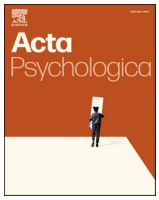
Acta Psychologica 255 (2025) 104892

Contents lists available at ScienceDirect

Acta Psychologica

journal homepage: www.elsevier.com/locate/actpsy



Toward a conceptual model to improve the user experience of a sustainable and secure intelligent transport system

Abdullah Alsaleh *

Department of Computer Engineering, College of Computer and Information Sciences, Majmaah University, Majmaah, Saudi Arabia
Department of Information Engineering, Florence University, Florence, Italy

ARTICLE INFO

Keywords:
Cloudlet
Cloud computing
Internet of things
Vehicular communication
Sustainable development goals

ABSTRACT

The rapid advancement of automotive technologies has spurred the development of innovative applications within intelligent transportation systems (ITS), aimed at enhancing safety, efficiency and sustainability. These applications, such as advanced driver assistance systems (ADAS), vehicle-to-everything (V2X) communication and autonomous driving, are transforming transportation by enabling adaptive cruise control, lane-keeping assistance, real-time traffic management and predictive maintenance. By leveraging cloud computing and vehicular networks, intelligent transportation solutions optimize traffic flow, improve emergency response systems, and forecast potential collisions, contributing to safer and more efficient roads. This study proposes a Vehicular Cloud-based Intelligent Transportation System (VCITS) model, integrating vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication through roadside units (RSUs) and cloudlets to provide real-time access to cloud resources. A novel search and management protocol, supported by a tailored algorithm, was developed to enhance resource allocation success rates for vehicles within a defined area of interest. The study also identifies critical security vulnerabilities in smart vehicle networks, emphasizing the need for robust solutions to protect data integrity and privacy. The simulation experiments evaluated the VCITS model under various traffic densities and resource request scenarios. Results demonstrated that the proposed model effectively maintained service availability rates exceeding 85 % even under high demand. Furthermore, the system exhibited scalability and stability, with minimal service loss and efficient handling of control messages. These findings highlight the potential of the VCITS model to advance smart traffic management while addressing computational efficiency and security challenges. Future research directions include integrating cybersecurity measures and leveraging emerging technologies like 5G and 6G to further enhance system performance and safety.

1. Introduction

Intelligent Transportation Systems (ITS) are at the forefront of transforming modern transportation by enabling efficient, safe and sustainable mobility. A critical aspect of ITS is computational efficiency, which ensures the timely and accurate processing of vast data streams essential for real-time decision-making and system operations. Key metrics of computational efficiency include processing speed, scalability and energy efficiency. Processing speed determines the system's ability to analyze and act on data rapidly, while scalability enables ITS to accommodate growing data volumes without performance degradation. Furthermore, energy efficiency is vital for reducing the power consumption of onboard devices and communication modules, making ITS more environmentally sustainable. Leveraging advanced optimization algorithms and integrating edge and cloud-based architectures further enhances the computational capabilities of ITS by reducing latency and optimizing resource allocation. These features collectively ensure that ITS can deliver reliable and responsive solutions, even in complex and dynamic environments. The advent of cloud computing has revolutionized ITS by providing scalable computational resources. Cloud platforms offered by providers such as Amazon Web Services and Google Cloud facilitate the sharing of vast computational power, enabling ITS to address challenges like traffic congestion and road safety. Modern vehicles, often referred to as “data centers on wheels,” generate and process significant amounts of data, creating opportunities to improve road safety, traffic flow and environmental sustainability (Schulz, 2011).

* Department of Computer Engineering, College of Computer and Information Sciences, Majmaah University, Majmaah, Saudi Arabia.
E-mail address: alsaleh@mu.edu.sa.

https://doi.org/10.1016/j.actpsy.2025.104892
Received 2 April 2024; Received in revised form 6 February 2025; Accepted 10 March 2025
Available online 12 March 2025

Vehicle ad hoc networks (VANETs) exemplify this innovation, acting as highly mobile, self-organizing networks that facilitate vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. These networks support critical ITS applications, such as collision avoidance, traffic management and intelligent routing, by leveraging technologies like the IEEE 802.11p standard for dedicated short-range communication (Boukerche, Oliveira, Nakamura, & Loureiro, 2008).

Despite these advances, ITS faces significant challenges, particularly in cybersecurity and privacy. Increasing connectivity between vehicles, infrastructure and external systems exposes ITS to cyber threats, including hacking, data breaches and malware attacks. Such vulnerabilities can compromise system integrity, user safety and public trust (Bharati, Podder, Mondal, & Robel, 2020; *Bleepingcomputer report*, 2018; Cai, Wang, Zhang, Gruffke, & Schweppe, 2019; Ivanov, Maple, Watson, & Lee, 2018; Li, Yu, Sun, & Chen, 2018; Muhammad & Safdar, 2018). Ensuring robust security measures, such as intrusion detection systems and advanced encryption protocols, is crucial to mitigating these risks. Additionally, the integration and interoperability of diverse ITS components are hindered by the lack of standardized communication protocols. Addressing these challenges is essential to achieving seamless interactions between various ITS technologies and realizing the vision of a fully connected and autonomous transportation ecosystem. Recent advancements have made notable strides in addressing ITS challenges. Technologies like vehicle-to-everything (V2X) communication and advanced driver assistance systems (ADAS) have significantly enhanced safety and efficiency by reducing human errors and traffic fatalities (Eiza & Ni, 2017; Klinedinst & King, 2016; Nie, Liu, & Du, 2017; *Threatpost report*, 2017; Vanhoef & Piessens, 2017; Yan, Xu, & Liu, 2016). Predictive maintenance systems, powered by IoT sensors and machine learning algorithms, now enable real-time vehicle diagnostics, minimizing breakdowns and optimizing operational costs. However, significant issues remain. Cybersecurity and privacy concerns are escalating as cyber threats become more sophisticated. Moreover, the scalability of ITS infrastructure and its ability to handle vast and growing data streams demand robust computational frameworks. Public acceptance of ITS technologies, especially autonomous vehicles, requires transparent communication about safety, reliability and ethical considerations (Bitam & Mellouk, 2011; Salahuddin, Al-Fuqaha, Guizani, & Cherkaoui, 2014; Zeadally, Hunt, Chen, Irwin, & Hassan, 2012). Smart vehicles, as integral components of ITS, represent both opportunities and challenges. These vehicles are increasingly equipped with sophisticated computing and communication capabilities, making them vulnerable to cyber-attacks if security measures are not adequately implemented. Vulnerabilities range from direct access points, such as diagnostic ports, to wireless access points, such as Bluetooth and Wi-Fi systems. These vulnerabilities are exploited by attackers to gain unauthorized access, manipulate onboard systems or breach sensitive data. Addressing these security issues requires a comprehensive approach that includes securing communication protocols, implementing intrusion detection systems and ensuring the privacy of sensitive user data. Regulatory frameworks and industry collaboration are also essential in standardizing security practices and addressing emerging threats.

In this paper, we propose a conceptual model aimed at improving the user experience of ITS while addressing key challenges such as security, privacy and computational efficiency. The structure of this paper is as follows: Section 2 reviews previous work on VANETs and ITS technologies. Section 3 presents the definition of the problem and the details of the proposed model. Section 4 outlines the simulation scenario and experimental setup. Section 5 provides an evaluation of the results, followed by a discussion in Section 6. Finally, Section 7 concludes the paper and outlines future research directions.

2. Related work

The development of VANETs has enabled significant advancements in ITS. VANETs consist of communication nodes, primarily vehicles, that exchange information dynamically. Fixed roadside units (RSUs) installed at critical locations, such as hazardous intersections and adverse weather-prone areas, facilitate V2I communication. This section reviews key contributions in vehicular cloud computing (VCC), the Internet of Vehicles (IoV), and connected and autonomous vehicles (CAV), highlighting their strengths, limitations and opportunities for further research.

2.1. Vehicular cloud computing (VCC)

Olariu et al. (Olariu, Hristov, & Yan, 2013) introduced the concept of the vehicular cloud, where vehicles' computing resources are utilized to form a dynamic mobile cloud. This approach leverages vehicles' data perception, processing and communication capabilities to create a network of coordinated nodes. Although the proposed system demonstrated the feasibility of resource sharing, it relied on conventional cloud models, limiting real-time data processing and resource utilization efficiency. To address challenges in VCC, Mershad and Artail (Mershad & Artail, 2013) developed the CROWN system, where RSUs acted as cloud interfaces and directories, enabling vehicles to access their recorded data. However, their study lacked integration of onboard computing capabilities, which are critical for decentralized and edge-based processing. Similarly, Baby et al. (Baby, Sabareesh, Saravanaguru, & Thangavelu, 2013) proposed using RSUs to extend traditional cloud services to vehicles, enabling access to both public and private vehicular services. This architecture, while innovative, still depended heavily on cloud gateways, reducing its efficiency in scenarios requiring ultra-low latency. Zingirian and Valenti (Zingirian & Valenti, 2012) proposed a "Sensor as a Service" model, where vehicles contributed their sensors for cloud-based services. Although this concept introduced new applications for sensor data, the lack of hybrid cloud utilization hindered its ability to meet the high processing demands of coordinated vehicular communication. Recent studies have proposed frameworks for resource optimization in VCC. For instance, a comprehensive review by (Lu, Niyato, & Wang, 2015) outlined hybrid VCC architectures aimed at improving resource management. Subsequent works, such as (Zhang, Xu, & Zhang, 2017; Zhao, Liu, & Shen, 2018), employed machine learning and stochastic optimization to enhance task offloading and resource allocation, addressing issues like latency and energy consumption. Despite these advancements, existing models often fail to fully account for the dynamic mobility of vehicles, highlighting the need for real-time adaptive mechanisms.

2.2. Internet of vehicles (IoV)

IoV extends VANETs by integrating vehicles with the broader Internet infrastructure, enabling advanced applications such as traffic prediction, real-time navigation and infotainment. A key focus of IoV research has been the integration of enabling technologies such as 5G and edge computing. Studies like (Goumidi, Aliouat, & Harous, 2019; He, Yan, & Xu, 2018) emphasize the potential of these technologies to enhance vehicular communications, offering improved latency, bandwidth utilization and reliability. A notable contribution to IoV is the development of blockchain-based security frameworks, as proposed by (Ning, Qin, & Zhang, 2017). These frameworks address data integrity, trust management and privacy issues in vehicular networks. However, challenges such as scalability and computational overhead persist. Additionally, IoV-based intelligent traffic management systems, like the one proposed in (Ali, Iqbal, & Iqbal, 2022), utilize AI and machine learning for traffic prediction and control. While effective in simulation environments, their real-world applicability remains limited due to infrastructure and scalability constraints. Research by (Shi, Cao, Zhang, Li, & Xu, 2016) investigated the role of edge computing in IoV, highlighting its potential to reduce latency and improve bandwidth utilization. Despite these benefits, practical implementations often face challenges in maintaining seamless connectivity in highly dynamic

vehicular environments. Addressing these issues requires robust hybrid architectures that combine edge, cloud and fog computing.

2.3. Connected and autonomous vehicles (CAV)

Connected and autonomous vehicles represent the next frontier in ITS, with research focusing on cooperative driving, perception, decision-making and control. Studies like (Litman, 2020; Zhou, Ai, & Jiang, 2020) highlight the importance of cooperative driving techniques, such as platooning and intersection management, in improving safety and efficiency. However, these approaches often rely on extensive communication infrastructure, which may not be universally available. Deep learning applications in CAVs, as reviewed in (Huang & Chen, 2020), have shown promise in enhancing perception and decision-making capabilities. However, their reliance on large-scale datasets and computationally intensive models presents challenges for real-time deployment. Furthermore, studies like (Huang, Fang, Qian, & Rose Qingyang, 2020) emphasize the importance of secure and private V2X communication to ensure reliable information exchange in CAV environments. Despite proposed solutions such as encryption and authentication protocols, the evolving nature of cyber threats necessitates ongoing research in this area.

2.4. Security and privacy in ITS

Security and privacy remain critical challenges in ITS, particularly in VCC, IoV and CAV contexts. Table 1 summarizes recent works addressing these issues, highlighting their strengths and limitations.

Despite the significant progress made in VCC, IoV and CAV research, several limitations must be addressed to fully realize their potential. Key areas for future exploration include:

1. Dynamic Resource Management: Advanced models leveraging AI and reinforcement learning to enhance resource allocation and quality of service (QoS).
2. Hybrid Architectures: Integration of edge, cloud and fog computing to address latency and bandwidth constraints while ensuring scalability.
3. Security and Privacy: Development of robust cryptographic protocols and privacy-preserving mechanisms to secure data exchange in highly dynamic environments.
4. Regulatory and Societal Factors: Establishing global standards and addressing societal concerns, such as ethical implications and public acceptance of autonomous systems.
5. Real-World Validation: Comprehensive testing of proposed frameworks and algorithms in diverse and real-world scenarios to ensure scalability and adaptability.

Addressing these challenges will require collaborative efforts from researchers, industry stakeholders and policymakers, alongside significant investment in infrastructure and technology development. The advancements in ITS will pave the way for more efficient, safe and intelligent transportation systems, shaping the future of mobility.

Table 1
Summary of Strengths and Limitations in Security and Privacy.

Item	Year	Strengths	Limitations
(Meneguette, De Grande, Ueyama, Rocha Filho, & Madeira, 2021)	2021	Demonstrated the benefits of vehicular edge computing in reducing latency and meeting service execution requirements.	Lacked detailed discussions on architectures, performance optimization and scalability.
(Masood, Lakew, & Cho, 2020)	2020	Highlighted autonomous sharing of heterogeneous resources among vehicles.	Limited focus on specific security and privacy threats.
(Limbasiya, Das, & Sahay, 2019)	2019	Addressed challenges in data collection and storage for connected vehicles.	Insufficient details on proposed data transmission protocols.
(Yang, Zhang, Zhao, Choo, & Zhang, 2022)	2022	Proposed a privacy-preserving aggregation authentication scheme for fog-cloud-based VANETs.	Lacked real-world validation and scalability considerations.
(Sheikh, Liang, & Wang, 2020)	2020	Reviewed architectures, trust models and applications in VANETs and VCC.	Did not provide technical details on cryptographic techniques.
(Limbasiya & Das, 2020)	2020	Identified key challenges in vehicular cloud storage and transmission.	Lacked comparative analysis and implementation details.
(Hataba, Sherif, Mahmoud, Abdallah, & Alasmary, 2022)	2022	Discussed the transformative impact of AI on vehicle autonomy.	Limited technical solutions and countermeasure examples.
(Nayak, Hota, Kumar, Turuk, & Chong, 2022)	2022	Highlighted VANET applications in ITS, such as safety and traffic management.	Offered limited solutions for overcoming identified challenges.

3. Preliminaries and problem definition

3.1. Overview

Fog computing has emerged as a crucial technology for supporting cloud-based applications by providing the required speed, scalability, latency, sensitivity, security and reliability. It extends cloud services closer to the data source by enabling computing at the edge of the network, rather than relying solely on centralized data centers. This decentralized approach helps address critical issues in vehicular networks, which are essential for the development of ITS (Chen et al., 2023; Kumar & Singh, 2021; Qu, Liu, Wang, & Ma, 2020; Rajyalakshmi & Lakshmanna, 2022; Rasheed, Hu, Hong, & Balasubramanian, 2021). In the context of ITS, achieving road safety and improving traffic efficiency in urban areas depends on reducing latency, ensuring robust security and enhancing system scalability (Bonomi, Milito, Zhu, & Addepalli, 2012; Chaib et al., 2020; Whaiduzzaman, Sookhak, Gani, & Buyya, 2014). This research introduces a novel communication model, the VANET-Cloud, designed to overcome these challenges by integrating traditional cloud architecture with vehicular networks. The VANET-Cloud builds on conventional cloud computing nodes and stationary computing infrastructure, extending them into the vehicular environment by incorporating mobile computing resources from the vehicles themselves. This model allows vehicles to contribute computing power and storage capacity, creating a more dynamic and adaptable infrastructure for managing transportation-related challenges. By leveraging the computational and storage capabilities of vehicles, VANET-Cloud can enable various services that enhance traffic management, accident handling and real-time road conditions monitoring. For example, it can help with traffic incident management, dynamic route optimization to reduce congestion and synchronization of traffic lights based on real-time traffic data. These services are facilitated through vehicular communication, which provides a robust foundation for managing complex road scenarios and improving overall traffic flow.

3.2. Proposed vehicular cloud-based model

The Vehicular Cloud-Based Intelligent Transport System (VCITS) is a comprehensive model designed to support vehicular communication services via VANET-Cloud. This model is particularly aimed at optimizing vehicle movement in critical road environments, such as

intersections, slick roads and construction zones. The VCITS is built on the principle of leveraging IoT sensor data to improve communication between vehicles, RSUs and other infrastructure elements. As connected vehicles approach RSUs, they share data, which is then processed and stored in the Vehicular-Cloud for real-time analysis and decision-making. This system provides a range of services, such as traffic management, road safety monitoring and accident notifications, all powered by the communication between vehicles and infrastructure. The VCITS operates through three main functions:

A. Resource Allocation and Sharing: Efficient management of the resources available within the vehicular network is key to maintaining seamless communication and ensuring the optimal distribution of computational and storage capacities.
B. Data Management and Storage: The massive amount of data generated by vehicles, including traffic conditions, road incidents and environmental factors, must be managed effectively to ensure quick retrieval and processing.
C. Interoperability Among Devices: The diverse range of devices, including vehicles, RSUs and mobile clouds, must be able to communicate seamlessly to enable the smooth functioning of the VCITS.

The VCITS model is designed to offer two main types of services:

A. Cooperation as a Service (CaaS): This service maximizes the efficiency of communication between vehicles and infrastructure. It supports a wide range of services, including traffic control, accident reporting, weather updates, parking availability and real-time traffic conditions. By using V2V and V2I communication, the model enables a hybrid communication system that can handle large volumes of data and reduce transmission congestion. A relay selection mechanism is employed to optimize data transmission and mitigate the impact of network congestion.
B. Data-Driven Services: The VANET-Cloud collects and processes data from vehicle sensors to deliver services that inform vehicles of potential incidents or changes in traffic conditions. The system uses advanced algorithms to analyze real-time traffic data and recommend optimal routes, helping drivers avoid congestion and potential accidents. This approach leverages mathematical methods to predict traffic conditions and suggest alternative routes to minimize delays and improve overall traffic efficiency.

The VCITS framework enhances V2V and V2I communication through three key domains: cloud services, communication, and consumers. The system architecture, as illustrated in Fig. 1, shows how these components interact to deliver real-time data and services to end-users (drivers and road authorities).

3.2.1. *Cloud services*

Cloud services within the VCITS model are responsible for managing and distributing data across the system. These services include centralized data centers such as Google, Microsoft or Amazon and distributed computing resources such as smartphones and in-vehicle systems, which are constantly connected to the cloud. The cloud services are divided into three sublayers:

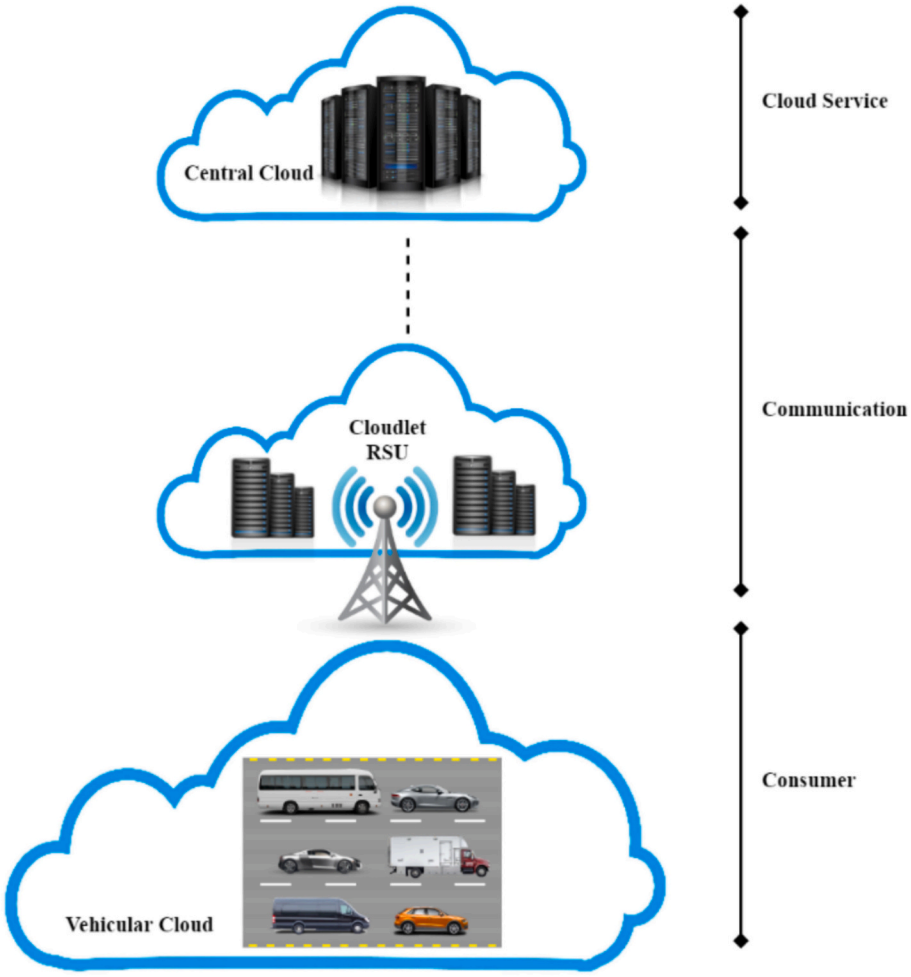


Fig. 1. VCITS abstraction.

- Central Cloud: Traditional cloud data centers equipped with advanced computational resources, providing the core infrastructure for data processing and management.
- Cloudlets: These are smaller, localized data processing units located at RSUs. Cloudlets assist in managing local resources and offloading tasks from the central cloud, ensuring faster response times and reduced network latency.
- Vehicular Mobile Cloud (VANET-Cloud): The VANET-Cloud is a dynamic layer of mobile cloud computing resources provided by moving vehicles. This cloud is highly flexible and can be used for both fixed and mobile applications. In fixed VANET-Cloud systems, vehicles in parking lots or idle state can rent their computational resources to others. In mobile systems, vehicles use V2V communication to share data and resources.

3.2.2. Communication

The communication layer is critical to maintaining the flow of information between mobile vehicles, RSUs and infrastructure. Several network types are involved, including Vehicle Networks, 4G/5G networks and wireless detection systems. Vehicles communicate through RSUs, Wi-Fi hotspots or cellular networks, and the system must support multiple network interfaces simultaneously to maintain seamless communication as vehicles move. To optimize communication and prevent network congestion, the proposed system employs the Proxy Mobile IPv6 (PMIPv6) protocol, which enables smooth handover between base stations as vehicles move through different network regions. Additionally, a new protocol is introduced to handle data distribution and network congestion, helping to maintain efficient communication even in highly congested areas. This protocol identifies an Area of Interest (AoI) based on the vehicle's location and selectively broadcasts messages to vehicles within the AoI, thus reducing network load and improving data delivery. The communication model also includes a propagation efficiency mechanism to determine when data should be transmitted. Vehicles periodically assess their message delivery efficiency, ensuring only relevant and timely messages are forwarded. The algorithm accounts for various factors, such as network congestion and vehicle mobility and optimizes message propagation accordingly. To formalize the proposed search and management protocol, we introduce the search and resource allocation model: Let represent the set of vehicles in the network, R the set of roadside units (RSUs), and C the set of cloudlets. The probability of successful resource allocation $P_{alloc}$is defined as shown in Eq. (1):

$$P_{alloc} = \frac{\sum_{i=1}^{N} S_i}{N} \tag{1}$$

where S is a binary success indicator (1 if the allocation is successful, 0 otherwise) and N is the total number of requests. The service availability rate of 85 % includes error margins calculated using standard deviationσ as shown in Eq. (2):

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N} (S_i - \mu)^2} \tag{2}$$

where μ is the mean availability rate. A confidence interval of 95 % is provided for statistical rigor.

3.2.3. Consumer

The consumer layer comprises the end-users, primarily the vehicles that rely on the VCITS for road optimization and safety. Vehicles utilize various sensors and computing devices, including GPS systems, onboard computers and proximity sensors, to interact with the network and request relevant services. The consumer layer is dynamic, with vehicles continually moving through different road segments and requiring real-time updates to optimize their routes and avoid hazards.

3.3. Performance analysis of the proposed VCITS model

To evaluate the performance of the VCITS model, a simulation experiment was conducted using the OMNeT++ event-based simulator. Urban mobility scenarios were created using the Simulation of Urban MObility (SUMO) tool and vehicle mobility was modeled using the Veins network model. These tools enabled the simulation of realistic traffic scenarios, including the impact of mobility on communication efficiency and the effectiveness of the VANET-Cloud in improving road safety and traffic flow. The performance analysis focused on evaluating key metrics such as message delivery success, network congestion and response time for critical events. The results demonstrated that the VCITS model significantly improved communication efficiency and reduced latency, even in highly dynamic and congested environments. The proposed VCITS model offers a promising solution to address the challenges faced by modern vehicular networks, providing a robust framework for intelligent transportation systems. By leveraging the capabilities of the VANET-Cloud, the model enhances communication, resource sharing and data management, leading to improved road safety, traffic efficiency and overall system performance.

4. Scenario construction

To simulate realistic traffic conditions, OpenStreetMap (OSM) was utilized to generate a detailed map for the simulation experiment. The simulation focused on a 4.5 km segment of the A11 highway, which is part of an 82 km stretch connecting Florence and Pisa in Italy. This section of road was chosen due to its varied terrain, including bends, steep gradients and intersections, which reflect real-world traffic dynamics and provide an ideal setting for examining the behavior of vehicles in a vehicular network environment. These road characteristics were crucial for the simulation's ability to replicate scenarios that involve overtaking and other driving behaviors relevant to an ITS. Three distinct traffic scenarios were modeled to replicate overtaking events within the vehicle cluster network. In the first scenario, vehicles were simulated traveling at a top speed of 120 km/h, with a distance of 3.5 m between them. This high-speed scenario reflects typical urban highway conditions where vehicles are traveling at maximum legal speeds with minimal space between them. The second scenario reduced the maximum speed of vehicles to 90 km/h, simulating more moderate traffic conditions. The third scenario involved heavy trucks, which were modeled to travel at 90 km/h with a larger distance of 18 m between them. This scenario represents truck convoys, which often travel at lower speeds and maintain greater distances, affecting traffic flow and vehicular communication. In addition to the individual vehicle types, a network composition was defined, consisting of 50 % cars, 30 % buses, and 20 % heavy trucks. This distribution is presented in Table 2 and was selected to reflect the typical vehicle mix found on the A11 highway, where cars dominate but buses and trucks also play significant roles in traffic dynamics.

Each vehicle in the simulation was assigned resources that could be shared with other vehicles. These resources, consisting of computational and storage capacities, were randomized for optimization purposes. Specifically, vehicles could either have 0 or 2 resources available for sharing with others, helping to ensure diversification and testing of the resource allocation system under different conditions. Once the simulation reached a stable state, a vehicle entered AoI and initiated the search process by sending query messages. These messages were

Table 2
Vehicle type.

Type of vehicles	Speed (km/h)	Size m	Network comprising %
Car	120	3.5	50
Buses	90	14	30
Heavy trucks	90	18	20

designed to search for three types of shared resources available in the mobile VANET-Cloud computing environment. Communication was established either through V2V communication or through V2I communication, depending on the proximity and availability of RSUs. The primary objective of the simulation was to assess several critical parameters of the vehicular network. These parameters included the time required for a vehicle to search for cloud resources, the delay time for resources to be made available to the requester and the overall network load created by the regulation and management of query messages. In particular, the simulation aimed to measure the efficiency of resource search, the impact of vehicle density and how delays in resource availability could affect the overall traffic flow and response times in emergency or high-traffic scenarios. Additionally, the simulation tracked the generation and flow of regulation messages within the network, which is essential for maintaining the stability of the communication system and ensuring the timely delivery of information. This scenario construction process is crucial for evaluating the performance of the proposed vehicular cloud-based model. By simulating diverse traffic conditions and various vehicle types, the experiment sought to identify potential bottlenecks and inefficiencies in the system, as well as to evaluate how well the VANET-Cloud could manage resource allocation and vehicle communication in real-world-like conditions. The insights gained from this simulation would inform the development of more robust and responsive ITS solutions, ultimately contributing to safer and more efficient road use.

5. Evaluation and results

To assess the effectiveness of the proposed VCITS, a comprehensive simulation was conducted to evaluate various parameters under different traffic conditions. The evaluation focused on measuring service availability, service absence and the number of control messages generated, with specific emphasis on beaconing and resource allocation efficiency. The simulation varied the traffic density by adjusting the number of vehicles on the highway, starting from 500 vehicles per hour and increasing in increments of 100 vehicles, up to 1000 vehicles per hour. In addition, the time required to access the services was varied, ranging from 20 to 60 s. This allowed for the assessment of the system's performance under both low and high-density traffic conditions. Several parameters were used to define the simulation environment, including the bit rate, transmission power and propagation model. The medium access control (MAC) layer was configured with a bit rate of 18 Mbit/s, and a power transfer power of 2.21 mW was used to calculate the data transfer range, which was found to be approximately 300 m using the two-ray ground propagation model (Sommer, Joerer, & Dressler, 2012). The simulation was conducted with a 95 % confidence interval and included 60 runs for statistical robustness. The key parameters used in the simulation are summarized in Table 3.

5.1. Service availability

Fig. 2 presents the results regarding the availability of services to requesters under varying traffic densities. The proposed protocol was able to allocate 100 % of the requested resources in scenarios where vehicles simultaneously queried all three available resources. This high service allocation rate demonstrates the robustness of the proposed system in handling multiple resource requests from vehicles. However, as the time required to make services available increased (e.g., 40 s and 60 s), a slight difference in service allocation performance was observed, particularly during periods when new allocations needed to be made. These delays were primarily due to the time spent on reassigning resources to meet the new demand, which is an inherent characteristic of systems involving dynamic resource sharing. Interestingly, the availability of services improved significantly as the highway density increased. This finding suggests that higher vehicle density leads to more frequent opportunities for resources to be shared and allocated, thereby enhancing the overall service availability in the system. The ability to efficiently allocate resources in high-density environments is crucial for the performance of vehicular networks, especially when traffic conditions are more congested.

Table 3
Simulation parameters.

Parameters	Value
Confidence interval	95 %
Number of runs	60
Ping time	5 s
Beacons time	0.5 s
Highway length	4.5 km
Bit rate	18 Mbit/s
Transmission range	300 m
Transmission power	2.2 mW

5.2. Service absence

In contrast to the service availability results, Fig. 3 shows the percentage of service absence, which is inversely related to the availability of services. As expected, a greater number of control messages and longer service allocation times contributed to a higher rate of service loss. The results indicated a service loss of approximately 15 %, which occurred mainly due to delays in the resource allocation process. This service absence can be attributed to the increased time spent managing control messages, particularly when there was a large volume of vehicles on the road. In scenarios where the vehicles were requesting services that required more time to allocate (40 and 60 s), the system experienced more control message overhead, which led to a greater loss of services. These findings emphasize the need for efficient management of control messages to reduce service delays and ensure that resources are allocated promptly, particularly during high traffic volumes.

5.3. Control messages and network overhead

Fig. 4 illustrates the overhead in terms of the number of control messages generated as a function of traffic density. As the number of vehicles on the road increased, so did the number of ping messages and control signals generated. This observation suggests that the greater the number of vehicles, the more frequent the need for vehicles to communicate and exchange information about available resources. The results also indicate that there was an increase in control messages when the system had to create new allocations in response to changing traffic conditions. Specifically, in scenarios where the time to allocate resources was set to 40 and 60 s, the system needed to instantiate new allocations for vehicles that had passed through certain monitored sections of the road. This process contributed to the observed rise in control messages. Interestingly, the results showed that even with the increase in network congestion and the need for new allocations, the proposed protocol maintained efficient management of resources. This suggests that the system is well-designed to handle large amounts of traffic and dynamically allocate resources based on the demand, without overwhelming the network with excessive control messages. In particular, the system was able to minimize delays and maintain a relatively low level of overhead, even as the traffic density increased.

5.4. Sensitivity and comparative analysis

The evaluation of system performance under varying conditions is crucial to understanding the robustness and adaptability of the proposed VCITS. One of the key factors affecting system efficiency is traffic density. As vehicle density increases, the availability of resources and services initially improves due to a higher number of participating nodes, which enhances V2V and V2I communication opportunities. However, beyond a certain threshold, congestion effects begin to degrade system

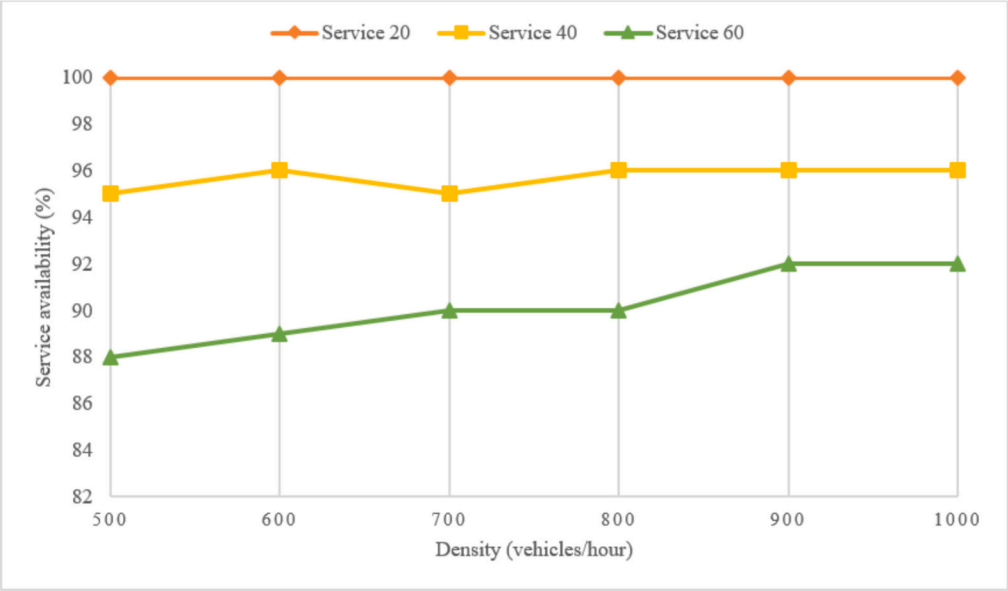


Fig. 2. Availability of service.

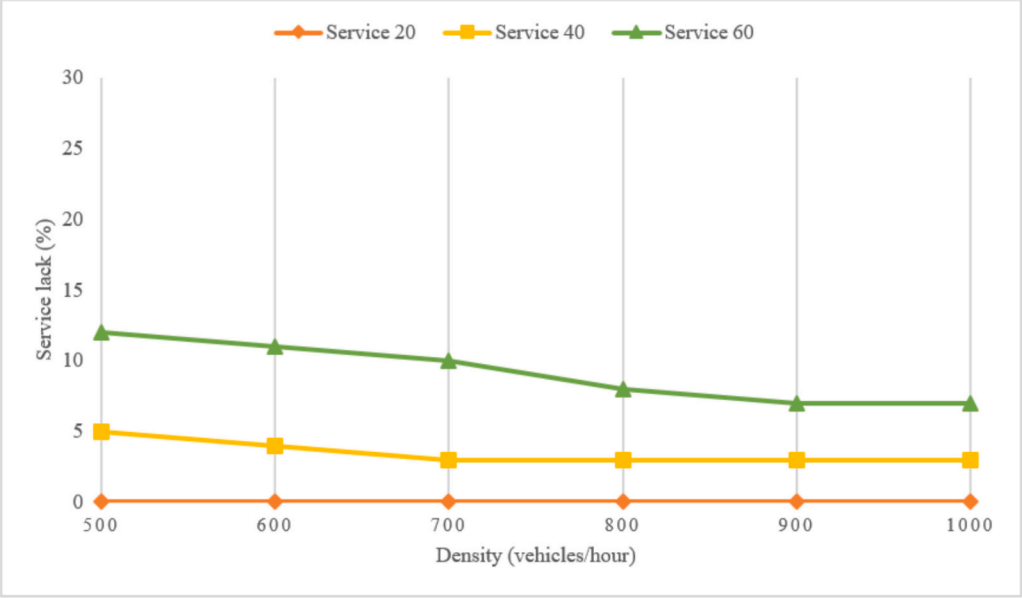


Fig. 3. Lack of service.

performance, leading to increased message collisions, network latency and service delays. This saturation point marks a critical limit where resource allocation mechanisms need to be optimized to maintain efficiency.

Another significant factor influencing system performance is resource allocation delay. Longer allocation times can reduce service continuity, as vehicles in need of computational resources or data services may experience disruptions. However, this issue can be mitigated through predictive load balancing, where anticipated resource demands are managed in advance using historical traffic patterns and real-time analytics. By implementing adaptive resource scheduling techniques, VCITS can ensure that resource distribution remains efficient, even under fluctuating network conditions. The analysis highlights that while the system performs optimally under normal traffic loads, further optimization strategies, such as dynamic task offloading and real-time congestion-aware computing, can enhance its resilience in high-density scenarios.

A comparison between VCITS and recent models highlights its advantages in terms of scalability, adaptability and resource management. The two benchmark models selected for comparison are (Mershad & Artail, 2013), which utilizes RSUs for cloud access but lacks decentralized computing efficiency and (Meneguette et al., 2021), which employs edge nodes for processing but does not fully leverage cloud-based resources for scalability. Table 4 below presents a structured comparison of these models:

From this comparison, it is evident that VCITS offers superior scalability and adaptability, as it efficiently integrates vehicular cloud, edge computing and predictive resource allocation techniques. Unlike (Mershad & Artail, 2013), which depends on RSU availability for cloud access, VCITS leverages distributed computing resources from vehicles, RSUs and cloudlets to ensure dynamic and scalable service provisioning. Additionally, while (Meneguette et al., 2021) provides efficient low-

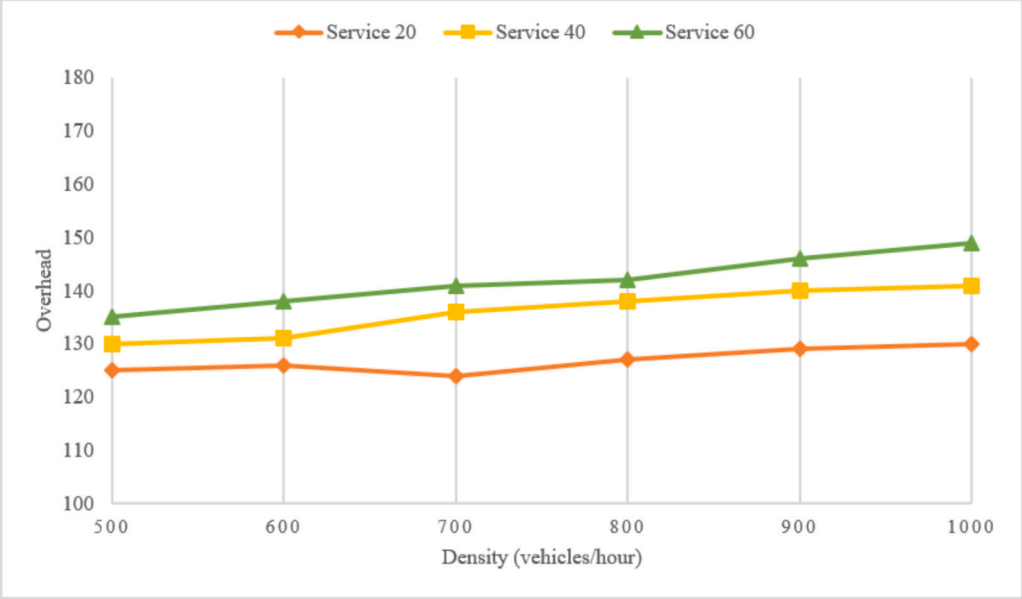


Fig. 4. Overhead versus traffic density.

Table 4
A comparison of models

Feature	VCITS	Mershad and Artail (2013)	Meneguette et al. (2021)
Scalability	High (utilizes cloud and edge resources dynamically)	Moderate (limited by RSU availability)	High (uses edge computing, but cloud integration is minimal)
Adaptability	High (supports real-time dynamic resource allocation)	Low (relies on predefined cloud access through RSUs)	Moderate (edge nodes provide adaptability but have processing limits)
Traffic Density Handling	Efficient under normal conditions, optimized for high-density scenarios	Struggles with high-density environments due to RSU limitations	Performs well but can face bandwidth limitations in edge-heavy scenarios
Resource Allocation Mechanism	Predictive load balancing and congestion-aware scheduling	Centralized allocation with RSU dependency	Edge-based distribution but lacks predictive modeling
Latency Reduction	Low latency due to hybrid edge-cloud architecture	Moderate latency due to RSU reliance	Low latency, but edge nodes can be overwhelmed under high demand

latency computation through edge nodes, it does not fully optimize resource distribution through predictive balancing, which is a key advantage of VCITS.

5.5. Overall performance

The simulation results demonstrated that the proposed vehicular cloud-based model consistently performed well across all scenarios, showing minimal variation in key performance metrics even under increasing vehicle densities. The availability of resources remained above 85 % even in the worst-case scenarios, which is a promising result for the real-world application of the VCITS model. This stability is particularly important for ensuring that the system can provide reliable communication and resource allocation, even in environments with fluctuating traffic conditions. The evaluation results validate the effectiveness of the proposed model in maintaining high service availability, minimizing service absence and efficiently managing network overhead. The model proved to be highly adaptable to varying traffic conditions, ensuring that vehicular communication and resource allocation can be performed optimally, even in dense traffic environments. These results are a significant step toward the development of a robust, scalable and efficient intelligent transport system based on cloud and vehicular networks.

5.6. Assumptions and limitations

The framework assumes reliable V2V and V2I communication without major disruptions. However, real-world environments may introduce packet loss and latency issues. In addition, cloudlets are assumed to have sufficient processing power and bandwidth. Their actual performance may vary based on hardware and network congestion. Furthermore, The study assumes general cyber threats but does not model adversarial attack scenarios explicitly.

6. Discussion

Recent technological advancements are transforming the landscape of smart vehicle systems, bringing significant benefits in the realms of safety, efficiency, connectivity and sustainability. This study introduces an innovative solution by integrating VANETs with cloud computing, aimed at optimizing traffic safety and management. The proposed framework, called VCITS, leverages the synergy between VANETs and cloud computing to improve vehicular communication, resource management and traffic flow. Specifically, a new search and management protocol for VANET-Cloud systems is introduced to reduce network congestion and optimize resource allocation, crucial for ensuring efficient communication among vehicles and infrastructure. The key performance indicator of this study was the protocol's ability to facilitate efficient resource search and establish connections between vehicles and cloud resources. The proposed system demonstrated minimal performance variation, regardless of traffic conditions, emphasizing its robustness and adaptability. The results indicate that the proposed method achieves reliable communication between vehicles, even under varying traffic densities, while optimizing resource utilization across the network. The protocol's performance is closely aligned with previous work in the field, including optimization techniques proposed by (Lim, Jeong, Park, & Lee, 2016), which combines scheduling and traffic

routing with resource allocation to enhance data transmission speeds and reduce congestion. Similarly, Min et al. (Min, Jeong, & Kang, 2018) presented a joint scheduling and resource allocation strategy (JRS-M and JRS-S algorithms) to maximize wireless network capacity, a concept mirrored in this study's design. The integration of scheduling and resource allocation in the context of VANET-Cloud systems enhances both data throughput and network stability, a crucial feature for real-time applications in vehicular environments.

A standout feature of the proposed model is the efficient transfer of computing resources from the VANET-Cloud infrastructure. As vehicles become increasingly equipped with advanced communication, storage and computational capabilities, the concept of VANET-Cloud, also known as a vehicular computing cloud, has emerged as a game-changer for road traffic management and safety. By leveraging the untapped resources available in vehicles, such as their onboard computing power, storage capacity and Internet connectivity, the VANET-Cloud model provides a scalable and dynamic solution for managing real-time traffic data, facilitating smoother traffic flows and improving overall road safety. This innovation significantly enhances the existing infrastructure, as it allows vehicles to offload computational tasks and access cloud-based resources without the limitations of traditional on-board systems.

In the context of this study, the proposed hybrid VANET-Cloud system highlights the potential for an advanced, collaborative infrastructure that supports computational, storage and communication functions across a vast network of vehicles and RSUs. This infrastructure serves as the backbone for ITS and provides the means for real-time decision-making, traffic monitoring and emergency response. The collaborative nature of the system allows for the dynamic allocation of resources based on traffic conditions and vehicle demands, leading to improved traffic management, reduced congestion and enhanced safety. A significant implication of the findings is that VANET-Cloud integration could be a key driver in the development of smart traffic control and safety systems in the future. As the transportation ecosystem continues to evolve, the role of cloud computing in supporting vehicular networks will become increasingly critical. By utilizing cloud resources, vehicles can tap into a vast pool of computational power and data storage, enabling a more seamless, efficient and responsive transportation environment. Furthermore, the proposed system aligns with current trends in intelligent vehicle technologies, including ADAS, connected vehicle networks and autonomous driving systems, which all rely on real-time data exchange and processing. The integration of cloud computing into these systems enhances their capabilities, allowing for better prediction, route planning and decision-making, all of which contribute to the safety and efficiency of road transport.

The implementation of the proposed VANET-Cloud system offers several advantages for both individual vehicles and the overall transportation network. First, it empowers vehicles with enhanced safety features by enabling communication between vehicles and between vehicles and infrastructure. This communication facilitates collision avoidance, emergency alerts, and optimal routing, which collectively contribute to reduced accidents and improved traffic flow. Second, the system enhances efficiency by enabling vehicles to make real-time adjustments based on available resources and traffic conditions. Third, the connectivity provided by the system allows for continuous updates and information sharing, ensuring that drivers and passengers are always informed of the most up-to-date road conditions. Lastly, the sustainability of the system is enhanced by reducing congestion, which leads to less fuel consumption and lower emissions, contributing to environmental goals. The proposed VCITS model represents a significant step forward in the development of smart transportation systems. By integrating VANETs with cloud computing, the model enables more efficient and reliable resource allocation, communication and traffic management. The system's adaptability to various traffic conditions and its ability to utilize available vehicle resources make it a promising solution for future transportation networks.

To enhance the security of data transmitted between vehicles, RSUs and cloud infrastructure, AES-256 encryption offers a great solution to support the model. AES-256 is a widely recognized symmetric encryption standard known for its high level of security due to its 256-bit key length, making it computationally infeasible to decrypt without the correct key. This encryption method is used to maintain the confidentiality of vehicular data, including location information and traffic conditions, against potential unauthorized access or passive eavesdropping.

In addition to encryption, the elliptic curve digital signature algorithm (ECDSA) plays an important role in authentication. ECDSA is a public key cryptographic technique designed to verify the legitimacy of communicating entities efficiently. Given the dynamic nature of vehicular networks, where vehicles frequently enter and exit the system, authentication plays a crucial role in ensuring that only legitimate vehicles participate in data exchanges. ECDSA helps maintain the integrity of the communication process without imposing excessive computational overhead, making it a suitable choice for resource-constrained vehicular environments. The use of digital signatures enhances trust in transmitted messages, reducing the likelihood of unauthorized data manipulation or impersonation.

To further enhance security monitoring, integrating machine learning-based intrusion detection for real-time anomaly recognition offers better enhancements. Traditional rule-based security mechanisms often struggle to identify novel or evolving cyber risks. By analyzing historical network traffic data, machine learning models can detect patterns that indicate unusual network activity, such as deviations from normal communication behavior. This approach enables the system to recognize potential anomalies, including irregular data transmissions or unauthorized access attempts, which could indicate security concerns.

While the proposed model demonstrates strong potential for improving vehicular cloud-based intelligent transportation systems, several real-world implementation challenges must be addressed to ensure its feasibility and effectiveness. One of the primary challenges is hardware constraints, particularly the computational limitations of in-vehicle processors and cloudlets. While modern vehicles are increasingly equipped with advanced computing capabilities, resource availability can vary significantly depending on the vehicle's make, model and onboard processing units. Many vehicles still rely on embedded processors with limited computational power, which may not be sufficient to handle the intensive data processing and real-time decision-making required for an efficient vehicular cloud system. Similarly, cloudlets deployed in roadside infrastructure must be optimized to balance processing loads efficiently. Another critical factor influencing real-world implementation is network congestion and bandwidth management. As vehicular networks grow, an increasing number of vehicles will generate and transmit data simultaneously, potentially leading to network overload and degraded communication performance. Congestion can impact V2V and V2I interactions, resulting in higher latency, packet loss and reduced service reliability. Additionally, the deployment costs associated with implementing large-scale vehicular cloud-based systems pose a significant challenge. Establishing the necessary infrastructure, including cloudlets, roadside units and high-speed wireless networks, requires substantial financial investment. The integration of security mechanisms, continuous software updates and regulatory compliance further contribute to long-term operational costs.

Future research should focus on refining the system's adaptability to real-world constraints, including hardware limitations, network congestion and deployment costs, to enhance the practical applicability of the model and ensure its successful large-scale deployment. Investigating strategies for dynamically distributing computational tasks across vehicular networks will be essential to ensuring that high-priority operations are handled by more capable nodes while maintaining energy efficiency. Additionally, advancements in edge computing and AI-driven resource allocation should be explored to minimize the computational burden on individual vehicles and enhance system scalability. Adaptive

bandwidth allocation strategies must also be developed to optimize data transmission based on real-time traffic density and network conditions. Integrating machine learning-based traffic prediction models could help preemptively allocate bandwidth resources, ensuring smooth data flow without overwhelming network infrastructure. Moreover, techniques such as data compression, multi-path communication and priority-based message scheduling should be explored to mitigate congestion and maintain efficient vehicular communication. In parallel, future studies should evaluate the economic feasibility of deploying such systems through cost-benefit analyses, exploration of funding models and assessment of government and private sector involvement. Leveraging existing smart city infrastructure by repurposing telecommunications networks and urban IoT platforms could help reduce implementation costs, while collaborative frameworks involving cloud service providers, automotive manufacturers and urban planners may offer a sustainable approach to infrastructure development. By refining computational resource management, optimizing bandwidth allocation and developing cost-effective deployment strategies, future research can ensure the practical viability and scalability of vehicular cloud-based intelligent transportation systems.

7. Summary and future directions

The integration and deployment of smart vehicle models, while offering substantial benefits, present significant challenges that must be addressed to ensure their successful adoption and widespread acceptance. These challenges encompass technological, regulatory and societal issues that require the concerted efforts of industry stakeholders, policymakers and regulatory bodies. By effectively addressing these barriers, we can unlock the full potential of smart vehicles and pave the way for a transformative shift in the future of transportation. This study introduced the vehicular cloud-based intelligent transportation system model, which is designed to optimize smart traffic management and urban safety. The model leverages cloud-based vehicular communication, known as VANET-Cloud, to facilitate the sharing of resources such as communication, processing power and storage. A key feature of the model is its search and management control protocol, which uses a specialized algorithm to transmit messages to vehicles within an area of interest. The simulation results demonstrated that the VCITS model can provide seamless communication and data exchange among vehicles and RSUs, even under heavy traffic conditions. With at least 85 % of service allocations being successful in the worst-case scenarios, the model showcased stable performance and resource allocation, even as the number of vehicles increased within the area of interest.

Looking ahead, several critical areas of research and development warrant attention to maximize the potential of VCITS and similar smart vehicle systems. One important consideration is the scalability of VANET-Cloud systems in real-world applications. While the proposed model demonstrated robustness in the simulation environment, further studies are needed to evaluate its performance in more dynamic, large-scale traffic networks. To ensure their reliability and adaptability, the real-world deployment of such systems will require extensive testing under various traffic conditions, particularly in urban areas with high vehicle density. Additionally, while the model addressed resource allocation effectively, further research should investigate the computational complexity of routing algorithms, especially under high-priority and emergency communication scenarios. Optimizing these algorithms will be crucial for enhancing traffic flow, particularly at critical points such as intersections, roundabouts and traffic signals.

A significant area of future exploration is the integration of advanced communication technologies such as 5G and 6G into the VANET-Cloud ecosystem. The adoption of these next-generation technologies will play a pivotal role in improving the performance and efficiency of vehicular networks. The high data transfer speeds and ultra-low latency offered by 5G and 6G will enable more effective coordination of vehicular nodes, allowing for real-time communication and improved traffic management. As these technologies evolve, it will be essential to explore how they can be seamlessly integrated into existing infrastructures to enhance the capabilities of smart transportation systems. Cybersecurity is another critical area that requires attention in future studies. As vehicles become more connected and reliant on cloud-based systems, ensuring the security of data and communications within VANETs will be paramount. Future research should focus on developing robust cybersecurity protocols to safeguard against potential threats, such as data breaches, cyberattacks and unauthorized access to vehicular networks. The IoV will be particularly susceptible to these vulnerabilities, and addressing these risks will be crucial for maintaining public trust and ensuring the safety of both passengers and the broader transportation ecosystem.

Moreover, future studies should expand the focus to include driver health and safety monitoring as part of the smart vehicle ecosystem. By incorporating sensors and monitoring systems, vehicles could detect signs of heart attacks, hypoglycemia, drug intoxication or drowsiness in drivers, thus preventing accidents caused by impaired driving. This would contribute significantly to the safety goals of intelligent transportation systems, as it allows vehicles to take proactive measures to prevent accidents before they occur. Additionally, the incorporation of predictive analytics could enable vehicles to assess road conditions, forecast weather and predict potential accidents, further improving road safety. Finally, the development of intelligent transportation systems should include a consideration of their societal and environmental impacts. Policymakers and social stakeholders must prioritize creating cities that are more affordable, safer and sustainable for all residents. By promoting collaboration between government, industry, academia and civil society, we can ensure the successful integration of smart vehicle technologies into urban infrastructure, improving the quality of life for all citizens. As these systems evolve, it will be essential to establish clear regulations and promote public acceptance to ensure the widespread adoption of smart vehicles. The successful deployment of smart vehicle technologies requires a coordinated effort across multiple sectors. The VCITS model proposed in this study offers a promising foundation for enhancing traffic management and urban safety through the integration of VANET and cloud computing. However, significant challenges remain, particularly about scalability, cybersecurity and the integration of emerging technologies. By addressing these challenges through continued collaboration and innovation, we can unlock the full potential of smart vehicles and transform the future of transportation.

CRediT authorship contribution statement

Abdullah Alsaleh: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Resources, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization.

Funding

The author extends the appreciation to the Deanship of Postgraduate Studies and Scientific Research at Majmaah University for funding this research work through the project number (R-2025-1652).

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Abdullah Alsaleh reports financial support was provided by Majmaah University. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The author is very thankful to all associated personnel in any capacity that contributed to the purpose of this research.

Data availability

Data will be made available on request.

References

Ali, S., Iqbal, M. A., & Iqbal, M. S. (2022). IoV-based traffic management in smart cities. *Journal of Advanced Transportation, 2022*, 1–15. https://doi.org/10.1155/2022/2314576

Baby, D., Sabareesh, R. D., Saravanaguru, R. A. K., & Thangavelu, A. (2013). VCR: Vehicular cloud for road side scenarios. *Advances in Computing and Information Technology*, 541–552. https://doi.org/10.1007/978-3-642-31600-5_53

Bharati, S., Podder, P., Mondal, M., & Robel, M. (2020). Threats and countermeasures of cyber security in direct and remote vehicle communication systems. In *arXiv: 2006.08723*. https://doi.org/10.48550/arXiv.2006.08723

Bitam, S., & Mellouk, A. (2011). QoS swarm bee routing protocol for vehicular ad hoc networks. In *2011 IEEE international conference on communications (ICC), Kyoto* (pp. 1–5). https://doi.org/10.1109/icc.2011.5963424

Bleepingcomputer report [online] https://www.bleepingcomputer.com/news/security/volkswagen-and-audi-cars-vulnerable-to-remote-hacking, (2018).

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on mobile cloud computing, ACM* (pp. 13–16). https://doi.org/10.1145/2342509.2342513.

Boukerche, A., Oliveira, H., Nakamura, E., & Loureiro, A. (2008). Vehicular ad hoc networks: A new challenge for localization-based systems. *Computer Communications, 31*(12), 2838–2849. https://doi.org/10.1016/j.comcom.2007.12.004

Cai, Z., Wang, A., Zhang, W., Gruffke, M., & Schweppe, H. (Aug. 2019). 0-days & mitigations: Roadways to exploit and secure connected BMW cars. In *, vol. 2019. Black Hat USA 2019* (p. 39) [online] https://i.blackhat.com/USA-19/Thursday/us-19-Cai-0-Days-And-Mitigations-Roadways-To-Exploit-And-Secure-Connected-BMW-Cars-wp.pdf.

Chaib, N., Oubbati, O. S., Bensaad, M. L., Lakas, A., Lorenz, P., et al. (Nov. 2020). BRT: Bus-based routing technique in urban vehicular networks. *IEEE Transactions on Intelligent Transportation Systems, 21*(11), 4550–4562. https://doi.org/10.1109/TITS.2019.2938871

Chen, C. M., Li, Z., Kumari, S., Srivastava, G., Lakshmanna, K., et al. (2023). A provably secure key transfer protocol for the fog-enabled social internet of vehicles based on a confidential computing environment. *Vehicular Communications, 39*, Article 100567. https://doi.org/10.1016/j.vehcom.2022.100567

Eiza, M. H., & Ni, Q. (Jun. 2017). Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. *IEEE Vehicular Technology Magazine, 12*(2), 45–51. https://doi.org/10.1109/MVT.2017.2669348 [online].

Goumidi, H., Aliouat, Z., & Harous, S. (2019). Vehicular cloud computing security: A survey. *Arabian Journal for Science and Engineering, 45*. https://doi.org/10.1007/s13369-019-04094-0

Hataba, M., Sherif, A., Mahmoud, M., Abdallah, M., & Alasmary, W. (2022). Security and privacy issues in autonomous vehicles: A layer-based survey. *IEEE Open Journal of the Communications Society, 3*, 811–829. https://doi.org/10.1109/OJCOMS.2022.3169500

He, J., Yan, Z., & Xu, Y. (2018). A survey on internet of vehicles: Applications, technologies, and challenges. *IEEE Communications Surveys & Tutorials, 20*(1), 426–445. https://doi.org/10.1109/COMST.2017.2765283

Huang, J., Fang, D., Qian, Y., & Rose Qingyang, H. (2020). Recent advances and challenges in security and privacy for V2X communications. *IEEE Open Journal of Vehicular Technology, 1*, 244–266.

Huang, Y., & Chen, Y. (2020). Autonomous driving with deep learning: A survey of state-of-art technologies. In *arXiv preprint arXiv:2006.06091*.

Ivanov, I., Maple, C., Watson, T., & Lee, S. (2018). Cyber security standards and issues in V2X communications for internet of vehicles. In *Proc. living internet things cybersecurity. (IoT)* (pp. 1–6). https://doi.org/10.1049/cp.2018.0046

Klinedinst, D., & King, C. (2016). *On board diagnostics: Risks and vulnerabilities of the connected vehicle. 10* [online] https://resources.sei.cmu.edu/asset_files/whitepaper/2016_019_001_453877.pdf.

Kumar, S., & Singh, V. (2021). A review of digital signature and hash function based approach for secure routing in VANET. In *Proc. int. conf. artif. intell. smart syst. (ICAIS)* (pp. 1301–1305). https://doi.org/10.1109/ICAIS50930.2021.9395882

Li, X., Yu, Y., Sun, G., & Chen, K. (May 2018). Connected vehicles' security from the perspective of the in-vehicle network. *IEEE Network, 32*(3), 58–63. https://doi.org/10.1109/MNET.2018.1700319

Lim, J. B., Jeong, Y. S., Park, D. S., & Lee, H. M. (2016). An efficient distributed mutual exclusion algorithm for intersection traffic control. *The Journal of Supercomputing, 74*(3), 1090–1107. https://doi.org/10.1007/s11227-016-1799-3

Limbasiya, T., & Das, D. (2020). SearchCom: Vehicular cloud-based secure and energy-efficient communication and searching system for smart transportation. In *Proceedings of the 21st international conference on distributed computing and networking (ICDCN '20). Association for Computing Machinery, New York, NY, USA, article 9* (pp. 1–10). https://doi.org/10.1145/3369740.3369772

Limbasiya, T., Das, D., & Sahay, S. K. (2019). Secure communication protocol for smart transportation based on vehicular cloud. In *Adjunct proceedings of the 2019 ACM international joint conference on pervasive and ubiquitous computing and proceedings of the 2019 ACM international symposium on wearable computers (UbiComp/ISWC '19 adjunct)* (pp. 372–376). New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3341162.3349305.

Litman, T. (2020). *Connected and autonomous vehicles: Research challenges and opportunities*. Victoria Transport Policy Institute.

Lu, Z., Niyato, D., & Wang, P. (Jan. 2015). Vehicular cloud computing: Architectures, applications, and challenges. *IEEE Network, 29*(1), 38–43.

Masood, A., Lakew, D. S., & Cho, S. (2020). Security and privacy challenges in connected vehicular cloud computing. *IEEE Communications Surveys & Tutorials, 22*(4), 2725–2764. Fourthquarter https://doi.org/10.1109/COMST.2020.3012961.

Meneguette, R., De Grande, R., Ueyama, J., Rocha Filho, G. P., & Madeira, E. (2021). Vehicular edge computing: Architecture, resource management, security, and challenges. *ACM Computing Surveys, 55*(1). https://doi.org/10.1145/3485129. Article 4 (January 2023), 46 pages.

Mershad, K., & Artail, H. (2013). Finding a STAR in a vehicular cloud. *IEEE Intelligent Transportation Systems Magazine, 5*(2), 55–68. Summer https://doi.org/10.1109/MITS.2013.2240041.

Min, S., Jeong, Y., & Kang, J. (2018). Cross-layer design and performance analysis for maximizing the network utilization of wireless mesh networks in cloud computing. *The Journal of Supercomputing, 74*(3), 1227–1254. https://doi.org/10.1007/s11227-017-2146-z

Muhammad, M., & Safdar, G. (Apr. 2018). Survey on existing authentication issues for cellular-assisted V2X communication. *Vehicular Communications, 12*, 50–65. https://doi.org/10.1016/j.vehcom.2018.01.008

Nayak, B. P., Hota, L., Kumar, A., Turuk, A. K., & Chong, P. H. J. (March 2022). Autonomous vehicles: Resource allocation, security, and data privacy. *IEEE Transactions on Green Communications and Networking, 6*(1), 117–131. https://doi.org/10.1109/TGCN.2021.3110822

Nie, S., Liu, L., & Du, Y. (Jul. 2017). Free-fall: Hacking Tesla from wireless to CAN bus. In *, 25. Briefing black hat USA* (pp. 1–16) [online] https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf.

Ning, H., Qin, Z., & Zhang, Y. (2017). Blockchain for internet of vehicles: A decentralized network security framework. In *IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)* (pp. 643–648). https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.104

Olariu, S., Hristov, T., & Yan, G. (2013). The next paradigm shift: From vehicular networks to vehicular clouds. In *Mobile ad hoc networking: Cutting edge directions*. Wiley. https://doi.org/10.1002/9781118511305.ch19.

Qu, X., Liu, E., Wang, R., & Ma, H. (Apr. 2020). Complex network analysis of VANET topology with realistic vehicular traces. *IEEE Transactions on Vehicular Technology, 69*(4), 4426–4438. https://doi.org/10.1109/TVT.2020.2976937

Rajyalakshmi, V., & Lakshmanna, K. (2022). A review on smart city - IoT and deep learning algorithms, challenges. *International Journal of Engineering Systems Modelling and Simulation, 13*(1), 3–26. https://doi.org/10.1504/IJESMS.2022.122733

Rasheed, I., Hu, F., Hong, Y.-K., & Balasubramanian, B. (May 2021). Intelligent vehicle network routing with adaptive 3D beam alignment for mmWave 5G-based V2X communications. *IEEE Transactions on Intelligent Transportation Systems, 22*(5), 2706–2718. https://doi.org/10.1109/TITS.2020.2973859

Salahuddin, M., Al-Fuqaha, A., Guizani, M., & Cherkaoui, S. (2014). RSU cloud and its resource management in support of enhanced vehicular applications. In *Globecom workshops (GC Wkshps)* (pp. 127–132). IEEE. https://doi.org/10.1109/GLOCOMW.2014.7063418.

Schulz, G. (2011). *Cloud and virtual data storage networking*. CRC Press [online] Available: https://www.taylorfrancis.com/books/9781439851746.

Sheikh, M. S., Liang, J., & Wang, W. (2020). Security and privacy in vehicular ad hoc network and vehicle cloud computing: A survey. *Wireless Communications and Mobile Computing, 2020*, Article 5129620, 25 pages https://doi.org/10.1155/2020/5129620.

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal, 3*(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198

Sommer, C., Joerer, S., & Dressler, F. (2012). On the applicability of Two-Ray path loss models for vehicular network simulation. In *2012 IEEE vehicular networking conference (VNC), Seoul* (pp. 64–69). https://doi.org/10.1109/VNC.2012.6407446

Threatpost report [online] https://threatpost.com/hyundai-patches-leaky-blue-link-mobile-app/125182/, (2017).

Vanhoef, M., & Piessens, F. (2017). Denial-of-service attacks against the 4-way Wi-Fi handshake. In *Proc. 9th int. conf. netw. commun. secur* (pp. 1–10) [online] https://papers.mathyvanhoef.com/ncs2017.pdf.

Whaiduzzaman, M., Sookhak, M., Gani, A., & Buyya, R. (2014). A survey on vehicular cloud computing. *Journal of Network and Computer Applications, 40*, 325–344. https://doi.org/10.1016/j.jnca.2013.08.004

Yan, C., Xu, W., & Liu, J. (2016). Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *Defcon, 24*(8), 109 [online] https://cyansec.com/files/articles/16DEFCON-Sensor.pdf.

Yang, Y., Zhang, L., Zhao, Y., Choo, K.-K. R., & Zhang, Y. (2022). Privacy-preserving aggregation-authentication scheme for safety warning system in fog-cloud based VANET. *IEEE Transactions on Information Forensics and Security, 17*, 317–331. https://doi.org/10.1109/TIFS.2022.3140657

Zeadally, S., Hunt, R., Chen, Y. S., Irwin, A., & Hassan, A. (2012). Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommunication Systems, 50* (4), 217–241. https://doi.org/10.1007/s11235-010-9400-5

Zhang, X., Xu, H., & Zhang, J. (2017). Task offloading in vehicular cloud computing: A stochastic optimization approach. *IEEE Transactions on Industrial Informatics, 14*(10), 4652–4661. https://doi.org/10.1109/TII.2017.2786319

Zhao, Y., Liu, L., & Shen, X. (2018). Dynamic resource allocation in vehicular cloud computing. *IEEE Transactions on Intelligent Transportation Systems, 19*(8), 2398–2407. https://doi.org/10.1109/TITS.2017.2787580

Zhou, H., Ai, B., & Jiang, D. (2020). Cooperative driving in connected and autonomous vehicles: A survey. *IEEE Communications Surveys & Tutorials, 22*(4), 2046–2075. https://doi.org/10.1109/COMST.2020.3004143

Zingirian, N., & Valenti, C. (2012). Sensor clouds for intelligent truck monitoring. In *2012 IEEE intelligent vehicles symposium, Alcala de Henares* (pp. 999–1004). https://doi.org/10.1109/IVS.2012.6232192