International Journal of Mathematics and Computer Research

ISSN: 2320-7167

Volume 14 Special Issue 03 March 2026, Page no. – 23-27

Impact Factor: 8.751

DOI: 10.47191/ijmcr/v14iSPC3.05

A Comprehensive Review on VANET-Cloud Architecture for Intelligent Transportation Systems

Satish kumar Mulgi, Prajakta Phakatkar, Yogesh Ingale

Department of Computer Science, Dr. D. Y. Patil, Arts, Commerce & Science College, Pimpri, Pune, Maharashtra, India

ARTICLE INFO

Published Online:
14 March 2026

Corresponding Author:
Satish kumar Mulgi

ABSTRACT

The rapid and unprecedented growth of urban populations has led to increased traffic congestion and road accidents, necessitating the development of Intelligent Transportation Systems (ITS) to improve road safety, traffic management, and driving efficiency. Among emerging technologies, Vehicular Ad Hoc Networks (VANETs) integrated with cloud computing have gained significant attention for enabling seamless vehicle-to-vehicle (V2V) and vehicle-to-cloud (V2C) communication. In such systems, vehicles are equipped with advanced sensors that collect real-time data about the environment, roadway, and surrounding vehicles. This data is processed, stored, and shared through cloud infrastructure to support a range of applications, including real-time traffic updates, collision avoidance alerts, navigation assistance, infotainment("information" and "entertainment."), and emergency response. The VAN-Cloud architecture offers a scalable and efficient framework for managing vehicular data and cloud resources, ensuring secure communication, low latency, and reliable data exchange. Furthermore, modern vehicles are increasingly equipped with intelligent onboard units that enhance these capabilities, contributing to the development of safer, smarter, and more efficient transportation systems.

KEYWORDS: Vehicular Cloud Computing, Vehicle Using Cloud, Vehicular Ad-Hoc Networks, Architecture, Security, Challenges.

1. INTRODUCTION

The variations of vehicular networking have changes drastically with the advancements of technologies. Vehicles are now equipped with high-tech sensors, computing devices and battery backup that enable these vehicles to become "smart vehicles." These smart vehicles become powerful nodes in vehicular networks. Vehicles communicate with each other, and vehicles with infrastructure using wireless technologies like dedicated short range communication (DSRC) [1], ZIGBEE [2], LTE/4G [[3][4]] etc. The vehicular ad-hoc networking (VANET) is the upper class of the mobile ad-hoc networking (MANET). The differences when comparing the MANET network to vehicular networking is that vehicles have enough storage, computing, and battery usage to maintain and use those resources. Taking into consideration the overhead of cloud computing, this gives each vehicle the ability to use these attributes of other vehicles. Therefore, utilizing these resources that are under used creates a new way of how vehicles can interact and prevent wasteful use of vehicular resources. To be more pragmatic, it is impractical for every vehicle in the vehicular network to maintain all information on every vehicle in that network. Every vehicle would not possess all information and there would be tremendous overhead costs. In lieu of this, there would be significant benefits in aspects like cloud computing services, computing service capability, and other potential internet services. Therefore, VANET could use cloud concepts in two different ways. First VCC (Vehicular Cloud Computing) [5] enables specific vehicles that are interested in renting out their resources to create their own vehicular cloud (VCC) and share resources with each other. The second model, VuC (Vehicles using Cloud) or VtC.

2. WHY VANET-CLOUD?

Vehicular ad-hoc networks are necessary to implement this intelligent transport system (ITS) infrastructure design. In the recent years vehicles are embedded now-a-days with onboard computing devices, sensor technologies, and immense storage capacity along with battery life. But vehicles are not using all these resources all the time. When a vehicle is parked at a cinema, hospital, work etc., all of the vehicle's resources are unused. We could be using these unused

resources to make services available to other vehicles that require them. Conversely vehicles can use the services of a conventional cloud. Conventional cloud provides several services to other vehicles including network as a service (NaaS), infrastructure as a service (IaaS), software as a service (SaaS), storage as a service (STaaS) etc. Services can be made available via a pay-as-you-go method. Vehicles can report weather, road conditions; traffic jams etc to cloud and make accurate real-time information available.

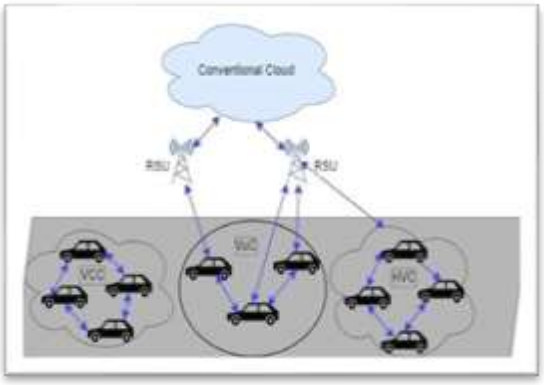

Figure 1: Three VANET Cloud Architecture

3. VANET- CLOUD ARCHITECTURE

Researcher have proposed the three VAN-Cloud architecture as shown in fig 1: VCC (Vehicular Cloud Computing), VuC (Vehicles using Cloud) and HVC (Hybrid Vehicular Cloud). On the basis of these studies following architecture, layers, services and communication types have been identified.

3.1 Vehicles to Cloud structure (VtC)

In the Vehicles-to-Cloud (VtC) architecture, vehicles communicate with the cloud through Road Side Units (RSUs) that act as gateways, since vehicles cannot store information about all others; cloud computing enables smart transport services, and to address service and security limitations, the VCC Service-Oriented Security Framework (VCC-SSF) was proposed, consisting of three layers—Core (communication), Security (authentication, encryption, and privacy), and Application Service (user services via V2X communication).

Various Vehicles-to-Cloud (VtC) and Vehicular Cloud Computing (VCC) architectures have been proposed to improve intelligent transportation systems (ITS). The Vehicular Cyber-Physical System and Mobile Cloud Computing Integration Architecture (VCMIA) enables seamless traffic management, real-time information sharing, and dynamic vehicle routing using GIS and cloud support. A three-layer VtC model includes the application, support, and network/perception layers to provide real-time ITS services. Another three-tier vehicular cloud model consists of the cloud infrastructure, intelligence, and system interface layers, designed for emergency response and data integration. The VANET–Cloud architecture features client, communication, and cloud layers, further enhanced by distinguishing between permanent and temporary clouds—the permanent cloud uses conventional cloud services (IaaS, PaaS, NaaS), while the temporary cloud is dynamically formed by vehicles sharing underutilized resources such as storage, computation, and network services.

3.2 Vehicular Cloud Computing (VCC)

In vehicular cloud computing architecture, users within vehicles access cloud resources through their own vehicle systems. The concept is based on utilizing the underused resources of vehicles, where some users act as **providers**, renting out their unused computing or storage capacity, while others act as **consumers**, accessing these resources on a pay-as-you-go basis. An **incentive-based secure architecture** encourages users to contribute their idle resources to the cloud in exchange for **tokens**, which can later be used to access cloud services. The cloud functions as a **trusted authority**, managing registration, authentication, and verification of vehicles through the **Service Provider Manager (SPM)** and the **Registration and Revocation Authorities (RA/TA)**.

Additionally, **zone-based systems** divide the network into multiple zones, each managed by a **Zone Authority (ZA)** responsible for validating data flow, managing requests, and maintaining privacy. **Cancellation schemes** are used to blacklist malicious or abandoned vehicles. **Transportation Management Systems (TMS)** built on vehicular cloud computing collect, analyze, and distribute traffic data through both local and internet-based processing, connecting vehicle clouds with conventional clouds for efficient data handling.

In **RSU-aided cluster-based vehicular clouds**, service-providing vehicles (SVs) and consumer vehicles (CVs) register through nearby **Roadside Units (RSUs)**, which form clusters of similar vehicles. The **cluster head** is selected based on **Euclidean distance**, ensuring efficient resource sharing and communication among vehicles in the network.

Table 1: The Summary of Related Literature of VAN-Cloud Architecture

Architecture	Layers	Application	Implementation
VuC	Core Technology Layer, Security, and Application Services Layer	Payment Service and Accident Management	No
VuC	Application layer Support layer Network layer Perception layer	Services to capture and sharereal-time accident/traffic footages.	Yes

VuC	Three tiers architecture: Device Level Communication Level Services level	Real time services	No
VuC	Three layer architecture: Cloud infrastructure layer, Intelligence Layer and System Interface layer.	Intelligent Disaster Management	Yes
VuC VCC	Client layer, communication layer and cloud layer	IaaS, StaaS	No
VuC VCC HVC	Car level layer Inter car level Cloud level	Traffic Information Dissemination	Yes, using VuC Architecture
VCC	Incentive based secure Architecture consist of VANET and Cloud layer	General services of Vehicles formed cloud: STaas, NaaS, SaaS	No, Only theoretical process of Public and Private key Athentication and generate token.
VCC	Zone Controller, VANET	use of underutilization of resources of vehicles	No
VCC	Vehicle Infrastructure Abstraction Layer Vehicle cloud layer Internet Cloud	Smart traffic management	No
VCC	RSU -aided Cluster-based Vehicular Clouds	use of underutilization of resources of vehicles	Yes

3.3 Hybrid Vehicular Cloud (HVC)

Mongrel pall computing is a mixed armature, which combines features of both the VUC and VCC infrastructures. VCC can act as both a consumer and supplier of pall-grounded services. On- road vehicles can give a wide variety of services as they can rent out their coffers on a pay per use base, plus request some services and calculating coffers from traditional shadows at the same time. VANET Cloud is a cold-blooded pall composed of both fixed static shadows and dynamic shadows. The stationary pall is made of fixed waiters in datacenters, and the dynamic pall consists of mobile vehicle bumps that give computing coffers. VANET Cloud retrieves data from a wide variety of media detectors and provides them to traditional shadows and end druggies. The vehicles can also communicate with a near VANET's Cloud to pierce different Internet- grounded operations and services. The mongrel vehicular pall can give services similar as smart business operation and entertainment.

4. VANET CLOUD APPLICATIONS

4.1 Infrastructure as services

Vehicles are equipped with many sensors, 5G internet connectivity and many times, have terabytes of storage space that allows them to communicate with other vehicles and infrastructure. Vehicles should not be assumed to utilize these resources all the time, VCC is a way to have vehicles lease out their resources to another vehicle in the network that needs it. Depending on the VuC design, the vehicles do not have much room for storing other vehicle information from networked vehicles. The traditional cloud is viewed as a data center which is there to store large amounts of data; it gives the driver the impression that the OBU (On Board Unit) and indeed, storage capacity is sufficient.

4.2 Software and Vanet applications as services

VANET-Cloud would have components (Vehicles, Conventional Cloud) and offer end users of different vehicular software/applications looking for information in terms of discovering geographic locations or real time information about vehicles parked and availability, gas stations, guest houses, resorts and other. Cloud computing in general enables a company's web server to have internet-based services. VANET Cloud has the large processing capacity to support web services and is faster and has more economical pricing than conventional web service providers using the vehicles onboard computers.

4.3 Gateway as a Service (GaaS)

Vehicular networks often face challenges in maintaining continuous Internet connectivity due to frequent topology changes and mobility. To address this, a **cloud-based Gateway as a Service (GaaS)** model is introduced to provide seamless Internet access for vehicles in a **VANET-Cloud environment**.

The GaaS model consists of four main components: the **gateway**, **client vehicle**, **relay vehicle**, and **cloud server**.

- The **gateway** is responsible for connecting vehicles to the Internet and can be either **stationary** (e.g., a Roadside Unit) or **mobile** (another vehicle).
- The **client vehicle** is the one requesting Internet connectivity through GaaS.
- The **relay vehicle** assists the client vehicle in establishing a connection when it is outside the gateway's coverage area.
- The **cloud server** manages service requests, resource allocation, and authentication, ensuring a seamless and efficient connection experience.

This architecture enhances the Internet accessibility and

overall network performance of vehicular networks, enabling continuous communication between vehicles and cloud services.

4.4 Smart Traffic Light System

Traffic efficiency applications in vehicular networks aim to enhance transportation system performance by sharing **real-time traffic information** among vehicles and roadside infrastructure. In a **VANET-Cloud-based Smart Traffic Light System**, information is exchanged between vehicles and RSUs to improve traffic flow, route guidance, and energy efficiency. Such systems integrate **car-to-car (C2C)** and **car-to-infrastructure (C2I)** communications to support use cases like **route guidance**, **navigation**, and **Green Light Optimal Speed Advisory (GLOSA)**.

- **Route guidance and navigation** enable infrastructure operators to collect and analyze large-scale traffic data, predict congestion, and provide vehicles with optimal route recommendations.
- **GLOSA** informs approaching vehicles about signalized intersections and the timing of upcoming green lights. This allows vehicles to adjust their speeds to minimize unnecessary stops and fuel consumption.

By leveraging VANET and cloud communication, smart traffic light systems help create a more efficient, predictive, and eco-friendly transportation environment.

4.5 Computing as a Service (CaaS)

In vehicular networks, vehicles often have limited computational capabilities to process complex tasks. The **standard cloud** can supplement this limitation by offering **Computing as a Service (CaaS)** to perform operations that vehicles cannot handle locally. Within the **Vehicles using Cloud (VuC)** architecture, vehicles can request on-demand computational resources from the cloud for data processing, route optimization, or multimedia applications. Conversely, in the **Vehicular Cloud Computing (VCC)** model, idle vehicles—such as those parked for long durations—can contribute their underutilized computing and storage resources to other vehicles for a fee. This distributed model increases overall productivity and resource utilization within the vehicular ecosystem.

4.6 Disaster Management

During natural disasters such as cyclones, hurricanes, or earthquakes, **VANET-Cloud systems** play a crucial role in **real-time information sharing, route optimization, and emergency response coordination**. By integrating cloud computing and vehicular networks, vehicles can access and disseminate critical data about **evacuation routes, fuel stations, medical facilities, and shelter locations**. RSUs and mobile nodes act as relays to transmit this information across affected areas, even when traditional communication networks are disrupted. The **VANET-Cloud infrastructure** ensures continuous data flow, allowing authorities to efficiently manage evacuation strategies and minimize loss of life.

4.7 Healthcare Services

Vehicular Cloud Computing (VCC) also supports **mobile healthcare services**, enabling **real-time medical assistance** for patients while in transit. A **RFID-based authentication mechanism** can identify and authenticate patients, medical staff, and vehicles to ensure secure data transmission and service delivery.

This system allows emergency medical units to access a patient's medical records instantly and provide immediate care en route to a hospital. By combining **RFID technology**, **VANET communication**, and **cloud storage**, the model enhances the speed, reliability, and security of healthcare services on the move.

4.8 Infotainment as a Service (IaaS)

The integration of cloud computing with vehicular networks also supports multimedia and infotainment services, which enhance both driver experience and road safety. The concept of Mobile Services in Cloud Vehicular Networks (MSCVNs) enables vehicles to access cloud-based storage and computing for media streaming, entertainment, and information sharing. Additionally, Cloud-based Intelligent Transport Systems (CITS) utilize a three-tier cloud structure—comprising data, service, and application layers—to deliver services such as intelligent parking, cloud data mining, and real-time VANET-based applications. CITS integrates IoT, artificial intelligence, and cloud computing to create smart mobility solutions. For instance, the intelligent parking service allows vehicles to locate and reserve parking spaces through mobile applications connected to the cloud. These infotainment and smart applications not only enhance user experience but also contribute to safer and more connected road environments.

5. SECURITY ISSUE IN VANET-CLOUD ARCHITECTURE

Security remains a major challenge in vehicular cloud systems due to their distributed, dynamic, and high-mobility nature. Key issues include:

- Data integrity and confidentiality
- Authentication and authorization
- Malicious node detection
- Data corruption and manipulation
- Privacy protection of users and vehicles

Since VCC allows vehicles to function as cloud nodes, compromised or malicious vehicles can spread false data, leading to network instability and unsafe driving conditions.

6. PROPOSED SECURITY-BASED VAN-CLOUD ARCHITECTURE

The proposed secure VAN-Cloud architecture includes three main layers:

1. **Client Layer:** Represents end-users (drivers, passengers, or onboard systems) accessing cloud services through **Service Access Points (SAPs)** such as smartphones, laptops, or OBUs.

2. **Communication Layer:** Provides connectivity between clients and the VANET-Cloud through RSUs and wireless networks.
3. **Standard Cloud Layer:** Comprises stationary cloud data centers managing VANET services. A **Security Layer** functions as a **third-party authentication service** using token-based validation. Vehicles must present valid tokens to access cloud applications, ensuring secure service access.

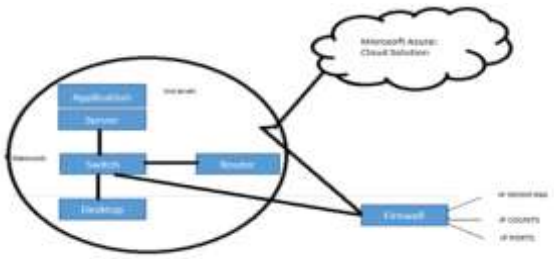

Fig 2: Secure VAN-Cloud Architecture

7. CONCLUSION

A wide range of applications and services, including healthcare, disaster management, Infrastructure as a service, Gateway as a service, Smart traffic light, Infotainment as Services, will potentially enhance the possibilities of the existing transportation system through VANETs with cloud computing services. This review paper aims to outline the possibilities for the VANETs Cloud, using the characteristics, and type of architecture, layers in the architecture, challenges to be addressed, and services offered. Although the VANETs Cloud concept will enhance the capabilities of VANETs and Intelligent Transportation Systems (ITS), it is quite comprehensive, and there are many security issues and implementations to address, before deploying a real-world service, this review has highlighted some of the emerging issues in the context of VANETs Cloud.

Our future work will begin detailed and deeper investigation in finding solutions to the issues and challenges noted in this review paper, to guarantee a safe and trusted implementation of VANETs Cloud services in the future.

REFERENCES

1. **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]
   – A foundational paper explaining VANET structure, applications, and threats.
2. **Raya, M., & Hubaux, J. P. (2005)**
   The security of vehicular ad hoc networks
   Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN).
   – Discusses core security issues in VANETs including authentication, privacy, and data integrity.
3. **Ahmed, E., Gani, A., Abu Bakar, K., & Khan, M. K. (2014)**
   Vehicular cloud computing: architecture, applications and security issues
   Vehicular Communications, 1(3), 125–132.
   [https://doi.org/10.1016/j.vehcom.2014.05.001]
   – An excellent overview of vehicular cloud computing with a special focus on architecture and security.
4. **Zhang, Y., Wang, L., Sun, H., & Wang, Y. (2017)**
   A survey of security and privacy issues in vehicular ad-hoc networks
   Smart Cities, 1(1), 26–39.
   – Covers attacks, threats, and cryptographic solutions for secure vehicular systems.
5. **Abuelela, M., & Olariu, S. (2010)**
   Taking VANET to the cloud
   Proceedings of the 8th ACM international workshop on Vehicular inter-networking (VANET 2010)
   – Proposes cloud integration with VANET and discusses the advantages and challenges.