and identifies research directions needed to achieve fully integrated intelligent transportation systems.

## 5. Challenges and Open Issues

The integration of VANET and IoT technologies promises to transform transportation systems into highly connected, context-aware, and autonomous environments. Despite these advances, several fundamental challenges hinder the large-scale deployment and reliability of such systems. These challenges emerge from the intrinsic characteristics of vehicular networks, including high mobility, dynamic topologies, latency constraints, and heterogeneous device capabilities—as well as from the limitations of IoT infrastructures that contribute sensing and computational support.

Addressing these issues requires coordinated solutions across communication, computation, and security layers. In particular, ensuring robust trust management, scalable resource allocation, seamless interoperability, and energy-efficient operation remain essential for achieving resilient and sustainable Intelligent Transportation Systems.

The following subsections outline the most prominent challenges identified in recent literature and highlight open research directions that must be addressed to realize the full potential of VANET–IoT integration.

### 5.1. Routing Taxonomy in VANET–IoT Systems

Routing plays a critical role in VANET–IoT systems due to high vehicle mobility, frequent topology changes, and heterogeneous communication technologies. Unlike traditional VANETs, IoV environments may leverage roadside infrastructure, cloud platforms, and IoT devices to support routing decisions. To improve clarity and provide structured guidance for researchers, routing protocols can be classified according to their dependence on RSUs and the supported communication types, including V2V, V2I, I2V, and I2I.

Table 9 summarizes this taxonomy and highlights representative routing approaches.

**Table 9.** Taxonomy of routing protocols in VANET–IoT systems based on infrastructure support, communication type, and representative studies.

| Routing Category                   | RSU Support  | Communication Type | Typical Routing Approaches                                        | Key Characteristics                                                                                   | Representative References |
|------------------------------------|--------------|--------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|---------------------------|
| Ad hoc VANET routing               | No RSU       | V2V                | AODV, DSR, GPSR, greedy geographic routing                        | Fully distributed; highly sensitive to mobility; frequent route breaks; low infrastructure dependency | [22,24,67]                |
| Infrastructure-assisted routing    | RSU-assisted | V2I/I2V            | RSU-based forwarding; cluster-based routing; infrastructure relay | Improved route stability; lower latency; reliance on roadside infrastructure availability             | [9,26,29]                 |
| Hybrid routing schemes             | Partial RSU  | V2V + V2I          | Adaptive hybrid routing; multi-hop assisted routing               | Flexible communication selection; improved robustness; increased signaling and coordination overhead  | [23,33]                   |
| IoV backbone and multi-hop routing | RSU + Cloud  | I2I/RSU–Cloud      | SDN-based routing; centralized or hierarchical coordination       | High scalability; global traffic awareness; higher control complexity and energy cost                 | [89,90]                   |

Routing protocols without RSU support mainly rely on direct V2V communication and suffer from frequent route breaks and high control overhead under dense or highly mobile scenarios. In contrast, RSU-assisted routing enables more stable paths and improved quality of service through infrastructure coordination. Hybrid approaches attempt to balance flexibility and performance by dynamically switching between V2V and infrastructure-assisted routing. However, these solutions often introduce additional signaling overhead and energy consumption, highlighting a trade-off between routing efficiency and energy scalability in VANET–IoT deployments.

### 5.2. Routing and Energy Efficiency Challenges in VANET–IoT Networks

Vehicular routing in VANET–IoT environments faces significant challenges due to high node mobility, frequent topology changes, intermittent connectivity, and heterogeneous

communication technologies. Traditional MANET routing protocols are often unsuitable, as they fail to cope with rapid link breakage and dynamic vehicle density. In addition, the integration of IoT devices and RSUs introduces multi-hop, multi-domain routing paths that further complicate route discovery and maintenance [77–79].

Routing decisions in VANET–IoT networks are closely coupled with energy consumption, particularly for IoT devices, RSUs, and edge nodes. Frequent route updates, beaconing, and multi-hop forwarding increase communication overhead and energy usage [39,80]. This issue is especially critical in dense V2V scenarios and in IoT-assisted V2X communications, where energy-constrained roadside sensors and gateways must sustain continuous data exchange [81].

The impact of routing on energy efficiency varies depending on the communication paradigm. In V2V communications, routing protocols prioritize low-latency and link stability, often at the cost of increased signaling overhead. In contrast, V2I and RSU-assisted routing can offload routing complexity to infrastructure nodes, reducing vehicle side energy consumption but increasing RSU processing load. Hybrid V2X approaches aim to balance these trade-offs by dynamically selecting routing paths based on traffic density, energy constraints, and application requirements [36,38,82]. Future research should further investigate joint routing and energy-aware optimization strategies tailored to heterogeneous VANET–IoT communication modes.

### 5.3. Security and Privacy Challenges

Security and privacy remain fundamental obstacles to the deployment of large-scale VANET–IoT systems. The open wireless medium, the mobility of vehicles, and the heterogeneity of IoT devices create a broad and dynamic attack surface that increases the risk of message forgery, identity manipulation, data tampering, and unauthorized access. Moreover, the strict latency and reliability requirements of safety-critical applications complicate the integration of conventional cybersecurity frameworks. This subsection reviews key threat categories, evaluates existing mitigation mechanisms, and highlights the limitations of current security architectures in vehicular environments.

#### 5.3.1. Threat Landscape

VANET–IoT ecosystems are exposed to several classes of attacks due to their decentralized and highly mobile nature. Message falsification and injection attacks allow adversaries to disseminate forged hazard alerts, leading to traffic disturbances or intentional rerouting. Sybil attacks, in which a malicious node artificially generates multiple identities, distort traffic density estimations and compromise cooperative perception [87]. Eavesdropping and data interception exploit the broadcast nature of V2V and V2I communications, enabling attackers to monitor vehicle movements or extract sensitive information. Denial-of-Service (DoS) and jamming attacks target the physical or MAC layers, disrupting channel availability and degrading the performance of time-critical applications [85].

Finally, malware propagation through IoT devices or compromised RSUs can affect both the vehicular subsystem and the surrounding infrastructure.

#### 5.3.2. Limitations of Classical Cryptographic Mechanisms

Public-key cryptography (PKI) is widely adopted to ensure message authentication and integrity in V2X systems. However, its scalability and latency remain significant concerns. Certificate verification and revocation processes can introduce delays incompatible with real-time safety applications [88]. The reliance on centralized certificate authorities also creates bottlenecks and single points of failure. Lightweight cryptographic schemes have been proposed for constrained IoT devices, but the heterogeneity of devices further

complicates unified key management. Cross-domain trust establishment is particularly challenging when vehicles move across regions served by different operators or authorities.

### 5.3.3. Privacy and Pseudonymity Constraints

Protecting driver privacy is essential, as continuous broadcasts of location and sensor data can reveal sensitive movement patterns. Short-term pseudonyms aim to prevent long-term tracking, but frequent pseudonym changes generate synchronization overhead and require robust revocation strategies. IoT-assisted RSUs can help manage pseudonym updates, yet adversaries equipped with multi-sensor fusion techniques can still correlate vehicular behavior to re-identify users. Ensuring unlinkability while maintaining accountability remains a difficult trade-off [91].

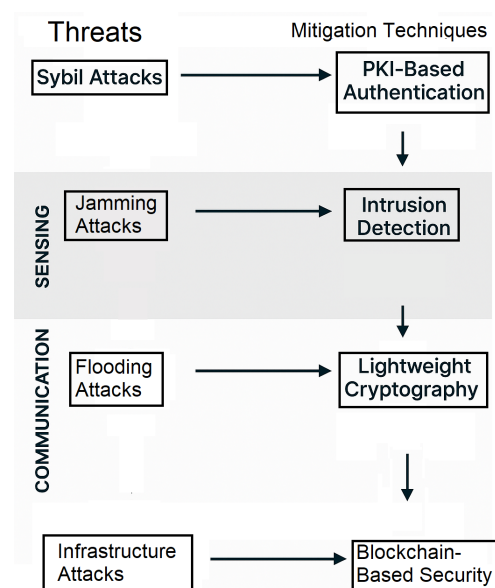
### 5.3.4. Blockchain-Based Security: Opportunities and Challenges

Blockchain technologies have attracted significant interest due to their auditability and resilience against tampering. Distributed ledgers can record pseudonym updates, certificate revocations, and event reports in a verifiable manner [92]. Lightweight consensus mechanisms such as PBFT or Delegated Proof-of-Stake have been proposed to reduce computational overhead. However, blockchain introduces its own challenges:

- (1) maintaining low latency under high mobility.
- (2) ensuring scalability as the ledger grows.
- (3) preventing congestion caused by simultaneous event reporting; and
- (4) addressing privacy issues arising from transparent records.

Hybrid architectures combining blockchain with edge computing have shown promise but remain at early stages of development.

Figure 9 summarizes the principal security threats affecting VANET-IoT systems—including Sybil attacks, message falsification, jamming/DoS, and infrastructure compromise—and maps them to widely adopted defense mechanisms such as PKI-based authentication, intrusion detection systems, lightweight cryptography, and blockchain. The flow highlights the need for multi-layer protection across sensing, communication, and infrastructure tiers.



**Figure 9.** Overview of major security threats and defense mechanisms in VANET-IoT systems.

Table 10 summarizes major security and privacy challenges affecting VANET-IoT integration documented in recent VANET-IoT literature [93–96]. It highlights how different

classes of attacks exploit the broadcast and distributed nature of V2X communication, and how weaknesses in trust management and privacy preservation impact system reliability.

**Table 10.** Security and privacy challenges in VANET–IoT systems.

| Challenge Category             | Description                                                              | Impact on VANET–IoT Systems                                                    | Representative References |
|--------------------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------------|---------------------------|
| Message Forgery and Injection  | Attackers generate false hazard or traffic messages                      | Disrupts cooperative safety; misleads routing; causes network instability      | [93,94]                   |
| Sybil Attacks                  | Nodes create false identities to manipulate the network                  | Distorts density estimation; weakens trust and reputation models               | [93]                      |
| Eavesdropping and Data Leakage | Interception of broadcast V2X messages                                   | Privacy violation; exposure of vehicle trajectories and behavioral patterns    | [96]                      |
| DoS and Jamming                | Saturation of wireless channels or RSUs                                  | Severely degrades latency; disrupts safety-critical message exchange           | [94]                      |
| Weak Key Management            | Inconsistent PKI deployment, constrained IoT devices, revocation delays  | Impacts authentication, trust establishment, and timely certificate revocation | [95]                      |
| Privacy and Re-identification  | Pseudonym-linking using multi-sensor fusion and side-channel information | Threatens driver and passenger privacy; requires frequent pseudonym change     | [96]                      |

### 5.3.5. Security Solutions for Dynamic and Low-Latency VANET–IoT Systems

Addressing security challenges in VANET–IoT systems requires solutions that can operate under stringent latency constraints, high node mobility, and dynamic network topology. Traditional centralized security mechanisms are often inadequate due to their reliance on persistent connectivity and high communication overhead. Consequently, recent research has focused on lightweight, distributed, and adaptive security solutions tailored to vehicular environments.

**Authentication and Trust Management:** Lightweight authentication mechanisms based on pseudonym certificates and public key infrastructure (PKI) remain widely adopted to ensure secure message exchange while preserving user privacy [67]. To reduce authentication latency, several approaches leverage short-lived pseudonyms and batch verification techniques, enabling rapid validation of safety messages in high-density traffic scenarios [72]. Trust management frameworks further complement authentication by dynamically assessing the reliability of vehicles and infrastructure nodes based on historical behavior and context awareness [16].

**Edge-Assisted Security Enforcement:** The integration of edge computing into VANET–IoT architectures enables security functions to be deployed closer to data sources. Roadside units (RSUs) can act as trusted edge nodes that perform real-time intrusion detection, misbehavior analysis, and access control enforcement with minimal delay. By offloading security-related processing from vehicles to RSUs or nearby edge servers, VANET–IoT systems can achieve faster threat detection while reducing the computational burden on on-board units [28,97].

**Blockchain-Based and Distributed Security Solutions:** Blockchain and distributed ledger technologies have been explored to provide decentralized trust establishment and tamper-resistant data sharing in VANET–IoT systems. Lightweight blockchain variants and consortium-based ledgers enable secure identity management, reputation tracking, and auditability without relying on a single trusted authority. However, their deployment must carefully balance security benefits against communication overhead and latency constraints, particularly for time-critical vehicular applications [66,98].

**Privacy-Preserving and Low-Latency Security Mechanisms:** To address privacy concerns, privacy-preserving authentication schemes such as pseudonym changing strategies and proxy re-encryption have been proposed [99]. These mechanisms aim to protect vehicle identities while maintaining low communication delay. Additionally, emerging approaches combine differential privacy and federated learning to enhance security analytics without exposing raw vehicular data, making them suitable for large-scale VANET-IoT deployments [97].

Overall, these solution-oriented approaches demonstrate that effective security in VANET-IoT systems requires a combination of lightweight cryptographic mechanisms, edge-assisted enforcement, and distributed trust models. Designing security solutions that jointly satisfy robustness, privacy preservation, and ultra-low latency remains a critical research direction for future intelligent transportation systems.

#### 5.4. Scalability and Mobility Management

Scalability and mobility management represent central challenges in VANET-IoT systems due to the highly dynamic and unpredictable nature of vehicular environments. As vehicle density fluctuates, communication links are frequently established and broken, producing rapid variations in network topology. These conditions significantly affect packet delivery reliability, channel contention, and computing resource allocation at both RSUs and edge servers. Ensuring that the system remains responsive under high density and high mobility is essential for supporting latency-sensitive applications such as cooperative perception and collision avoidance.

##### 5.4.1. Network Congestion and Density Fluctuations

In dense traffic scenarios—such as highways during rush hours or crowded urban intersections, simultaneous transmissions may saturate the wireless channel. High message arrival rates increase the likelihood of packet collisions, leading to degraded reliability and delayed delivery [99]. Furthermore, beaconing—periodic broadcasting of safety messages—escalates channel load when many vehicles occupy the same region. IoT-enabled RSUs may also become overloaded when processing multiple streams of sensor data from vehicles and environmental sensing devices.

Adaptive congestion control techniques have been proposed to mitigate this problem, including dynamic beaconing, transmit power adaptation, and priority-aware scheduling. However, most approaches require accurate, real-time estimation of traffic density, which remains difficult under rapidly changing mobility conditions.

##### 5.4.2. Dynamic Topology and Link Instability

High-speed mobility causes frequent link disruptions, making routing decisions particularly challenging. Traditional MANET routing protocols struggle to maintain route stability when vehicles travel at high speeds or move rapidly across RSU coverage zones [97]. IoT devices in the environment—such as cameras or weather stations—can help predict mobility patterns, but their spatial distribution is often sparse or irregular.

Multi-hop V2V routing is especially susceptible to link breaks, while V2I communication depends on the density and placement of RSUs. Maintaining reliable communication under such conditions requires both predictive mobility models and cross-layer optimization strategies that combine sensing, communication, and edge computation.

##### 5.4.3. Edge Resource Overload and Task Offloading Constraints

As more vehicles request cooperative services, edge servers may face resource contention, particularly in regions with high traffic density. Computationally expensive tasks—such as trajectory prediction, sensor fusion, and image processing—can overload

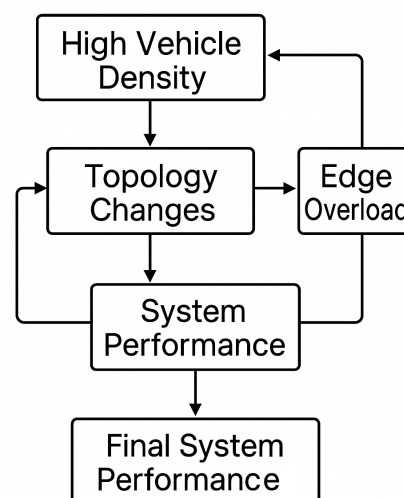
MEC servers, causing increased latency. Task offloading strategies must therefore account for available computing power, channel conditions, and vehicle mobility to avoid congestion at the edge [100].

Several studies propose learning-based approaches to predict future workload and distribute tasks among multiple edge nodes. However, these models require accurate mobility forecasts and sufficient training data, both of which remain difficult to obtain in large-scale deployments.

#### 5.4.4. Multi-Domain Scalability Challenges

VANET-IoT systems operate across multiple domains—communication, sensing, computing, and storage—which scale differently as the number of vehicles and IoT nodes increases. Cloud systems can handle large datasets but suffer from higher delays, while edge nodes offer low latency but limited computing capacity. Achieving a balanced allocation of tasks remains an open research problem.

Figure 10 illustrates the main scalability and mobility challenges in VANET-IoT systems. High vehicle density increases channel contention, topology changes cause frequent link disruptions, and edge server overload leads to variable processing delays. Together, these factors degrade overall system performance and create a cyclical feedback loop that must be addressed through adaptive congestion control, mobility prediction, and coordinated edge resource management.



**Figure 10.** Scalability and mobility challenges in VANET-IoT systems.

In addition, integrating heterogeneous IoT platforms—each with different communication standards, sampling rates, and data formats—introduces scalability issues at both the data management and application layers.

Table 11 summarizes the main scalability and mobility challenges in VANET-IoT systems, outlining their root causes, common mitigation techniques, and key limitations [29,101–105]. It highlights the need for adaptive congestion control, predictive mobility modeling, and coordinated edge resource management. In addition to network congestion and edge overload, routing overhead and energy scalability emerge as critical challenges in large-scale VANET-IoT deployments.

**Table 11.** Scalability challenges in VANET–IoT deployments and their typical mitigation approaches.

| Challenge                | Cause                                                                                       | Common Approaches                                                                                          | Key Limitations                                                                                | Representative References |
|--------------------------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|---------------------------|
| Network Congestion       | High vehicle density; overlapping wireless transmissions                                    | Adaptive beaconing, transmit power control, priority scheduling                                            | Requires accurate density estimation; unstable under fast-changing traffic                     | [101]                     |
| Link Instability         | High-speed mobility; RSU boundary transitions                                               | Mobility prediction, cross-layer routing protocols, multi-hop V2V communication                            | Prediction errors significantly degrade handover performance                                   | [102]                     |
| Edge Overload            | Simultaneous offloading by many vehicles                                                    | Load balancing, multi-edge coordination, task partitioning schemes                                         | Edge capacity remains limited; latency still fluctuates in dense scenarios                     | [103]                     |
| Multi-domain Scalability | Heterogeneous IoT + VANET + cloud–edge layers                                               | Hierarchical architectures, distributed caching, clustering algorithms                                     | High orchestration complexity; interoperability across domains is difficult                    | [101–103]                 |
| Routing Overhead         | Frequent topology changes; route discovery and broadcast storms in dense VANET–IoT networks | Geographic and position-based routing, RSU-assisted routing, clustering-based routing, SDN-enabled control | Control signaling overhead remains high; scalability degrades under high mobility              | [29,104]                  |
| Energy Scalability       | Continuous sensing, communication, and computation by vehicles, RSUs, and IoT devices       | Edge-assisted processing, energy-aware routing, adaptive duty cycling, cloud–edge task offloading          | Energy savings trade off with latency and reliability; limited battery capacity of IoT devices | [105]                     |

### 5.5. Interoperability and Standardization Issues

Interoperability is a central challenge in the deployment of large-scale VANET–IoT systems. Vehicles, roadside units, and IoT devices originate from different vendors, operate under distinct communication standards, and exchange heterogeneous data formats. This diversity complicates cross-platform operation and reduces the reliability of cooperative applications. Achieving seamless interoperability across sensing, communication, networking, and application layers is therefore critical for creating a unified, scalable, and dependable vehicular ecosystem.

#### 5.5.1. Heterogeneous Communication Technologies

Modern vehicular environments combine IEEE 802.11p/DSRC, LTE-V2X, NR-V2X, Wi-Fi, Bluetooth, ZigBee, and LoRaWAN depending on the device type and communication range. While this diversity increases flexibility, it also introduces compatibility issues. DSRC and C-V2X follow fundamentally different channel access mechanisms, making coexistence and interoperability difficult without additional coordination layers [106]. Similarly, IoT devices using lightweight protocols such as MQTT or CoAP may not natively integrate with V2X safety messaging standards, requiring translation or gateway-based adaptation.

#### 5.5.2. Semantic and Data-Level Incompatibilities

Even when communication links are established, the meaning, structure, and granularity of exchanged data may not align. Vehicles produce high-rate sensor streams, while IoT devices often rely on low-frequency environmental measurements. Differences in message formats—such as Cooperative Awareness Messages (CAMs), Basic Safety Messages (BSMs), and IoT sensor payloads—require semantic harmonization to avoid misinterpretation or

data loss. Without common data models, cooperative perception and decision-making processes suffer degradation due to inconsistent or incomplete information [98].

### 5.5.3. Multi-Layer Standardization Gaps

Current V2X and IoT standards provide fragmented guidance across the protocol stack. While standards bodies such as ETSI, IEEE, and 3GPP define communication rules, they offer limited support for multi-layer interactions. Application-layer standardization remains weak, resulting in incompatible APIs, inconsistent data sampling rates, and divergent system configurations. Interoperability testing across vendors is also insufficient, making large-scale deployment error-prone and costly [107].

### 5.5.4. Cross-Domain Integration Challenges

Full integration of VANET and IoT infrastructures requires harmonizing two distinct technological domains. IoT systems prioritize low power consumption, simple communication, and high device heterogeneity. In contrast, VANET applications demand ultra-low latency, strong reliability, and high mobility support. Aligning these conflicting requirements is challenging. For example, IoT devices may not generate data at a frequency sufficient to support real-time driving decisions, while vehicles may overload IoT gateways with high-rate sensor flows.

Hybrid architectures—combining edge processing, protocol translation, and semantic middleware—have been proposed, but achieving full interoperability remains an open problem. Continuous standardization efforts and cross-industry collaboration are necessary to ensure consistent behavior across devices and infrastructures.

Table 12 outlines major interoperability challenges in VANET–IoT systems, covering communication, data, and application layers, as discussed in [29,104,105]. It highlights how fragmented standards and heterogeneous technologies hinder large-scale, reliable integration.

**Table 12.** Interoperability challenges in VANET–IoT ecosystems.

| Challenge Type                        | Description                                                     | Impact on System Performance                                              | Representative References |
|---------------------------------------|-----------------------------------------------------------------|---------------------------------------------------------------------------|---------------------------|
| Heterogeneous Communication Standards | Coexistence of DSRC, LTE-V2X, NR-V2X, Wi-Fi, and IoT protocols  | Connectivity inconsistencies; dependence on protocol translation gateways | [29]                      |
| Semantic Incompatibility              | Different message formats (CAM, BSM, IoT payloads)              | Conflicts in cooperative perception and decision-making processes         | [104]                     |
| Application-Layer Fragmentation       | Divergent APIs, update cycles, sampling rates across vendors    | Weak cross-vendor interoperability; inconsistent application behavior     | [105]                     |
| Cross-Domain Integration              | IoT: low-power, intermittent; VANET: low-latency, high-mobility | Mismatch in data frequency, reliability, and QoS requirements             | [29,104,105]              |

### 5.6. Practical Deployment Challenges and Standardization Issues

Despite significant advances in VANET–IoT research, the large-scale deployment of IoV systems in real-world environments remains challenging. One of the primary practical issues concerns the management of massive and heterogeneous data streams generated by vehicles, roadside infrastructure, and IoT sensors. These data flows vary in volume, velocity, and reliability, placing considerable pressure on edge and cloud resources for real-time processing, storage, and analytics [10].

Another major challenge lies in the integration of heterogeneous systems across different vendors, communication technologies, and regional regulations. VANET–IoT deployments often rely on a combination of DSRC, C-V2X, cellular networks, and IoT protocols, which complicates interoperability and system coordination. Differences in hardware capa-

bilities, software platforms, and communication stacks further exacerbate these integration issues, particularly in cross-border or multi-city deployments [1,11].

Standardization plays a critical role in addressing these challenges. While ongoing efforts by standardization bodies have contributed to harmonizing V2X and IoT communication frameworks, practical deployment still faces gaps in unified data models, interface definitions, and cross-layer coordination mechanisms [13,14]. Without consistent standards, achieving seamless interoperability and scalable deployment across heterogeneous environments remains difficult [30].

These practical constraints highlight the need for deployment-aware architectures that jointly consider data management, interoperability, and standardization. Addressing these issues is essential for transitioning VANET-IoT systems from experimental testbeds to reliable, large-scale intelligent transportation infrastructures

In addition to deployment-related interoperability challenges, recent standardization efforts have contributed to improving cross-domain integration in VANET-IoT systems. On the communication side, initiatives such as ETSI ITS-G5 and 3GPP C-V2X have established common foundations for V2X connectivity, with ongoing evolution toward NR-V2X to support higher reliability and scalability [14,30]. However, the coexistence of multiple access technologies and regional regulatory differences continues to hinder seamless interoperability across deployments.

From a data perspective, standard message formats such as Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs) enable basic safety information exchange, yet higher-level data generated by heterogeneous IoT sensors and edge analytics platforms still lack unified semantic models and standardized data representations. This limitation complicates cross vendor data fusion and large-scale system integration. Despite progress toward service oriented architectures and middleware-based solutions, achieving end-to-end standardization across communication protocols, data formats, and computing layers remains an open challenge for practical VANET-IoT deployments.

### 5.7. Human Factors and Ethical Considerations

As IoV systems become increasingly integrated into daily transportation, human factors and ethical considerations emerge as critical challenges beyond purely technical aspects. Driver acceptance and trust in connected and autonomous vehicle technologies significantly influence deployment success. Issues related to human-machine interaction, such as information overload, interface usability, and situational awareness, directly affect safety and user confidence in VANET-IoT-enabled systems [82].

Ethical concerns also play a central role in the evolution of IoV ecosystems. Data ownership and privacy are particularly sensitive, as vehicles continuously collect and exchange location, behavioral, and environmental data [67]. Ensuring transparent data governance and protecting users from unauthorized data exploitation remain open challenges, especially in large-scale and cross-jurisdictional deployments [91].

Moreover, algorithmic bias in data-driven traffic management and decision-making systems may lead to unfair or suboptimal outcomes for certain user groups or regions. These concerns are amplified by the increasing reliance on machine learning and distributed intelligence at the edge. In addition, liability and accountability issues in accident scenarios involving autonomous or semi-autonomous vehicles remain largely unresolved, raising complex legal and ethical questions [87,106].

Addressing human and ethical factors requires interdisciplinary approaches that combine technical design with regulatory frameworks and user-centered methodologies.

Incorporating these considerations into VANET–IoT research is essential for developing socially acceptable, trustworthy, and sustainable IoV systems.

### 5.8. Energy and Resource Constraints

Energy and resource constraints constitute another major barrier to the deployment of large-scale VANET–IoT systems. While vehicles typically have access to ample power, roadside IoT devices, environmental sensors, and edge nodes often operate under strict energy budgets. In addition, the continuous flow of high-rate sensor data, cooperative perception exchanges, and task offloading requests impose significant computational and communication burdens on edge servers and network infrastructure. Ensuring energy-efficient operation across heterogeneous devices is therefore crucial for maintaining long-term sustainability and reliable service quality.

#### 5.8.1. Energy Limitations of IoT and Roadside Devices

Many IoT sensors deployed along roadsides or embedded in urban infrastructure run on batteries or energy-harvesting modules. These devices must balance sensing frequency, communication overhead, and local processing demands. High-frequency sampling can quickly drain available power, while infrequent sampling may produce outdated or incomplete environmental information. Furthermore, protocols such as MQTT, CoAP, and LoRaWAN have different energy footprints, making it challenging to define unified communication strategies suitable for all device types [108].

#### 5.8.2. Computational Constraints and Offloading Overheads

Task offloading is widely used to reduce the workload on vehicles by transferring compute-intensive tasks—such as object detection or multi-vehicle data fusion—to MEC servers. However, offloading itself carries energy and latency costs. Transmitting large sensor frames consumes substantial power, and frequent offloading can overwhelm edge servers, degrading the performance of latency-sensitive applications [109]. Additionally, fluctuating vehicle mobility complicates scheduling decisions, since a task may not be completed before the vehicle leaves the coverage of the serving edge node.

#### 5.8.3. Resource Fragmentation Across the Cloud–Edge–Vehicle Continuum

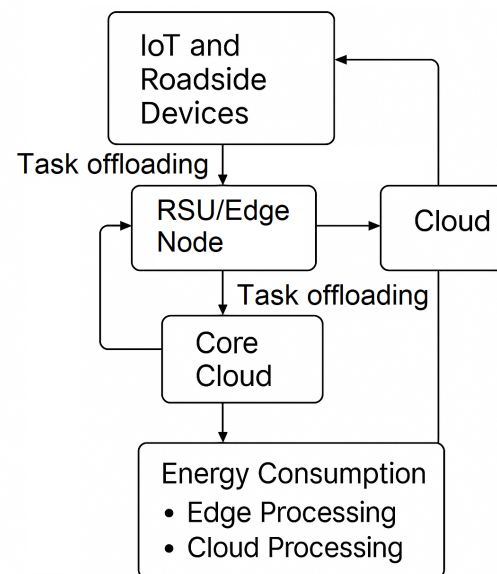
VANET–IoT systems rely on distributed computation across cloud servers, multiple edge nodes, and in-vehicle platforms. These resources differ significantly in capacity, availability, and connectivity. Without coordinated orchestration, tasks may be assigned to overloaded nodes, resulting in inefficient energy use and unpredictable delays. Recent efforts propose hierarchical task scheduling models and energy-aware resource allocation to distribute computation more effectively, but cross-layer optimization remains an open research problem [110].

#### 5.8.4. Energy-Aware Communication and Sensing Strategies

Energy efficiency must also be addressed at the communication level. Adaptive transmission power control can extend device lifetime, but it must be balanced with link reliability and safety requirements. Similarly, context-aware sensing strategies—where sensors adjust sampling rates based on environmental conditions—can reduce unnecessary measurements and communication overhead. AI-based predictive models have been explored to dynamically tune sensing frequencies and offloading decisions based on mobility patterns, expected workload, or predicted battery levels [111].

Figure 11 illustrates how energy consumption and computational load are distributed across IoT roadside devices, RSU/edge nodes, and cloud servers in VANET–IoT systems. Task offloading occurs at multiple stages, and each step in the chain introduces additional

energy costs. The diagram highlights the need for energy-aware sensing, communication, and computation strategies.



**Figure 11.** Energy and computation flow across IoT devices, edge nodes, and cloud servers in VANET-IoT systems.

Table 13 summarizes major energy and resource challenges in VANET-IoT systems, drawing from studies [17,36,53,103]. It outlines the causes of energy constraints across heterogeneous devices and computing tiers, and highlights representative mitigation strategies along with their intrinsic limitations. Addressing these challenges requires coordinated optimization across sensing, communication, and computation layers.

**Table 13.** Energy-related challenges in VANET-IoT systems and common mitigation strategies.

| Challenge                     | Underlying Cause                                                         | Mitigation Strategies                                                               | Limitations                                                                             | Representative References |
|-------------------------------|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|---------------------------|
| IoT Device Energy Constraints | Battery-powered roadside sensors; limited energy harvesting              | Adaptive sensing frequency; duty cycling; low-power communication protocols         | Reduced sensing accuracy under low sampling rates                                       | [36]                      |
| Offloading Overhead           | High-rate sensing workloads; large payload transmissions to edge servers | Selective offloading; data compression; cooperative filtering among nearby vehicles | Transmission energy cost remains high; mobility interruptions break offloading sessions | [17]                      |
| Resource Fragmentation        | Distributed resources across vehicle, edge, and cloud tiers              | Hierarchical scheduling; energy-aware resource allocation mechanisms                | Requires accurate workload prediction; coordination overhead between domains            | [103]                     |
| Communication Energy Cost     | Transmission power scaling; multi-hop V2X forwarding                     | Power control; context-aware transmission scheduling                                | Trade-off between link reliability and energy savings                                   | [53]                      |

## 6. Comparative Study

This section synthesizes the main architectural, communication, and protocol-level considerations of VANET–IoT integration. While previous sections have examined technical components individually, the goal here is to provide a cross-dimensional comparison that highlights the trade-offs and complementarities between existing approaches. The comparative analysis is organized into three perspectives: (1) cloud-, edge-, and hybrid-based architectures; (2) V2X communication technologies; and (3) IoT data exchange protocols. Each comparison aims to clarify the strengths, limitations, and suitability of different technologies for VANET–IoT applications.

### 6.1. Cloud-Based, Edge-Based, and Hybrid Architectures

Architectural choices significantly affect the performance, scalability, and responsiveness of integrated VANET–IoT systems. Cloud-based architectures offer substantial computational power, large-scale analytics, and global context awareness. They are well suited for applications involving long-term traffic modeling, HD map generation, and historical data aggregation [89]. However, their reliance on backhaul connectivity introduces latency that limits their effectiveness for safety-critical tasks.

In contrast, edge-based architectures provide low-latency processing by executing computation closer to vehicles, typically through RSUs or MEC servers. These architectures are ideal for real-time tasks such as cooperative perception, collision avoidance, and local anomaly detection [90]. Their main limitations stem from constrained computational capacity and uneven geographic deployment.

Hybrid architectures combine cloud and edge strengths by distributing workload based on latency requirements, computational complexity, and mobility context. Time-sensitive tasks can be executed at the edge, while the cloud handles storage-intensive or computation-heavy workloads. This distributed model is increasingly recognized as a promising foundation for next-generation intelligent transportation systems, though it introduces challenges related to task orchestration, model synchronization, and cross-layer coordination [112].

### 6.2. Comparison of V2X Communication Technologies

V2X connectivity is fundamental to enabling cooperation between vehicles, infrastructure, and IoT devices. DSRC (IEEE 802.11p) provides low-latency broadcast communication and has been widely studied due to its simplicity and decentralized operation. It performs well under moderate vehicle density but suffers from channel contention and packet collisions in congested environments [113].

LTE-V2X and NR-V2X, standardized by 3GPP, offer enhanced reliability and communication range. LTE-V2X supports both direct sidelink communication and network-assisted connectivity, enabling broader service coverage. NR-V2X enhances scheduling flexibility, quality-of-service management, and the ability to support cooperative perception through high-throughput links [114]. However, these cellular technologies depend on operator-managed infrastructure, which may not be uniformly available across all regions.

From an IoT integration perspective, the coexistence of DSRC, LTE-V2X, cellular IoT, Wi-Fi, and LPWAN introduces interoperability challenges. Each technology offers distinct trade-offs in terms of latency, range, bandwidth, and deployment cost. Selecting the appropriate communication technology depends on application requirements and the density and capabilities of roadside infrastructure.

### 6.3. IoT Communication Protocols: MQTT, CoAP, and DDS

IoT data exchange protocols further influence the efficiency and reliability of VANET–IoT systems. MQTT, a lightweight publish/subscribe protocol, is widely used for cloud-centric communication and asynchronous data dissemination. Its low overhead and scalability make it suitable for environmental monitoring and vehicle-to-cloud data flows, although its reliance on a broker introduces a single point of failure [93].

CoAP, designed for constrained devices, enables request/response communication over UDP and supports confirmable messaging. It is typically used in roadside IoT nodes where low-power operation is essential [94]. CoAP is effective for event-driven sensing but may require additional adaptation layers to interact with V2X safety messages.

DDS (Data Distribution Service) provides real-time publish/subscribe communication with fine-grained quality-of-service control. DDS is increasingly used in autonomous driving platforms to support deterministic data sharing among sensors, control modules, and perception systems [95]. However, DDS implementations tend to be computationally demanding compared to MQTT and CoAP.

Table 14 provides a comparative analysis of architecture options, V2X technologies, and IoT protocols based on recent contributions [28,33–35,42,54,55]. It highlights the strengths and limitations of cloud-, edge-, and hybrid-based computing models; compares major V2X technologies; and contrasts the characteristics of common IoT protocols based on their suitability for vehicular applications.

**Table 14.** Comparison of architectural, communication, and protocol design options in VANET–IoT systems.

| Category       | Option         | Strengths                                                    | Limitations                                     | Best Use Cases                                          | Representative References |
|----------------|----------------|--------------------------------------------------------------|-------------------------------------------------|---------------------------------------------------------|---------------------------|
| Architecture   | Cloud-Based    | High computational power; large-scale analytics              | High latency; backhaul dependency               | Traffic prediction; HD map generation; global analytics | [35]                      |
| Architecture   | Edge-Based     | Low latency; supports real-time decisions                    | Limited computing capacity; uneven RSU coverage | Cooperative perception; safety-critical tasks           | [55]                      |
| Architecture   | Hybrid         | Balanced latency and scalability; flexible task distribution | Complex orchestration; synchronization overhead | Integrated ITS platforms; mixed workloads               | [42]                      |
| V2X Technology | DSRC (802.11p) | Low latency; decentralized operation                         | Performance degradation in dense traffic        | Local safety alerts; short-range broadcasts             | [33]                      |
| V2X Technology | LTE-V2X/NR-V2X | High reliability; long range; QoS control                    | Requires operator infrastructure                | Cooperative perception; high-mobility scenarios         | [28]                      |
| IoT Protocols  | MQTT           | Lightweight; scalable; cloud-friendly publish/subscribe      | Broker dependency; not real-time                | Environmental sensing; telemetry data                   | [34]                      |
| IoT Protocols  | CoAP           | Energy-efficient; ideal for constrained devices              | Limited QoS; adaptation needed for V2X          | Roadside sensing; low-power IoT nodes                   | [34]                      |
| IoT Protocols  | DDS            | Real-time operation; deterministic QoS control               | Higher computational cost                       | Autonomous driving; multi-sensor fusion                 | [54]                      |

### 6.4. Critical Discussion and Comparative Insights

Beyond this comparison, existing VANET–IoT studies exhibit notable differences in design priorities, assumptions, and performance trade-offs. Architectures emphasizing

cloud-centric processing provide global coordination and powerful analytics but suffer from increased latency and limited suitability for safety-critical applications. In contrast, edge-based and RSU-assisted approaches significantly reduce response time and improve local adaptability, at the expense of partial network visibility and constrained computational resources.

From a communication perspective, DSRC-based solutions favor deterministic latency and mature safety messaging, whereas cellular V2X and NR-V2X approaches enhance scalability, coverage, and integration with mobile networks. However, the latter introduce dependency on network operators and raise coexistence challenges in heterogeneous deployments.

Similarly, AI-driven and learning-based approaches outperform traditional rule-based methods in terms of adaptability and decision accuracy, particularly in dynamic traffic environments. Nevertheless, they introduce challenges related to model complexity, training data availability, explainability, and communication overhead. These observations highlight that no single solution is optimal across all VANET–IoT scenarios, reinforcing the need for hybrid and adaptive system designs.

## 7. Future Research Directions

The integration of VANET and IoT technologies continues to evolve rapidly, driven by advances in wireless communication, distributed intelligence, and large-scale sensing infrastructures. Although current systems already demonstrate significant capabilities in cooperative awareness, traffic management, and environmental monitoring, emerging technologies have the potential to reshape the architectural and operational foundations of next-generation intelligent transportation systems. This section outlines promising research directions, focusing on foundational technological shifts, innovative use cases, and key open challenges that must be addressed to fully realize the vision of connected, autonomous, and sustainable mobility.

### 7.1. Foundational Advancements

#### 7.1.1. 5G Versus 6G Challenges in VANET–IoT Communications

Although 5G technologies have significantly improved latency, bandwidth, and reliability for V2X communications, several challenges remain in large-scale VANET–IoT deployments [30]. Ultra-reliable low-latency communication (URLLC) is difficult to guarantee under high-mobility and dense traffic conditions, while frequent handovers introduce signaling overhead and potential service interruption. Moreover, 5G networks rely heavily on centralized control and dense infrastructure deployment, which limits scalability and increases operational complexity for heterogeneous IoT-integrated vehicular environments [96].

6G-enabled VANET–IoT communications aim to overcome these limitations by introducing sub-THz communications, AI-native networking, integrated sensing and communication, and ultra-massive connectivity [115]. However, these advances also introduce new challenges, including severe propagation loss at high frequencies, increased energy consumption, complex resource management, and the need for intelligent coordination across vehicles, RSUs, edge, and cloud domains. Ensuring reliability, security, and energy efficiency in such highly dynamic and intelligent 6G-enabled vehicular networks remains an open research challenge [45]. Bridging the gap between 5G limitations and 6G ambitions will require cross-layer design, energy-aware networking, and intelligent orchestration tailored to VANET–IoT systems.

#### 7.1.2. 6G-Enabled Vehicular Intelligence

The emergence of 6G networks introduces new opportunities for VANET–IoT integration through sub-THz communication, ultra-low latency, holographic beamforming,

and AI-native network control. 6G architectures aim to support extremely dense connectivity with millisecond-level reliability, enabling fine-grained cooperative perception, high-definition map sharing, and swarm-level decision-making [96]. For vehicular applications, these features can significantly enhance sensing fidelity, reduce communication uncertainty, and facilitate dynamic coordination among vehicles, RSUs, drones, and cloud services.

#### 7.1.3. Reconfigurable Intelligent Surfaces (RISs)

RIS technology allows the propagation environment itself to be dynamically manipulated. Programmable reflecting surfaces can correct non-line-of-sight conditions, reshape radio beams, and extend communication coverage in dense urban areas [115]. Incorporating RISs into vehicular networks could mitigate blockage caused by buildings, trucks, or adverse weather, enabling more reliable high-frequency communication between vehicles and infrastructure.

#### 7.1.4. Joint Communication and Sensing (JCAS)

JCAS systems aim to unify radar sensing and communication into a single hardware and waveform framework. For vehicular networks, this enables simultaneous data exchange and real-time perception, reducing hardware redundancy and improving spectral efficiency. Emerging research explores cooperative JCAS, where vehicles jointly sense the environment and share sensing information through V2X links, unlocking new possibilities for collaborative driving and high-resolution environmental reconstruction.

#### 7.1.5. Neuro-Symbolic and Federated Vehicular AI

Traditional deep learning struggles with explainability and cross-domain generalization. Neuro-symbolic AI—which combines neural reasoning with logical structures—offers the potential for safer, more transparent decision-making in vehicular environments [101]. Furthermore, federated learning (FL) provides a privacy-preserving approach to training AI models across distributed vehicles and edge nodes without sharing raw data. Integrating FL with vehicular edge computing may enable continuously updated perception and prediction models tailored to local traffic conditions.

#### 7.1.6. Quantum-Assisted Vehicular Computing

Although still exploratory, quantum pre-processing and quantum-inspired optimization could accelerate complex vehicular tasks such as multi-agent planning, resource allocation, and secure cryptographic operations [102]. These capabilities may become increasingly relevant as cooperative perception and V2X data volumes continue to grow.

### 7.2. Artificial Intelligence and Machine Learning in VANET-IoT Systems

Artificial intelligence and machine learning have become key enablers for enhancing perception, prediction, and decision-making capabilities in VANET-IoT systems. By leveraging heterogeneous data collected from vehicles, roadside infrastructure, and IoT sensors, AI-driven approaches enable intelligent transportation systems to operate more autonomously, efficiently, and adaptively in highly dynamic environments.

#### 7.2.1. AI/ML for Cooperative Perception

In VANET-IoT environments, cooperative perception aims to overcome the limitations of individual vehicle sensors by fusing data from multiple sources, including on-board units, roadside cameras, radar sensors, and other IoT devices. Deep learning techniques, such as convolutional neural networks and sensor fusion models, are widely used to enhance object detection, tracking, and classification accuracy [18]. By performing perception tasks collaboratively through Vehicle-to-Vehicle and Vehicle-to-Infrastructure communication,

AI-enabled cooperative perception improves situational awareness in complex scenarios, particularly at urban intersections and in non-line-of-sight conditions [36].

#### 7.2.2. AI/ML for Traffic and Mobility Prediction

Prediction plays a crucial role in proactive traffic management and resource allocation within VANET-IoT systems. Machine learning models, including recurrent neural networks, graph-based learning, and spatio-temporal prediction techniques, are employed to forecast traffic flow, vehicle mobility patterns, and congestion evolution. These predictive capabilities support anticipatory decision-making at both edge and cloud levels, enabling more efficient routing, adaptive traffic signal control, and improved quality of service under varying traffic conditions [43,79].

#### 7.2.3. AI/ML for Decision-Making and Resource Management

Decision-making in VANET-IoT systems involves selecting optimal actions under strict latency and reliability constraints. Reinforcement learning and deep reinforcement learning approaches have been extensively investigated to address decision-making problems such as task offloading, routing optimization, spectrum allocation, and cooperative control. By continuously learning from environmental feedback, AI-driven decision-making mechanisms can adapt to network dynamics, vehicle mobility, and workload variations. When deployed at edge nodes such as RSUs, these mechanisms enable near-real-time control decisions while reducing reliance on centralized cloud processing [116].

Overall, AI and ML techniques significantly enhance the intelligence and adaptability of VANET-IoT systems by enabling data-driven perception, predictive analytics, and autonomous decision-making. However, their deployment also introduces challenges related to model complexity, training data availability, communication overhead, and trustworthiness, highlighting the need for lightweight, explainable, and edge-aware AI solutions in future vehicular networks.

### 7.3. Emerging Use Cases

#### 7.3.1. Aerial and Space-Assisted Vehicular Networks (A-V2X)

Future transportation systems will increasingly rely on aerial platforms such as UAVs, stratospheric balloons, and low-Earth-orbit satellites. These platforms can extend connectivity to rural areas, assist in incident detection, and provide rapidly deployable communication infrastructure during emergencies [103]. Integrating airborne sensing with ground-level vehicular data enables multi-layer situational awareness and enhances resilience.

#### 7.3.2. Industrial Vehicle-to-Everything (IV2X)

Beyond urban mobility, V2X technologies are expanding into industrial environments, including warehouses, ports, and smart logistics hubs. Automated guided vehicles, drones, and robotic equipment require deterministic latency and precise coordination. IoT-enhanced V2X communication can support collision avoidance, task orchestration, and digital-twin-based operational optimization [29].

#### 7.3.3. Metaverse-Driven Simulation and Digital Twins

The convergence of VANET-IoT systems with metaverse-based digital twins offers powerful tools for modeling large-scale transportation systems [104]. These environments integrate real-time data from vehicles and IoT sensors with virtual simulation platforms, enabling scenario testing, predictive maintenance, and hybrid human-machine interaction models. Such systems can support infrastructure planning, fleet optimization, and proactive traffic policy design.

#### 7.3.4. Extended Reality (XR) for Cooperative Driving

Emerging XR interfaces can assist drivers, pedestrians, and road workers by overlaying situational information onto the physical environment. Combined with V2X communication, XR systems may provide real-time hazard visualization, augmented navigation cues, and collaborative driving assistance [105].

#### 7.4. Open Research Challenges for Future VANET–IoT

Despite the rapid progress outlined above, several open research questions remain central to the advancement of next-generation vehicular networks.

##### 7.4.1. AI Trustworthiness and Safety Guarantees

As AI becomes embedded in perception, prediction, and planning modules, ensuring transparency, robustness, and certifiable safety remains challenging. Methods for verifying AI components under extreme mobility, diverse environments, and rare events are still immature.

##### 7.4.2. Spectrum Coexistence and High-Frequency Reliability

6G and sub-THz communications require reliable propagation under mobility, but susceptibility to blockage and reflection poses challenges. Effective coexistence between DSRC, C-V2X, NR-V2X, Wi-Fi, and IoT protocols must also be ensured through adaptive spectrum sharing and interference management.

##### 7.4.3. Large-Scale Digital Twin Synchronization

Digital twin-enabled transport systems need continuous synchronization between physical and virtual environments. Achieving this at city scale requires highly efficient data ingestion pipelines, semantic consistency, and coordinated updates between vehicles, IoT sensors, and cloud platforms.

##### 7.4.4. Cross-Domain Privacy and Data Governance

Future VANET–IoT ecosystems must integrate heterogeneous data from public agencies, private fleets, individual vehicles, drones, and roadside IoT sensors. Ensuring privacy while maintaining data utility for learning and optimization remains an open challenge that requires advances in differential privacy, federated learning, and policy-driven data governance.

Table 15 highlights emerging research directions shaping future VANET–IoT systems, with representative examples from [96,101–105,115]. It highlights emerging technologies, their expected contributions to vehicular ecosystems, and the remaining scientific challenges that must be addressed in upcoming research.

**Table 15.** Emerging technologies and future research directions in VANET–IoT systems.

| Technology / Direction                     | Expected Contribution                               | Key Open Problems                                                | Representative References |
|--------------------------------------------|-----------------------------------------------------|------------------------------------------------------------------|---------------------------|
| 6G Networks                                | Ultra-low latency; sub-THz links; AI-native control | Reliability under high mobility; spectrum coexistence challenges | [96]                      |
| Reconfigurable Intelligent Surfaces (RISs) | Improved coverage; dynamic beam reconfiguration     | Optimal surface placement; real-time adaptation and control      | [115]                     |
| JCAS (Joint Communication and Sensing)     | Unified communication and sensing framework         | Hardware integration; multi-vehicle cooperative sensing          | [101]                     |

Table 15. Cont.

| Technology / Direction              | Expected Contribution                                       | Key Open Problems                                         | Representative References |
|-------------------------------------|-------------------------------------------------------------|-----------------------------------------------------------|---------------------------|
| Neuro-Symbolic and Federated AI     | Explainable models; privacy-preserving distributed learning | Model drift; formal verification; device heterogeneity    | [101]                     |
| Quantum-Assisted Optimization       | Faster resource allocation, routing, and planning           | Hardware immaturity; scalability limits                   | [102]                     |
| Aerial V2X (UAV-Assisted)           | Extended coverage; improved resilience in emergencies       | Handover complexity; routing stability at altitude        | [103]                     |
| Digital Twins and Metaverse Systems | Real-time simulation; predictive ITS management             | Synchronization overhead; semantic consistency            | [104]                     |
| XR-Assisted Driving                 | Enhanced environmental awareness; collaborative safety      | Latency constraints; human-machine interaction challenges | [105]                     |

## 8. Conclusions

This survey examined the technological, architectural, and operational foundations of VANET–IoT integration and highlighted its transformative potential for future intelligent transportation systems. By analyzing communication models, computing paradigms, and protocol choices, the study showed that the evolution toward the Internet of Vehicles relies on a coordinated interplay between cloud, edge, and in-vehicle computing. Technologies such as C-V2X and NR-V2X, when combined with IoT-driven sensing and adaptive offloading mechanisms, are essential to meeting the stringent latency, reliability, and scalability requirements of cooperative mobility.

Across the system stack, the review identified security, interoperability, mobility-induced instability, and energy constraints as persistent challenges. These issues are not independent; rather, they form an interconnected landscape in which improvements at one layer influence—and often depend on—advances at others. Addressing these challenges requires unified approaches that combine lightweight security mechanisms, standardized data models, intelligent resource allocation, and cross-layer optimization strategies. Looking ahead, emerging technologies such as 6G communication, reconfigurable intelligent surfaces, joint communication-and-sensing frameworks, AI-enhanced digital twins, and quantum-assisted optimization have the potential to reshape the design of vehicular networks. At the same time, new application domains, including aerial V2X, industrial automation, and metaverse-enabled simulation, will demand unprecedented levels of integration between vehicles, infrastructure, and distributed sensing systems.

Realizing this vision will require sustained research efforts focused on trustworthy AI, large-scale interoperability, comprehensive standardization, and energy-efficient architecture. By addressing these open issues, the integration of VANET and IoT can evolve from an emerging paradigm into a robust and pervasive foundation for safe, efficient, and sustainable transportation ecosystems.

**Author Contributions:** Conceptualization, K.K. and S.N.; Methodology, K.K. and S.N.; Formal Analysis, K.K. and L.B.; Investigation, K.K., L.B. and H.B.; Resources, S.N. and H.B.; Data Curation, L.B. and H.B.; Writing—Original Draft Preparation, K.K.; Writing—Review and Editing, S.N., L.B. and H.B.; Visualization, K.K.; Supervision, S.N. and H.B.; Project Administration, K.K. and S.N. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

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

**Acknowledgments:** The authors would like to thank the faculty members, researchers, and technical staff who contributed valuable insights during the preparation of this survey. Their feedback helped refine the structure, improve the clarity of the analysis, and strengthen the overall quality of the manuscript. The authors also acknowledge the support of their respective institutions for providing access to research facilities, scientific resources, and academic databases that enabled the completion of this work.

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

## Abbreviations

The following abbreviations are used in this manuscript:

|        |                                                  |
|--------|--------------------------------------------------|
| AI     | Artificial Intelligence                          |
| BSM    | Basic Safety Message                             |
| CAM    | Cooperative Awareness Message                    |
| CAN    | Controller Area Network                          |
| C-V2X  | Cellular Vehicle-to-Everything                   |
| CoAP   | Constrained Application Protocol                 |
| DDS    | Data Distribution Service                        |
| DENM   | Decentralized Environmental Notification Message |
| DoS    | Denial of Service                                |
| DT     | Digital Twin                                     |
| FL     | Federated Learning                               |
| GNSS   | Global Navigation Satellite System               |
| HD Map | High-Definition Map                              |
| IMU    | Inertial Measurement Unit                        |
| IoT    | Internet of Things                               |
| IoV    | Internet of Vehicles                             |
| ITS    | Intelligent Transportation System                |
| JCAS   | Joint Communication and Sensing                  |
| MEC    | Mobile Edge Computing                            |
| ML     | Machine Learning                                 |
| MQTT   | Message Queuing Telemetry Transport              |
| NR-V2X | New Radio Vehicle-to-Everything                  |
| OBU    | On-Board Unit                                    |
| PC5    | Direct Sidelink Interface                        |
| PKI    | Public Key Infrastructure                        |
| QoS    | Quality of Service                               |
| RIS    | Reconfigurable Intelligent Surface               |
| RSU    | Roadside Unit                                    |
| Uu     | Cellular Uplink/Downlink Interface               |
| URLLC  | Ultra-Reliable Low-Latency Communication         |
| V2I    | Vehicle-to-Infrastructure                        |
| V2N    | Vehicle-to-Network                               |
| V2P    | Vehicle-to-Pedestrian                            |
| V2V    | Vehicle-to-Vehicle                               |
| V2X    | Vehicle-to-Everything                            |
| VANET  | Vehicular Ad Hoc Network                         |
| XR     | Extended Reality                                 |

## References

- Vogt, J.; Schotten, H.D.; Wieker, H. Intelligent transportation system protocol interoperability evaluation. *IEEE Open J. Intell. Transp. Syst.* **2025**, *6*, 67–94.
- Ansari, K. Joint use of DSRC and C-V2X for V2X communications in the 5.9 GHz ITS band. *IET Intell. Transp. Syst.* **2021**, *15*, 213–224.
- Bazzi, A.; Berthet, A.O.; Campolo, C.; Masini, B.M.; Molinaro, A.; Zanella, A. On the design of sidelink for cellular V2X: A literature review and outlook for future. *IEEE Access* **2021**, *9*, 97953–97980.
- Lombardi, M.; Pascale, F.; Santaniello, D. Internet of Things: A general overview between architectures, protocols and applications. *Information* **2021**, *12*, 87.
- Wu, Y.; Zhang, K.; Zhang, Y. Digital twin networks: A survey. *IEEE Internet Things J.* **2021**, *8*, 13789–13804.
- Jooriah, M.; Datsenko, D.; Almeida, J.; Sousa, A.; Silva, J.; Ferreira, J. A co-simulation platform for V2X-based cooperative driving automation systems. In Proceedings of the 2024 IEEE Vehicular Networking Conference (VNC), Kobe, Japan, 29–31 May 2024; pp. 227–230.
- Cui, G.; Zhang, W.; Xiao, Y.; Yao, L.; Fang, Z. Cooperative perception technology of autonomous driving in the Internet of Vehicles environment: A review. *Sensors* **2022**, *22*, 5535.
- Sedar, R.; Lopez, O.; Heinrich, R.; García, M.; Kowalski, T.; Novak, P.; Schmidt, F.; Rossi, L.; Kumar, A.; Zhang, Y. Standards-compliant multi-protocol on-board unit for the evaluation of connected and automated mobility services in multi-vendor environments. *Sensors* **2021**, *21*, 2090.
- Arthurs, P.; Gillam, L.; Krause, P.; Wang, N.; Halder, K.; Mouzakitis, A. A taxonomy and survey of edge cloud computing for intelligent transportation systems and connected vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 6206–6221.
- Mostefaoui, A.; Merzoug, M.A.; Haroun, A.; Nassar, A.; Dessables, F. Big data architecture for connected vehicles: Feedback and application examples from an automotive group. *Future Gener. Comput. Syst.* **2022**, *134*, 374–387.
- Agbaje, P.; Anjum, A.; Mitra, A.; Al-Dulaimi, A.; Mohanty, A. Survey of interoperability challenges in the Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 22838–22861.
- Gao, J.; Zuo, F.; Yang, D.; Wang, Y.; Ozbay, K.; Seeley, M. Toward equitable progress: A review of equity assessment and perspectives in emerging technologies and mobility innovations in transportation. *J. Transp. Eng.* **2025**, *151*, 03124003.
- Clancy, J.; Mullins, D.; Deegan, B.; Horgan, J.; Ward, E.; Eising, C.; Denny, P.; Jones, E.; Glavin, M. Wireless access for V2X communications: Research, challenges and opportunities. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 2082–2119.
- Garcia, M.H.C.; Molina-Galan, A.; Boban, M.; Gozalvez, J.; Coll-Perales, B.; Şahin, T.; Kousaridas, A. A tutorial on 5G NR V2X communications. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1972–2026.
- Verma, A.; Saha, R.; Kumar, G.; Kim, T. The security perspectives of vehicular networks: A taxonomical analysis of attacks and solutions. *Appl. Sci.* **2021**, *11*, 4682.
- Amari, H.; El Houda, Z.A.; Khoukhi, L.; Belguith, L.H. Trust management in vehicular ad-hoc networks: Extensive survey. *IEEE Access* **2023**, *11*, 47659–47680.
- Guo, H.; Liu, J.; Ren, J.; Zhang, Y. Intelligent task offloading in vehicular edge computing networks. *IEEE Wirel. Commun.* **2020**, *27*, 126–132.
- Han, Y.; Zhang, H.; Li, H.; Jin, Y.; Lang, C.; Li, Y. Collaborative perception in autonomous driving: Methods, datasets, and challenges. *IEEE Intell. Transp. Syst. Mag.* **2023**, *15*, 131–151.
- Jebamikyous, H.; Kashef, R. Autonomous vehicles perception (AVP) using deep learning: Modeling, assessment, and challenges. *IEEE Access* **2022**, *10*, 10523–10535.
- Gebrezgihaer, Y.T.; Jeremiah, S.R.; Deng, X.; Park, J.H. Machine learning-based blockchain technology for secure V2X communication: Open challenges and solutions. *Sensors* **2025**, *25*, 4793.
- Wu, Q.; Xu, J.; Zeng, Y.; Ng, D.W.K.; Schober, R.; Swindlehurst, A.L. A comprehensive overview on 5G-and-beyond networks with UAVs: From communications to sensing and intelligence. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 2912–2945.
- Wahid, I.; Hussein, N.H.; Yaw, C.T.; Koh, S.P. Vehicular ad hoc networks routing strategies for intelligent transportation system. *Electronics* **2022**, *11*, 3215.
- Hussein, N.H.; Yaw, C.T.; Koh, S.P.; Tiong, S.K.; Chong, K.H. A comprehensive survey on vehicular networking: Communications, applications, challenges, and upcoming research directions. *IEEE Access* **2022**, *10*, 86127–86180.
- Sharma, S.; Kaul, A.; Ahmed, S.; Sharma, S. A detailed tutorial survey on VANETs: Emerging architectures, applications, security issues, and solutions. *Int. J. Commun. Syst.* **2021**, *34*, e4905.
- González, E.E.; Garcia-Roger, D.; Monserrat, J.F. LTE/NR V2X communication modes and future requirements of intelligent transportation systems based on MR-DC architectures. *Sustainability* **2022**, *14*, 3879.
- Jurczenia, K.; Rak, J. A survey of vehicular network systems for road traffic management. *IEEE Access* **2022**, *10*, 42365–42385.
- Raza, S.; Wang, S.; Ahmed, M.; Anwar, M.R. A survey on vehicular edge computing: Architecture, applications, technical issues, and future directions. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 3159762.

28. Gu, H.; Zhao, L.; Han, Z.; Zheng, G.; Song, S. AI-enhanced cloud-edge-terminal collaborative network: Survey, applications, and future directions. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 1322–1385.
29. Creß, C.; Bing, Z.; Knoll, A.C. Intelligent transportation systems using roadside infrastructure: A literature survey. *IEEE Trans. Intell. Transp. Syst.* **2023**, *25*, 6309–6327.
30. Naik, G.; Choudhury, B.; Park, J.-M. IEEE 802.11bd & 5G NR V2X: Evolution of radio access technologies for V2X communications. *IEEE Access* **2019**, *7*, 70169–70184.
31. Liu, X.; Li, Z.; Yang, P.; Dong, Y. Information-centric mobile ad hoc networks and content routing: A survey. *Ad Hoc Netw.* **2017**, *58*, 255–268.
32. Qiu, T.; Chen, N.; Li, K.; Qiao, D.; Fu, Z. Heterogeneous ad hoc networks: Architectures, advances and challenges. *Ad Hoc Netw.* **2017**, *55*, 143–152.
33. Rajkumar, Y.; Santhosh Kumar, S.V.N. A comprehensive survey on communication techniques for the realization of intelligent transportation systems in IoT-based smart cities. *Peer- Netw. Appl.* **2024**, *17*, 1263–1308.
34. Pandharipande, A.; Vlaminc, G.; Bogdanov, A.; Gonsalves, T.; Meijer, D.; van Liempd, B.; Seshadrinathan, K.; O'Connor, D.; O'Regan, J. Sensing and machine learning for automotive perception: A review. *IEEE Sens. J.* **2023**, *23*, 11097–11115.
35. Chib, P.S.; Singh, P. Recent advancements in end-to-end autonomous driving using deep learning: A survey. *IEEE Trans. Intell. Veh.* **2023**, *9*, 103–118.
36. Gao, X.; Zhang, X.; Lu, Y.; Huang, Y.; Yang, L.; Xiong, Y.; Liu, P. A survey of collaborative perception in intelligent vehicles at intersections. *IEEE Trans. Intell. Veh.* **2024**, *9*, 103–118.
37. Elghazaly, G.; Frank, R.; Harvey, S.; Safko, S. High-definition maps: Comprehensive survey, challenges, and future perspectives. *IEEE Open J. Intell. Transp. Syst.* **2023**, *4*, 527–550.
38. Roy, D.; Li, Y.; Jian, T.; Tian, P.; Chowdhury, K.; Ioannidis, S. Multi-modality sensing and data fusion for multi-vehicle detection. *IEEE Trans. Multimed.* **2022**, *25*, 2280–2295.
39. Rehman, A.; Saba, T.; Haseeb, K.; Jeon, G.; Alam, T. Modeling and optimizing IoT-driven autonomous vehicle transportation systems using intelligent multimedia sensors. *Multimed. Tools Appl.* **2023**, *83*, 1–15.
40. Zhang, C.; He, J.; Bai, C.; Yan, X.; Gong, J.; Zhang, H. How to use advanced fleet management system to promote energy saving in transportation: A survey of drivers' awareness of fuel-saving factors. *J. Adv. Transp.* **2021**, *2021*, 9987101.
41. Hamdi, A.M.A.; Hussain, F.K.; Hussain, O.K. Task offloading in vehicular fog computing: State-of-the-art and open issues. *Future Gener. Comput. Syst.* **2022**, *133*, 201–212.
42. Juet, Y.; Bekkouche, F.; Corre, Y.; Gorce, J.-M. Joint secure offloading and resource allocation for vehicular edge computing network: A multi-agent deep reinforcement learning approach. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 5555–5569.
43. Yuan, T.; de Araujo Neto, W.; Rothenberg, C.E.; Obraczka, K.; Barakat, C.; Turletti, T. Machine learning for next-generation intelligent transportation systems: A survey. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4427.
44. Jia, N.; Qu, Z.; Ye, B.; Wang, Y.; Hu, S.; Guo, S. A comprehensive survey on communication-efficient federated learning in mobile edge environments. *IEEE Commun. Surv. Tutor.* **2025**, *27*, 3710–3741.
45. Jha, A.V.; Appasani, B.; Khan, M.S.; Zeadally, S.; Katib, I. 6G for intelligent transportation systems: Standards, technologies, and challenges. *Telecommun. Syst.* **2024**, *86*, 241–268.
46. Moradi-Pari, E.; Nasri, R.; Andaroodi, M.; Ghasemi, A.; Shaghaghi, A.; Rastegar, M.; Habibi, D.; Moghaddam, M. DSRC versus LTE-V2X: Empirical performance analysis of direct vehicular communication technologies. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 4889–4903.
47. Clancy, J.; Mullins, D.; Deegan, B.; Horgan, J.; Ward, E.; Denny, P.; Glavin, M. Feasibility study of V2X communications in initial 5G NR deployments. *IEEE Access* **2023**, *11*, 75269–75284.
48. Chen, S.; Hu, J.; Shi, Y.; Zhao, L.; Li, W. A vision of C-V2X: Technologies, field testing, and challenges with Chinese development. *IEEE Internet Things J.* **2020**, *7*, 3872–3881.
49. Arbab-Zavar, B.; Palacios-García, E.J.; Vasquez, J.C.; Guerrero, J.M. Message queuing telemetry transport communication infrastructure for grid-connected AC microgrids management. *Energies* **2021**, *14*, 5610.
50. Hiremath, S.C.; Mallapur, J.D. QoS-based scheduling mechanism for electrical vehicles in cloud-assisted VANET using deep RNN. *Int. J. Syst. Assur. Eng. Manag.* **2024**, *15*, 2571–2587.
51. Nagy, A.M.; Simon, V. Survey on traffic prediction in smart cities. *Pervasive Mob. Comput.* **2018**, *50*, 148–163.
52. Redondo, J.; Yuan, Z.; Aslam, N. Performance analysis of high-definition map distribution in VANET. In Proceedings of the 2023 International Wireless Communications and Mobile Computing (IWCMC), Marrakesh, Morocco, 19–23 June 2023; pp. 55–60.
53. Zhang, J.; Guo, H.; Liu, J.; Zhang, Y. Task offloading in vehicular edge computing networks: A load-balancing solution. *IEEE Trans. Veh. Technol.* **2019**, *69*, 2092–2104.
54. Karimi, E.; Chen, Y.; Akbari, B. Task offloading in vehicular edge computing networks via deep reinforcement learning. *Comput. Commun.* **2022**, *189*, 193–204.

55. Chougule, S.B.; Chaudhari, B.S.; Ghorpade, S.N.; Zennaro, M. Exploring computing paradigms for electric vehicles: From cloud to edge intelligence, challenges and future directions. *World Electr. Veh. J.* **2024**, *15*, 39.
56. Kumar, K.S.; Radha, A.S.; Sundaresan, S.; Ananth Kumar, T. Modeling of VANET for future generation transportation system through edge/fog/cloud computing powered by 6G. In *Cloud and IoT-based Vehicular Ad Hoc Networks*; Wiley: Hoboken, NJ, USA, 2021; pp. 105–124.
57. Elleuch, I.; Makni, A.; Bouaziz, R. Cooperative intersection collision avoidance persistent system based on V2V communication and real-time databases. In Proceedings of the 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, Tunisia, 30 October – 3 November 2017; pp. 1082–1089.
58. Wu, Y.; Wu, J.; Chen, L.; Yan, J.; Han, Y. Load balance guaranteed vehicle-to-vehicle computation offloading for min-max fairness in VANETs. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 11994–12013.
59. Xue, Z.; Liu, Y.; Han, G.; Ayaz, F.; Sheng, Z.; Wang, Y. Two-layer distributed content caching for infotainment applications in VANETs. *IEEE Internet Things J.* **2021**, *9*, 1696–1711.
60. Habibi, P.; Farhoudi, M.; Kazemian, S.; Khorsandi, S.; Leon-Garcia, A. Fog computing: A comprehensive architectural survey. *IEEE Access* **2020**, *8*, 69105–69133.
61. Mahor, V.; Bijrothiya, S.; Mishra, R.; Rawat, R. A technique for monitoring cyber-attacks on self-driving automobiles-based VANET. In *Autonomous Vehicles Volume 2: Smart Vehicles*; Wiley: Hoboken, NJ, USA, 2022; pp. 317–333.
62. Alladi, T.; Gera, B.; Agrawal, A.; Chamola, V.; Yu, F.R. DeepADV: A deep neural network framework for anomaly detection in VANETs. *IEEE Trans. Veh. Technol.* **2021**, *70*, 12013–12023.
63. Setia, H.; Sharma, S.; Singh, P.; Gupta, N.; Dhiman, G.; Kumar, V.; Alshahrani, A.; Alzahrani, A. Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments. *Cybersecur. Appl.* **2024**, *2*, 100037.
64. Mo, Z.; Gao, Z.; Zhao, C.; Lin, Y. FedDQ: A communication-efficient federated learning approach for Internet of Vehicles. *J. Syst. Archit.* **2022**, *131*, 102690.
65. Alqubaysi, T.; Asmari, A.F.A.; Alanazi, F.; Almutairi, A.; Armghan, A. Federated learning-based predictive traffic management using a contained privacy-preserving scheme for autonomous vehicles. *Sensors* **2025**, *25*, 1116.
66. Kudva, S.; Badsha, S.; Sengupta, S.; Khalil, I.; Zomaya, A. Towards secure and practical consensus for blockchain based VANET. *Inf. Sci.* **2021**, *545*, 170–187.
67. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANET security challenges and solutions: A survey. *Veh. Commun.* **2017**, *7*, 7–20.
68. Fernandes, C.P.; Montez, C.; Adriano, D.D.; Boukerche, A.; Wangham, M.S. A blockchain-based reputation system for trusted VANET nodes. *Ad Hoc Netw.* **2023**, *140*, 103071.
69. Nath, H.J.; Choudhury, H. Privacy-preserving authentication protocols in VANET. *SN Comput. Sci.* **2023**, *4*, 589.
70. Mohammed, B.A.; Khan, M.A.; Aldosary, A.S.; Zolkipli, M.F.; Ullah, A.; Khan, I.; Abbas, S.; Saad, N.M.; Arif, S.; Hassan, R. Efficient blockchain-based pseudonym authentication scheme supporting revocation for 5G-assisted vehicular fog computing. *IEEE Access* **2024**, *12*, 33089–33099.
71. Choi, J.; Marojenic, V.; Dietrich, C.B.; Reed, J.H.; Ahn, S. Survey of spectrum regulation for intelligent transportation systems. *IEEE Access* **2020**, *8*, 140145–140160.
72. Boualouache, A.; Senouci, S.-M.; Moussaoui, S. A survey on pseudonym changing strategies for vehicular ad-hoc networks. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 770–790.
73. Yuan, H.; Li, G. A survey of traffic prediction: From spatio-temporal data to intelligent transportation. *Data Sci. Eng.* **2021**, *6*, 63–85.
74. Su, Z.; Liu, T.; Hao, X.; Hu, X. Spatial-temporal graph convolutional networks for traffic flow prediction considering multiple traffic parameters. *J. Supercomput.* **2023**, *79*, 18293–18312.
75. Garg, S.; Mehrotra, D.; Pandey, H.M.; Pandey, S. Accessible review of Internet of Vehicle models for intelligent transportation and research gaps for potential future directions. *Peer- Netw. Appl.* **2021**, *14*, 978–1005.
76. Mokhi, C.E.; Erguig, H.; Hmina, N.; Hachimi, H. Intelligent traffic management systems: A literature review on AI-based traffic light control. In *The Future of Urban Living: Smart Cities and Sustainable Infrastructure Technologies*, Springer: Kenitra, Morocco, 17–18 April 2025; pp. 154–171.
77. Rosayyan, P.; Paul, J.; Subramaniam, S.; Ganesan, S.I. An optimal control strategy for emergency vehicle priority system in smart cities using edge computing and IoT sensors. *Meas. Sensors* **2023**, *26*, 100697.
78. Zhang, L.; Zhou, Z.; Yi, B.; Wang, J.; Chen, C.M.; Shi, C. Edge-cloud framework for vehicle-road cooperative traffic signal control in augmented Internet of Things. *IEEE Internet Things J.* **2024**, *11*, 18234–18247.
79. Jia, W.; Ji, M. Multi-agent deep reinforcement learning for large-scale traffic signal control with spatio-temporal attention mechanism. *Appl. Sci.* **2025**, *15*, 8605.
80. Chu, T.; Wang, J.; Codecà, L.; Li, Z. Multi-agent deep reinforcement learning for large-scale traffic signal control. *IEEE Trans. Intell. Transp. Syst.* **2019**, *21*, 1086–1095.

81. Ricord, S.; Wang, Y. Investigation of equity biases in transportation data: A literature review synthesis. *J. Transp. Eng.* **2023**, *149*, 03123004.
82. Pipicelli, M.; Gimelli, A.; Sessa, B.; De Nola, F.; Toscano, G.; Di Blasio, G. Architecture and potential of connected and autonomous vehicles. *Vehicles* **2024**, *6*, 275–304.
83. Jia, Y.; Nie, Z.; Wang, W.; Lian, Y.; Guerrero, J.M.; Outbib, R. Eco-driving policy for connected and automated fuel cell hybrid vehicles platoon in dynamic traffic scenarios. *Int. J. Hydrog. Energy* **2023**, *48*, 18816–18834.
84. Jung, J.J.; Nguyen, L.V.; Park, L.; Nguyen, T.H. Cooperative negotiation-based traffic control for connected vehicles at signal-free intersections. In *International Symposium on Intelligent and Distributed Computing*; Springer International Publishing: Cham, Bremen, Germany, 14–16 September 2022; pp. 297–306.
85. Tulay, H.B.; Koksall, C.E. Sybil attack detection based on signal clustering in vehicular networks. *IEEE Trans. Mach. Learn. Commun. Netw.* **2024**, *2*, 753–765.
86. Liu, W.; Wang, Y.; Gao, H.; Wei, Y.; Hu, J.; Sun, Z.; Li, L. A systematic survey of control techniques and applications in connected and automated vehicles. *IEEE Internet Things J.* **2023**, *10*, 21892–21916.
87. Wang, Z.; Wei, H.; Wang, J.; Zeng, X.; Chang, Y. Security issues and solutions for connected and autonomous vehicles in a sustainable city: A survey. *Sustainability* **2022**, *14*, 12409.
88. Luo, F.; Jiang, Y.; Zhang, Z.; Ren, Y.; Hou, S. Threat analysis and risk assessment for connected vehicles: A survey. *Secur. Commun. Netw.* **2021**, *2021*, 1263820.
89. Gaouar, N.; Lehsaini, M. Toward vehicular cloud/fog communication: A survey on data dissemination in vehicular ad hoc networks using vehicular cloud/fog computing. *Int. J. Commun. Syst.* **2021**, *34*, e4906.
90. Khan, M.A.; Aslam, N.; Qasim, U.; Alshamrani, S.M.; Alghamdi, S.S.; Almogren, A.; Alayyas, O.M.; Khan, I.; Khan, Z.; Almuflihi, A. Robust, resilient, and reliable architecture for V2X communications. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4414–4430.
91. Ying, Z.; Wang, K.; Xiong, J.; Ma, M. A literature review on V2X communications security: Foundation, solutions, status, and future. *IET Commun.* **2024**, *18*, 1683–1715.
92. Hakeem, S.A.A.; El-Gawad, M.A.A.; Kim, H. Comparative experiments of V2X security protocol based on hash chain cryptography. *Sensors* **2020**, *20*, 5719.
93. Farsimadan, E.; Moradi, L.; Palmieri, F. A review on security challenges in V2X communications technology for VANETs. *IEEE Access* **2025**, *13*, 12345–12367.
94. Behura, A.; Kumar, A.; Jain, P.K. A comparative performance analysis of vehicular routing protocols in intelligent transportation systems. *Telecommun. Syst.* **2025**, *88*, 26–45.
95. Arroba, P.; Buyya, R.; Cárdenas, R.; Risco-Martín, J.L.; Moya, J.M. Sustainable edge computing: Challenges and future directions. *Softw. Pract. Exp.* **2024**, *54*, 2272–2296.
96. Chen, W.; Lin, X.; Lee, J.; Toskala, A.; Sun, S.; Chiasserini, C.F. 5G-Advanced toward 6G: Past, present, and future. *IEEE J. Sel. Areas Commun.* **2023**, *41*, 1592–1619.
97. Han, X.; Tian, D.; Zhou, J.; Duan, X.; Sheng, Z.; Leung, V.C.M. Privacy-preserving proxy re-encryption with decentralized trust management for MEC-empowered VANETs. *IEEE Trans. Intell. Veh.* **2023**, *8*, 4105–4119.
98. Diallo, E.; Dib, O.; Al Agha, K. A scalable blockchain-based scheme for traffic-related data sharing in VANETs. *Blockchain Res. Appl.* **2022**, *3*, 100087.
99. Chen, X.; Zhang, T.; Shen, S.; Zhu, T.; Xiong, P. An optimized differential privacy scheme with reinforcement learning in VANET. *Comput. Secur.* **2021**, *110*, 102446.
100. Twardokus, G.; Bindel, N.; Rahbari, H.; McCarthy, S. When cryptography needs a hand: Practical post-quantum authentication for V2V communications. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2024)*, San Diego, CA, USA, 26 February–1 March 2024.
101. Zhang, P.; Chen, N.; Shen, S.; Yu, S.; Wu, S.; Kumar, N. Future quantum communications and networking: A review and vision. *IEEE Wirel. Commun.* **2022**, *31*, 141–148.
102. Wu, D.; Zheng, A.; Yu, W.; Cao, H.; Ling, Q.; Liu, J.; Zhou, D. Digital twin technology in transportation infrastructure: A comprehensive survey of current applications, challenges, and future directions. *Appl. Sci.* **2025**, *15*, 1911.
103. Ali, S.; Abu-Samah, A.; Abdullah, N.F.; Mohd Kamal, N.L. Propagation modeling of unmanned aerial vehicle (UAV) 5G wireless networks in rural mountainous regions using ray tracing. *Drones* **2024**, *8*, 334.
104. Hasan, M.K.; Hossain, M.S.; Rahman, M.A.; Alhumam, A.; Muhammad, G.; Alamri, A.; Ghoneim, A.; Kaur, A. Federated learning for computational offloading and resource management of vehicular edge computing in 6G-V2X network. *IEEE Trans. Consum. Electron.* **2024**, *70*, 3827–3847.
105. Alhashimi, H.F.; Alzubaidi, L.; Al-Aswad, H.; Çabuk, U.; Lin, C.-Y.; Alghamdi, N.S.; Albahri, A.S.; Albahri, O.S. A survey on resource management for 6G heterogeneous networks: Current research, future trends, and challenges. *Electronics* **2023**, *12*, 647.
106. Higgins, M.; Jha, D.N.; Blundell, D.; Wallom, D. Security-by-design issues in autonomous vehicles. *IT Prof.* **2025**, *27*, 50–56.

107. Sharshembiev, K.; Yoo, S.M.; Elmahdi, E. Protocol misbehavior detection framework using machine learning classification in vehicular ad hoc networks. *Wirel. Netw.* **2021**, *27*, 2103–2118.
108. Alkaabi, S.R.; Gregory, M.A.; Li, S. Multi-access edge computing handover strategies, management, and challenges: A review. *IEEE Access* **2024**, *12*, 4660–4673.
109. Fan, W.; Su, Y.; Liu, J.; Li, S.; Huang, W.; Wu, F.; Liu, Y. Joint task offloading and resource allocation for vehicular edge computing based on V2I and V2V modes. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 4277–4292.
110. Alhameed, M.; Mahgoub, I.; Limouchi, E. Intelligent high-awareness and channel-efficient adaptive beaconing based on density and distribution for vehicular networks. *Electronics* **2024**, *13*, 891.
111. Chen, Z.; Huang, S.; Min, G.; Ning, Z.; Li, J.; Zhang, Y. Mobility-aware seamless service migration and resource allocation in multi-edge IoV systems. *IEEE Trans. Mob. Comput.* **2025**, *24*, 1556–1570.
112. Chen, Q.; Song, X.; Song, T.; Yang, Y. Vehicular edge computing networks optimization via DRL-based communication resource allocation and load balancing. *IEEE Trans. Mob. Comput.* **2025**, *24*, 1571–1585.
113. Liu, Z.; Deng, Y. Resource allocation strategy for vehicular communication networks based on multi-agent deep reinforcement learning. *Veh. Commun.* **2025**, *53*, 100895.
114. Ali, S.A.; Elsaid, S.A.; Ateya, A.A.; ElAffendi, M.; El-Latif, A.A.A. Enabling technologies for next-generation smart cities: A comprehensive review and research directions. *Future Internet* **2023**, *15*, 398.
115. Alraih, S.; Khan, M.A.; Alghamdi, S.; Khattak, H.A.; Alshamrani, S.M.; Almogren, A.; Tolba, A.; Baz, A.; Tariq, U.; Khan, I. Revolution or evolution? Technical requirements and considerations toward 6G mobile communications. *Sensors* **2022**, *22*, 762.
116. Gu, X.; Wu, Q.; Fan, P.; Fan, Q.; Cheng, N.; Chen, W.; Letaief, K.B. DRL-based resource allocation for motion blur resistant federated self-supervised learning in IoV. *IEEE Internet Things J.* **2024**, *12*, 7067–7085.

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