Available online at www.garmian.edu.krd

Passer Journal

Passer 7 (Issue 1) (2025) 37-61

Original Article

Enhanced Security Taxonomy for Fog-Enabled VANETs: A Comprehensive Survey on Attacks, Challenges, Applications and Architectures

Dana Kareem Hama*[1], Foad Salem Mubarek[2], Firas Abdulhameed Abdullatif [3]

[1] *Department of Computer Science, College of Science, University of Garmian, Sulemaniya, Kalar, Iraq*
[2] *College of Computer Science and Information Technology, University of Anbar, Ramadi, Anbar, Iraq*
[3] *Department of Computer Science, College of Education for Pure Sciences (Ibn Al-Haitham), University of Baghdad, Baghdad, Iraq*

Received 11 November 2024; revised 30 November 2024;
accepted 01 January 2025; available online 31 January 2025

DOI: 10.24271/PSR.2024.488319.1811

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) are integral to Intelligent Transportation Systems (ITS), enabling real-time communication between vehicles and infrastructure to enhance traffic flow, road safety, and passenger experience. However, the open and dynamic nature of VANETs presents significant privacy and security challenges, including data eavesdropping, message manipulation, and unauthorized access. This study addresses these concerns by leveraging advancements in Fog Computing (FC), which offers low-latency, distributed data processing near-end devices to enhance the resilience and security of VANET communications. The paper comprehensively analyzes the security frameworks for fog-enabled VANETs, introducing a novel taxonomy that classifies threats, attack vectors, and mitigation strategies across various applications and architectures. Additionally, this study outlines methods for secure data sharing, real-time authentication, and threat mitigation while evaluating emerging security frameworks. By highlighting the advantages of FC—such as localized data privacy management, mobility support, and real-time decision-making—this survey establishes a foundation for future research and innovation in developing secure, scalable, and robust VANET systems. The findings offer practical implications for designing next-generation ITS with enhanced security and operational efficiency.

Keywords: VANET, Fog Computing, Security, Intelligent Transportation Systems, Fog servers, Vehicle Fog Computing.

1 Introduction

Regarding Intelligent Transport Systems, Vehicular Ad Hoc Networks (VANETs) are crucial because they allow vehicles and roadside equipment to communicate wirelessly. Nevertheless, VANETs have challenges because of their large-scale and dynamic nature, calling for robust security measures to prevent assaults that might endanger lives. Because open wireless communication is vulnerable to assaults such as message manipulation, eavesdropping, and deletion, security is a big concern with VANETs. Stringent authentication procedures must be implemented to safeguard personal information and avoid illegal access. In order to detect and prevent malicious actions, such as data packet discarding and information tampering, security mechanisms are essential in VANETs[1-3].

* Corresponding author
E-mail address Dana.Kareem@garmian.edu.krd (Instructor).
Peer-reviewed under the responsibility of the University of Garmian.

By shifting focus to FC, we may improve low-latency services, reduce incoming traffic to the cloud, and streamline computing processes between end devices and the cloud. A fog server (FS) is a bridge between a vehicle and the cloud that collects data from sensors mounted on the vehicle and provides instant responses to apps that can't handle delays [4]. The main benefits of combining VANET design with Fog Computing (FC) are low latency, wireless connection availability, geographical dispersion, real-time communication, vehicle movement optimization, scalability, and expansion possibilities[4-6].

Integrating FC into VANET enhances security, and storing sensitive data locally in fog nodes strengthens privacy and security standards by reducing the amount of data sent over the internet, making it less susceptible to cyber-attacks. Companies can more easily comply with data sovereignty and privacy regulations when they process data locally since this allows them to keep sensitive information within certain geographic or legal boundaries[5,7,8].

The emergence of vehicles integrated with communication hardware and software has enabled them to function as fog infrastructure, creating virtual storage, communication, and computing capabilities; this transformation is referred to as vehicular fog computing (VFC)[6,7]. The[8] centers on methodologies for detecting traffic congestion utilizing data from connected automobiles. The[9] provided an exhaustive study. Proposed a novel classification system for Vehicle Fog Computing (VFC) operations that organizes the challenges faced at each stage into specific categories: phase, node selection, secure data sharing, authentication, encryption, auditing, and data privacy; resource allocation in task division, scheduling, and load balancing; and result retrieval in phase, node selection, and path recovery.

The integration of the Internet with traffic management in transportation has been facilitated by the widespread adoption of Internet of Things (IoT) technologies, particularly in intelligent transportation systems (ITS). These systems are anticipated to enhance road traffic and safety conditions substantially. Effective traffic monitoring, encompassing aspects such as speed limits, pollution checks, and emergency response to accidents, is crucial [10,11].

Vehicular Ad-hoc Networks (VANETs) are mobile networks consisting of vehicles with changing network structures and intermittent connectivity. Ensuring security and privacy in VANETs is of utmost importance because information is distributed in a publicly accessible setting. To maintain the effectiveness and dependability of VANETs, they must fulfil security protocols that preserve the integrity of transmitted messages, preventing any unauthorized modifications by potential attackers[12].

VANET, or vehicle-area network, is an ad hoc mobile network that aims to improve traffic flow and decrease vehicle accidents by transmitting relevant data to vehicles and drivers. Registration and administration depend on on-board units (OBUs) and roadside units (RSUs). Through Dedicated Short-Range Communication (DSRC), VANETs enable vehicles to interact with one another, with RSUs, and with authorized parties. Sensors, cellular devices, global positioning systems, and event recorders will be standard equipment for most VANET cars to monitor traffic and congestion. VANETs offer various applications, including entertainment, traffic efficiency, active road safety, and management. Security is crucial for VANET, as it is a wireless communication system and careful security architecture is necessary to protect against abusive activities[3,13-15].

The primary elements of intelligent vehicles are numerous advanced technologies integrated into vehicles to provide real-time measurement and safety functions. All of these devices can self-organize communication to establish a sensor network. Environmental data from the vehicle is collected via internal sensors. System architecture should be developed to assist drivers in accident prevention. The intelligent vehicle is generally equipped with multi-beam LIDARs, microwave radars, high-resolution cameras, and other devices to get precise and enough environmental data. An intelligent vehicle generally comprises the following components and technologies, as illustrated in Figure 1[16]:

1. CPU: Efficiently executes instructions by performing arithmetic, logical, and input/output activities.
2. Wireless transceiver: employs vehicle-to-vehicle and vehicle-to-infrastructure communications to convey data and information.
3. GPS receiver: This apparatus acquires data from the Global Positioning System and facilitates navigational services. By interfacing with communication equipment, a GPS can autonomously transmit the exact location of the vehicle with an accuracy of under 1 meter. The collected information facilitates group creation and enables prompt and precise alerts regarding accidents, hazardous driving conditions, and similar issues.
4. Sensors: A vehicle is equipped with several sensors, both internally and externally, to gauge parameters such as velocity, distance from other cars, and more. An ultrasonic sensor utilizes sound waves reflected from objects. It assesses the closeness and velocities of adjacent objects.
5. I/O interface: facilitates straightforward human-vehicle interaction.
6. Radar: Utilizes radio waves to identify and monitor adjacent cars. There are two categories of vehicle radars: long-range radars and short-range radars. Currently, adaptive cruise control systems employ these sensors.
7. LIDAR: Light Detection and Ranging utilizes a sensor with one-dimensional scanning capability to accurately ascertain a vehicle's relative distance by scanning a horizontal surface with laser beams. This sensor emits infrared light pulses with a wavelength ranging from 850 to 950 nm, utilizing high-intensity laser beams.
8. OBU: Internal division. Every vehicle in the system is equipped with an On-Board Unit (OBU) that manages the vehicle's connectivity with Roadside Units (RSU), Smart Mobile Base Stations (SMBS), and other vehicles using Dedicated Short-Range Communications (DSRC) or LTE-V.
9. LCS: A local camera sensor is a device that monitors driving behavior while concurrently and correctly identifying objects.

This study thoroughly analyzes VANETs, including security, applications, networking, and challenges. None of them collected extensive data in a singular survey. Although several designs have been proposed in the literature to improve the security of VANETs, a comprehensive evaluation is still necessary to determine the effectiveness and precision of these architectures. It is imperative to meticulously assess the security vulnerabilities arising from amalgamating emerging technologies, such as Fog Computing, with the existing VANET. When sophisticated

technologies like AI and ML are integrated into Vehicular Ad-Hoc Networks (VANETs), security flaws and privacy problems become more apparent. Therefore, data transmissions between cars must be protected by stringent measures to ensure their authenticity and privacy[20].

The rest of this paper is structured as illustrated in Figure 2. This study aims to examine, classify, compare, and summarize research conducted in Fog-based security in VANETs from 2017 to 2024. The contributions of this study can be delineated as follows:

1) Provision of taxonomy of VANET services and applications, accompanied by a comprehensive description of all services.

2) Summarize the survey by discussing the many new research problems and offering ideas with recommended references to meet them.

3) Extensive study to classify different security threats in VANETs.

4) Provide an overview of VANET and Fog computing to emphasize the advantages and disadvantages associated with these technologies.

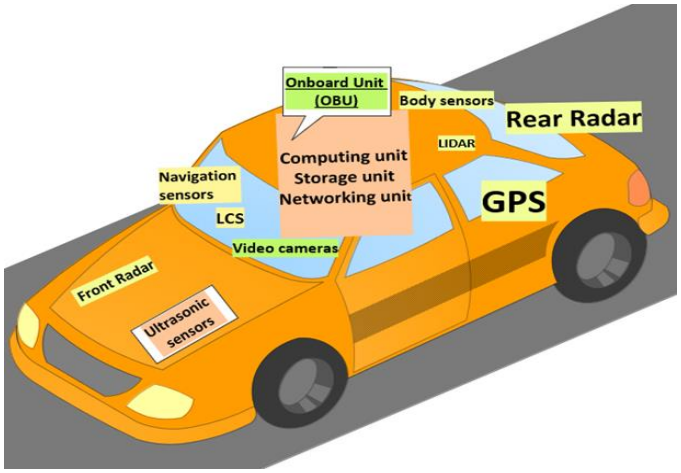

Figure 1: Smart Vehicle Component in VANET[16].

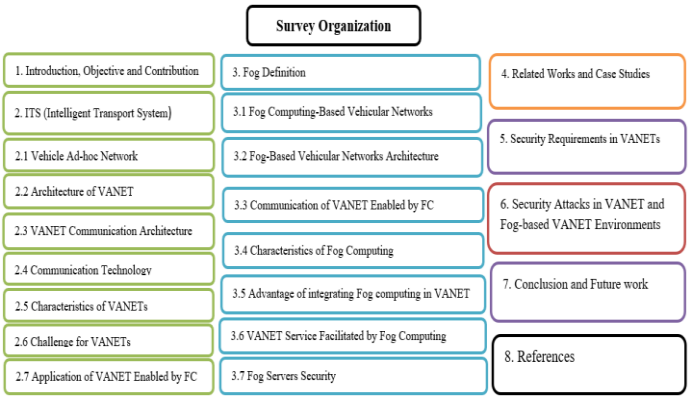

Figure 2: Survey Organization.

2 ITS (Intelligent Transport System)

The intelligent transportation system (ITS) is designed to enhance consumers' everyday lives, as a significant portion of their day is spent in transportation. The ITS offers various services, including transportation and road safety applications, internet surfing, text messaging, phone communication, video conferencing, and file downloading. Vehicular ad-hoc networks (VANETs) are the essential technology of Intelligent Transportation Systems (ITS) that combines modern wireless technology with cars[13,17,18].

The advancement of public transportation networks globally, whether for commercial or personal use, has necessitated the development of Intelligent Transportation networks or VANET. Based on the most recent figures, the global vehicle population now stands at 1 billion, with projections suggesting it may surpass 2 billion by 2035. In Vehicular Ad-Hoc Networks (VANETs), real-time information on road conditions and safety may be transmitted wirelessly between cars, either directly or through other means such as passengers' handheld devices, Roadside Units (RSUs), Unmanned Aerial cars (UAVs), and so on. Efficiently preventing traffic accidents and road congestion is possible[19,20].

The allocation of 75 MHz of the recurrence range by the Federal Communications Commission (FCC) has been designated explicitly for dedicated short-range communications (DSRC), enabling correspondence between vehicles and between vehicles and roadside. These networks provide many services, such as information on car safety, broadcast of traffic alerts, planning of routes, context-aware infotainments, and surveillance solutions. Nevertheless, the management of conventional architectures is hindered by several issues, including the need for optimal resource usage, the need to balance traffic flow, the imposition of delay limitations, and the requirement for high mobility [13,21].

The ITS plays a pivotal role in transforming transportation and road safety. The fundamental concept of ITS involves continuous communication among vehicles on the road, facilitated by vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication. However, implementing the necessary technologies for seamless communication has been gradual and costly, requiring extensive equipment like Roadside Units (RSUs) and On-Board Units (OBUs) in vehicles and along roadways. Achieving full saturation of these units is essential for the optimal functioning of ITS [2,10,17,22].

2.1 Vehicle Ad-hoc Network

Wireless Ad Hoc Networks (WANET) are the theoretical foundations upon which all ad hoc networks rest. An example of a mobile ad hoc network (MANET) is a vehicular ad hoc network. Without a central network, mobile nodes in a MANET can communicate with one another. The network's nodes may repair themselves automatically. Because nodes in a Mobile Ad hoc Network (MANET) tend to wander about randomly, the network's topology often changes over time. With its unique behaviour, each node acts as a router. VANET has developed into a more reliable and stringent system alternative to MANET.

Because nodes in a VANET are free to join and leave the network at will, a different set of routing protocols is required than in a MANET.VANET is made up of RSU and mobile nodes. An OBU, which processes incoming and departing data, is installed in every vehicle. It incorporates sensing devices. Highways are dotted with RSUs, which act as go-betweens for mobile nodes and the trusted authority [1,24].

One of VANET's main goals is to make it easier for drivers to share information safely and reliably online. Mobile nodes are usually sensor-equipped cars, and static infrastructure, including RSAPs (permanent roadside access points), makes up the system. In addition, it incorporates several wireless connections, including those between vehicles, between vehicles and infrastructure access points, and between access points and vehicles [8,19].

2.1 Architecture of VANET

VANET is a self-sufficient network that has emerged due to recent progress in networking technology. The VANET architecture has three fundamental components: The On-Board Unit (OBU), the Roadside Unit (RSU), and the Application Unit (AU). Vehicles in VANETs are equipped with On-Board Units (OBUs), which are wireless communication devices. This component enables the transmission of information between the vehicle and Roadside Units (RSUs) and among other cars or On-Board Units (OBUs). The OBU device uses an interface to connect with other OBUs. The OBU provides several services, encompassing routing and network congestion management. The second component, the Roadside Unit (RSU), is a device or equipment strategically positioned along the roadway or at certain locations like intersections. The third component, AU, denotes a device incorporated into the vehicle. The AU initiates communication with the network via the OBU. The OBU may be connected either wirelessly or via a wired connection[1,17,23,24].

The main objective of a VANET is to allow nearby vehicles to communicate with one another. Virtual Ad Hoc Networks (VANETs) rely on movable nodes, such as automobiles, to form a robust communication network. The following is an explanation of the main parts of VANETs.

- **Vehicles:** they are the backbone of VANETs; they communicate with each other and the infrastructure via onboard units (OBUs). Typical components of these OBUs include sensors, wireless communication devices, GPS devices, and other technologies that facilitate the exchange and processing of data [4,26,28].
- **Roadside Units (RSUs):** are fixed infrastructure located along highways or at specific areas such as intersections. RSUs collaborate with OBUs in vehicles to provide essential services such as internet access, traffic information, and safety notifications. They can also collect data from passing vehicles to evaluate traffic conditions or environmental concerns [23,25,26].
- **OBUs:** devices attached to vehicles communicating with RSUs and other OBUs. They typically include components like a CPU, memory, GPS receiver, and several transceivers for various communication protocols (e.g., dedicated short-range communication (DSRC), Wi-Fi, and long-term evolution (LTE)). OBUs process and store data to improve navigation, augment safety features, and deliver entertainment services [23,25,26].
- **The Traffic Management Centre (TMC):** is the operational hub for monitoring traffic and infrastructure communication. It examines data acquired from RSUs and vehicles to monitor traffic conditions, coordinate traffic signals, and dispatch emergency services as necessary. Traffic Management Centers employ data to implement traffic management strategies and provide real-time traffic information to drivers [25,27].
- **Communication Systems:** VANETs comprise many wireless technologies, including Dedicated Short-Range Communications (DSRC), Wi-Fi, cellular networks (LTE and 5G), and satellite communications. These systems facilitate vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) connections, essential for the functioning of VANETs [5,23,26].
- **Sensors and Actuators:** Vehicle sensors collect various data, such as speed, direction, fuel level, engine metrics, and proximity to nearby objects. Actuators implement commands from the vehicle's processing system to perform actions such as stopping, adjusting speed, or changing direction based on sensor inputs and communication data [25,28].
- **Security and Privacy Protections:** Given the substantial dangers linked to vehicle communications, especially regarding safety and privacy, VANETs incorporate extensive security and privacy protections. This includes cryptographic techniques, secure authentication protocols, and data privacy measures to protect against unauthorized access while maintaining the integrity and confidentiality of transmitted information [25,29,30].

2.3 VANET Communication Architecture

Vehicular Ad Hoc Networks (VANETs) are a kind of Mobile Ad Hoc Networks (MANETs) where the nodes are automobiles—their great mobility results from the road layout, quick network architecture, and an unstable communication environment. Vehicular ad hoc networks (VANETs) consist of five distinct communication patterns: Vehicle-To-Vehicle (V2V), Vehicle-To-Infrastructure (V2I), Vehicle-To-Pedestrian (V2P), In-vehicle (InV) communication and Vehicle-To-Network (V2N) [1,2,19,31]. Several sorts of communication linkages may be classified based on the entities involved in the communication, as shown in Figure 3.

The provision of ubiquitous connection between cars in Vehicular Ad-hoc Networks depends not only on fixed infrastructure. The categorization of Vehicular Communication Infrastructure (VCI) is as follows. A different type of architecture exists, known as communication architecture. The vehicle communication architecture consists of eight distinct modes of communication, which are outlined as follows[31].

- **Vehicle to Vehicle (V2V) Communication or Inter-Vehicle Communication (IVC):** A multi-hop multicast or broadcast technique is used to disseminate messages in V2V or IVC communication. When a vehicle can't establish a direct connection to the RSU, this method of communication is used. While opposed to V2I, V2V uses less bandwidth while sending messages [14,19,31-34].
- **Vehicle to Infrastructure (V2I) or Infrastructure to Vehicle (I2V) Communication or Roadside Vehicle Communication (RVC):** The message is propagated utilizing the RSUs and vehicles in V2I, I2V, or RVC communication. The RSU notifies all nearby cars of an upcoming event using single- or multi-hop transmission. To communicate with cars that are not immediately in its path. Both vehicle-to-vehicle (V2V) and infrastructure-to-vehicle (I2V) communication subtypes include sparse roadside vehicle communication (SRVC) and ubiquitous roadside vehicle communication (URVC). Compared to V2V communication, which demands lower bandwidth, V2I communication demands larger bandwidth. For example, after reviewing its internal database, the RSU will periodically broadcast the speed limit warning message to cars after determining the proper restriction. This is done to broadcast speed warnings or limitations. In addition, the RSU will need extra bandwidth so that it can alert the vehicle, either visually or audibly, to slow down if it exceeds the desired speed limit[14,31,32,35].
- **Infrastructure-to-infrastructure (I2I):** Connections provide the exchange of global road traffic information between infrastructures located in specific regions[33,35,36].
- **In-vehicle (InV) communication:** Vehicle communications refer to the customized communication system installed within a vehicle. Research in VANETs is crucial since it allows for monitoring a vehicle's performance and the driver's physical state, including signs of sleepiness or fatigue. These factors pose significant risks to the safety of the vehicle, driver, and general public[2].
- **Vehicle-to-Pedestrian (V2P):** Communications enable the exchange of information between cars and portable devices in the vicinity of pedestrians[19,34,35,37,38].
- **Vehicle-to-Barrier (V2B):** Connections are necessary for exchanging data with the roadside barriers. This connection is enhanced by a vast array of sensors installed in vehicles to prevent accidents caused by vehicles veering off the road[2,19].
- **V2I (Vehicle-to-Internet) or V2N (Vehicle-to-Network):** This technology enables direct connections between automobiles and the Internet, including servers and other related systems. This form of communication relies on cellular technologies such as 3G, 4G, and 5G, roadside Wi-Fi access points (AP), and satellite connections. The introduction of mobile (femtocell) is a small, low-power cellular base station or mobile tiny cell aimed at addressing the high mobility requirements of Intelligent Transportation Systems (ITS)[35,39].
- **Vehicle-to-Cloud (V2C):** Communication enables the exchange of information between Roadside Units (RSUs) and cloud servers. This connection serves several purposes, including data analysis, decision-making, and transportation prediction[2,36].
- **Vehicle-to-UAV (V2U):** Communication involves wireless data transfer between vehicles and (UAVs) unmanned aerial vehicles via Ground to Aerial connections[36].
- **Vehicle-to-Everything (V2X):** encompasses the data exchange between a vehicle and any other network-enabled entity, including all components engaged in this connection. This vehicular communication technique is broad and encompasses various approaches, including V2I, V2V, Vehicle-to-Pedestrian (V2P), Vehicle-to-Device (V2D), and Vehicle-to-Grid (V2G)[24].
- **Vehicle-to-Sensors (V2S):** Communication enables the transmission of sensing data between cars and embedded sensors on the road and the surrounding environment. Sensors are designed to detect and collect data on the condition of the vehicle and its surrounding environment. The collected data will be sent to the Electric Control Unit (ECU) for data processing. The V2S system utilizes either wired or wireless communication. The sensors and ECU can interact through physical connections such as Local Interconnect Network (LIN), Controller Area Network (CAN), (Flex Ray), which is defined as a high bandwidth communication protocol intended for high-speed technology in automotive vehicles and Media Oriented Systems. Transport (MOST). They can also communicate wirelessly using D2D Out-band mode, which includes technologies like Zigbee, Wi-Fi Direct, Bluetooth, and ultra-wideband[11,19,35].
- **Hybrid Vehicle Communication (HVC):** HVC uses both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) or vehicle-to-vehicle (I2V) communications. Many ITS cooperative applications now use HVC networks. Some examples of these services include entertainment (including road condition sensors), interactive gaming, traffic management, and accident warning systems. In

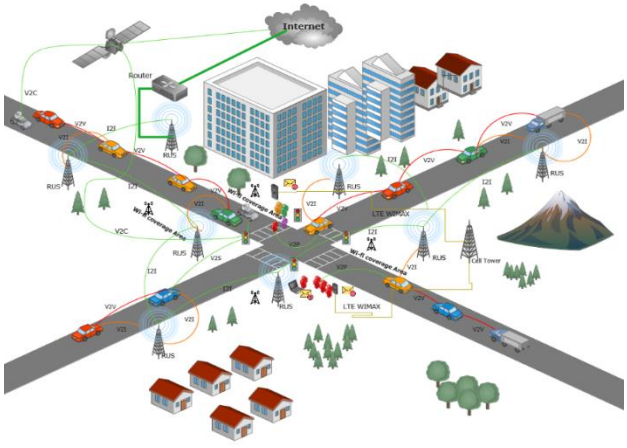

Figure 3: Vehicular Communication Infrastructure in the VANET.

situations when the path is not explicitly given, packets are routed via routing-based (RB) Communication[31].

2.4 Communication Technology

Dedicated Short-Range Communication (DSRC) and Wireless Access in Automotive Environments (WAVE) are two medium-range protocols standardized for automotive networks. WAVE offers interoperable, efficient, and dependable radio communications for both safety and non-safety applications via V2V, V2I, and V2R communications utilizing DSRC. The WAVE protocols (IEEE 802.11p/1609) exhibit scaling challenges, restricted coverage, and indefinite latency. DSRC is utilized for the physical (PHY) and medium access control (MAC) layers in IEEE 802.11p (WAVE). The Federal Communications Commission (FCC) in the USA has designated 75 MHz of spectrum within the 5.9 GHz band (ranging from 5.850 to 5.925 GHz), which includes one control channel (CCH) for Vehicle-to-Vehicle (V2V) Dedicated Short-Range Communications (DSRC). This allocation provides seven channels, facilitating vehicle speeds of up to 200 km/h, communication ranges of 300 to 1000 meters, and data rates between 6 Mbps and 27 Mbps. In high-density situations, increased packet competition and collisions result in elevated packet delay and loss. The MAC layer must regulate access to the shared channel to ensure equitable car usage. The CSMA/CA protocol serves as the default media access method in WAVE MAC and employs a distributed coordination function (DCF) to avert collisions[19,40-42].

2.5 Characteristics of VANETs

In a Vehicular Ad-Hoc Network, cars are seen as mobile nodes that autonomously arrange and configure themselves and establish communication with other vehicles to exchange information. VANETs have many attributes owing to their dynamic nature, although they also present several obstacles [20]. The following features are necessary for comprehending and crucial for developing security in VANET[1]. VANETs have additional inherent characteristics that set them apart from conventional Ad hoc Networks. The subsequent attributes characterize the properties of VANETs[31].

- **Frequently changing topology and frequently disconnected Network:** The primary attribute of this system is the frequent alteration in the network topology caused by the nodes' significant mobility and frequent repositioning. Frequent disconnections result from elevated mobility and a highly dynamic structure. The evolving network architecture and frequent interruptions provide considerable obstacles in creating a resilient routing system for VANETs[20]. In Vehicular Ad Hoc Networks, the speed of vehicles demonstrates consistent variations, while the network structure depends on the mobility of these vehicles. As a result of the fast alterations in the topology, the maintenance of communication among cars is severely compromised. When building a VANET protocol, it is essential to take into account the issue of frequent network disconnection [31,32]. Vehicles can join in VANETs at any given moment. Therefore, the vehicle that first joined the VANET may not join later. Consequently, VANETs provide a significant security problem[1].
- **Dynamic Network Topology:** Because of the constantly changing network structure, it is exceedingly challenging to identify malevolent vehicles that are travelling at high velocities[1],[32,43]. And VANETs have a high degree of scalability. They may be deployed in rural areas, and they can subsequently expand to encompass several urban centres. The network size of this kind is indeterminate and can be considered geographically unbounded[20].
- **Real-Time Constraints:** The vehicles engage in limited real-time communication, necessitating prompt responses and decision-making within a constrained timeframe[1,32].
- **Delay Constraints:** For some ITS uses, like emergency brake warnings, getting the word out in time to prevent a collision is paramount. Delay management becomes increasingly critical in these contexts—limitations as an alternative to offering high data speeds[31]. Within a VANET, vehicles travel at high velocities and have limited tolerance for delays that may occur during vehicle-to-vehicle communication[1]. Due to the varying velocities and unpredictable changes in the direction of the nodes, the communication between them is time-sensitive[20].
- **Predicting the Mobility of Vehicles:** The nodes of VANET adhere to a predetermined trajectory of movement. VANET falls within the area of geographical communication since it aligns itself according to the map. By employing this habit, we can anticipate their pattern of movement[20]. Traffic patterns and route directions limit vehicle movement in VANETs. These future mobility models and projections are necessary for VANET protocol design. It is critical to take the vehicle's directions into account[31-43].
- **Urban and Highway Traffic Scenarios:** There are two distinct kinds of traffic that VANETs can handle: highway and urban. The absence of impediments makes the highway situation easy to understand, in contrast to the complex urban traffic scenario. Streets, buildings, and barriers make up the complex. Both urban and rural traffic circumstances, as well as the effects of shadowing and path loss on communication, should be taken into account while developing a VANET protocol[31].
- **Rich in Resources:** Nodes in a VANET have sufficient processing power, memory, and other resources, including OBUs. Typically, OBUs are installed on vehicles and communicate with RSUs or other OBUs. Each OBU has its own Resource Command Processor (RCP), and resources have their read/write memory for storing and retrieving data. In addition to a network device for short-range wireless communication based on IEEE 802.11p technology, OBUs also have a user interface that can connect to other OBUs[31]. A benefit of the nodes in VANET is their abundant energy supply and storage capacity. Specifically, the nodes in a VANET

consist of automobiles, which provide abundant power supply and substantial storage capacity compared to nodes in ad-hoc networks. Thus, power and storage are always abundant on VANETs[20].

- **Interaction with onboard sensors:** sensors are crucial in VANETs as they are responsible for capturing real-world events, such as the vehicle's velocity[15].
- **High Application Requirements:** VANETs have several uses, the most notable being safety applications. These applications have high requirements regarding real-time reaction, efficiency, and dependability. Ensuring the prompt and seamless delivery of services from start to finish is of utmost importance for safety applications. Even a minor delay might result in adverse outcomes[20].

2.6 Challenges for VANETs

Due to certain features and difficulties, providing services and assuring their dependability are complicated and multi-metric dependent concerns in VANET networks. This survey explains a few of these challenges.

- **Mobility Variation:** In the VANET network, the objects that communicate can be categorized as stationary (e.g., RSUs), slow-moving cars (e.g., automobiles in traffic jams and road junctions), or fast-moving entities such as vehicles on sparsely populated highways. The variability in the mobility of nodes has presented several problems with communication in VANETs. In the case of high-velocity scenarios, the chances of successful communication between VANET entities would be limited due to the restricted transmission range. In a case where the velocity is moderate, the communication in VANET will be negatively affected by the Doppler Effect, frequent connection disruptions, and increased end-to-end (E2E) latency. In the dense environment scenario, although there is a large capacity for data transfer, there are several challenges related to increasing road traffic density. These concerns include data collisions, limited bandwidth, channel fading, packet loss, and signal interference[1,19,32,44-46].
- **Frequent Network Fragmentation:** The density of vehicles might vary depending on the time and location. For instance, the density is often high at crossroads and roads near offices and marketplaces. Additionally, the density is often greater during the daytime than at nighttime. The density and mobility of VANET nodes will significantly influence the fragmentation of the VANET network. The network will experience several fragmentations as the node density declines, leading to a detrimental impact on communication continuity and packet forwarding. Furthermore, accelerating the cars to high speeds will enhance the dynamic nature of the VANET structure. As a result, the VANET network may get fractured into several distinct segments[19].
- **Heterogeneity:** The VANET network consists of several nodes that vary in their features and use. These nodes, such as Roadside Units (RSUs), can be stationary or mobile, such as cars. In addition, certain automobiles need to share entertainment data, while others necessitate exchanging safety-related data. In addition, manufacturers impose several limitations that restrict data transfer and exchange procedures. Autonomous car makers may impose further limitations on the privacy of the vehicle's data. Consequently, a VANET system must address the diversity of nodes and services[19,20,44].
- **Scalability:** In VANET, communication can occur in metropolitan areas, multiple urban areas, or across huge cities and nations. Therefore, the VANET network has the potential to be geographically infinite in size. One of the primary obstacles in vehicular communication is scalability. Consequently, the VANET connection must exhibit dependable performance, even when the number of communication nodes is limited. Scalability refers to the capacity of a network to expand and adjust itself to accommodate future expansion and modifications. This is feasible if the system can locate and utilize the location information of each node in the data forwarding mechanism. This obviates the necessity of being aware of the network topology of the VANET, hence reducing the burden of control messages[1,19,20,44,45].
- **Low fault tolerance:** Real-time communication is necessary for safety-related services on the VANET network. Nevertheless, flaws or inaccuracies might lead to further postponement in data transmission, culminating in traffic buildup and perhaps catastrophic events. To prevent such scenarios, it is crucial to implement proactive security measures promptly, enabling drivers to respond promptly in the event of an emergency[19,44,46].
- **Data security:** to guarantee reliable and efficient communication, secure data transmission is essential. The data destination is responsible for ensuring the packets remain unaltered throughout transit. Encryption must also ensure that no one can decipher or access the data if it is in transit. Verifying the message's provenance from the intended sender, not an intermediate, is crucial. Security must be a top priority when adopting VANETs since hacked vehicles may cause traffic jams and deadly accidents if hackers can take control of the network[19,20].
- **Data privacy:** Many people are wary of giving up information that could identify where they're going, such as details on the cars they drive. The emergence of data privacy as a key problem highlights the need to find a careful equilibrium between strong privacy protections and personal preferences[19,20].

2.6 Application of VANET

The many classifications of VANET applications include distinct demands, including performance, QoS, security, and privacy. Safety-related applications have strict security requirements, including mutual authentication, authorization, integrity, resilience against attacks, nonrepudiation, and trust management. Performance-wise, these applications are very responsive to both latency and delay, requiring minimal delay and latency. This is

crucial since the decisions made based on the information in these messages have a direct impact on human lives [18,24,47].

Figure 4 represents the classification of VANET services and the many applications within each category[24]. These apps need context awareness and robust security measures to protect against attacks. On the other hand, entertainment and other value-added VANET applications and services may tolerate delays and have less strict security requirements[47].

- **Safety Warning Applications:** These applications aim to alert drivers to potentially dangerous circumstances on the road and deliver warnings when they receive such messages using wireless communication technologies. Apps with strict delay limits are designed to guarantee the timely transmission of life-or-death notifications[14,31,44]. The Local camera sensors (LCS) may transmit a warning message to the driver for certain procedures. To assist the driver in evading and avoiding perilous situations, it is advantageous to furnish him with timely and repeated alerts. The LCS device must be capable of generating this type of warning message for the drivers. Upon transmitting a specified warning message, LCS will relay the blocked vehicle exercise to the VF server. The identification includes evidence of functioning and the number of vehicles [14,20,25,30].
- **Entertainment Applications and General Information Services:** Providing passengers with entertainment services and enhancing traffic efficiency are the primary goals of these programs, which also offer general information services. Services that allow users to communicate with one another while on the line include traffic and weather reports, recommendations for the best routes to take, value-added services, and nearby restaurants and petrol stations. V2I connectivity is often essential for these applications[18,20,24,31].
- **Transportation Traffic Improvement Application:** Traffic optimization programs aim to enhance road traffic and reduce road accidents by managing traffic flow and regulating transportation congestion [19,20,47]. All cars transmit their present states (speed and position) and gathered information (weather and road conditions) to the linked server inside connection zone I, as delineated by the FSs in VANET facilitated by FC. Upon collecting data from vehicles, the server may ascertain the present traffic conditions in the vicinity and monitor its dynamics. To avert traffic congestion, one may employ this method[25].
- **Driving System Monitoring Application:** These applications focus on monitoring the driver's physical well-being when driving and tracking the state of the vehicle and its components [14,19,44]. Due to its image processing capabilities, the camera positioned at the traffic light could interpret license plates inside its range of vision. Alongside the vehicle's identifying number, it may relay its latest location to an adjacent FS. Local camera sensors (LCSs) are affixed to the front of automobiles to monitor the driver's actions. The concept of spatiotemporal segmentation for video objects is utilized to determine when the driver is interacting with their handheld cameras[25]. The driver's physiological condition is crucial for ensuring public transportation safety[20,47].

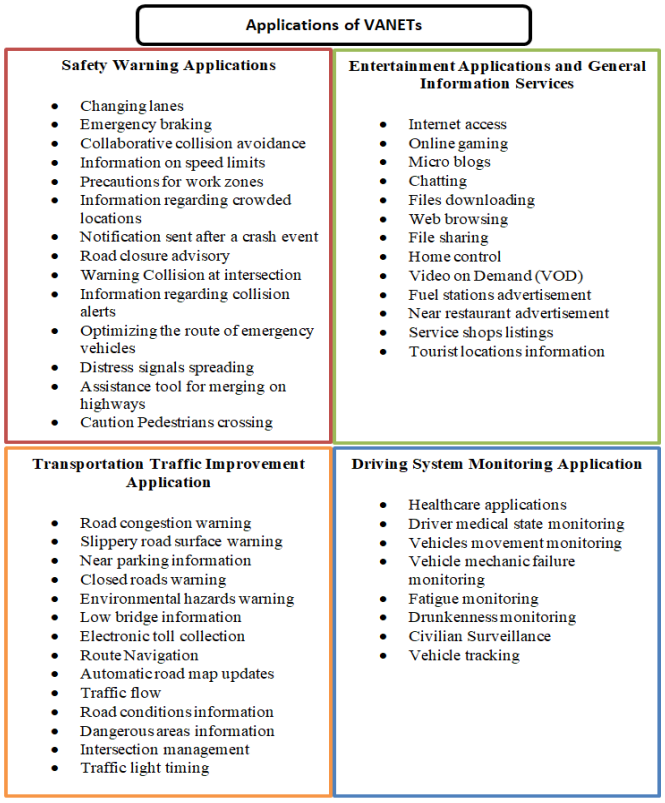

Figure 4: VANET applications classification.

3 Fog definition

Fog computing is a distributed computing architecture that brings storage and processing resources closer to edge devices. Fog nodes refer to nodes that have been enhanced with communication, processing, and storage capabilities. Undoubtedly, the number of devices linked to the internet is increasing, and the bandwidth required to accommodate them is substantial. In addition to bandwidth, it is necessary to have a standard for translating communication protocols[34,48].

Fog computing (FC) is an advanced cloud computing that involves processing data at the network edge, closer to where the data is generated. This is in contrast to the centralized processing at cloud servers in traditional cloud computing. Therefore, FC decreases the burden on the core network and provides an effective method to guarantee Quality of Service (QoS) for applications that rely on local data and real-time analysis, such as location awareness and mobility management[17].

3.1 Fog Computing-Based Vehicular Networks

Edge Computing seeks to relocate the computational resources of cloud computing nearer to the data source. This approach utilizes

devices' processing and storage capacities to establish an intermediary layer between the cloud and end devices. It addresses the challenges of conventional cloud data centers, including network congestion and deterioration of service quality. The Edge layer implementation may be categorized into Mobile Edge Computing (MEC) and Fog Computing (FC). Fog computing. Cisco Systems established the notion of FC in 2012. It possesses a computer layer that utilizes heterogeneous devices such as wireless routers, access points, switches, and IoT gateways. These devices are called Fog Computing nodes and are utilized to process or store data from end devices locally before transmitting it to the cloud[23,34,49].

Fog computing offers a virtualized system that delivers storage, data, and services. It allows for the seamless transfer of real-time data from the cloud to the network edge. This architectural design optimizes the utilization of bandwidth resources, minimizes energy usage, and decreases delay. Fog computing mitigates the limitations of SDN for time-sensitive applications such as linked automobiles and emergency alerts, resulting in decreased service latency. Fog servers are often deployed in macro cell base stations and Wi-Fi access points. Cisco Systems' Locator/ID separation protocol (LISP) facilitates mobility by enabling communication between Fog servers and end devices[29,49]. While implementing fog computing in VANET to enhance efficiency, maximizing the length of connections between automobiles in the context of VANETs is crucial[34,15,50].

3.2 Fog-Based Vehicular Networks Architecture

Fog computing is not a standalone paradigm but rather an extension of cloud services to the periphery. Furthermore, the fog possesses the ability to process data locally with an optimal latency[51]. The architecture of fog computing comprises several layers, and various forms of fog computing are examined. Due to the ongoing development of the VFN and the growing association of many qualities with it, the fog computing paradigm provides heterogeneity by extending fog devices to access points, routers, and end-user devices. This ensures greater suitability for VANET, IoTs, smart environments, pervasive wireless networks, smart watches, green cities, and microgrids, as they require time-sensitive capabilities[25,50]. Multiple architectures with distinct layers have been suggested for fog architecture. Figure 5 illustrates the division of fog architecture into 8 levels.

- **Physical layer- Terminal layer:** The physical layer produces the data. In the context of VANET, data often originates from embedded sensors in vehicles, pedestrians, Road Side Units, and cameras[34]. This layer consists of several end devices that are geographically dispersed. These devices assume the job of retrieving and transmitting data to a superior layer for processing and storage. The gadgets may encompass wearable technology, sensors, autonomous cars, mobile phones, and more items[51]. Physical devices connect with the fog layer via various communication protocols, including 3G, 4G, 5G, Wi-Fi, Bluetooth, Zigbee, etc. This is why the low latency and little delay during data transmission. This stratum covers a rather modest region[22,52].
- **Gateway, server, and fog device layer:** These entities can refer to either a standalone or Internet of Things (IoT) device. However, the fog server possesses superior capabilities compared to the fog device. Many sensors, such as an automobile, can be hierarchically linked to a fog device. Similarly, many fog devices can be connected to a fog server. Under certain circumstances, A fog server and many fog devices may collectively perform extensive activities. This layer also enables communication across fog servers[37,52]. Fog computing resides in the intermediary layer of the architecture. The fog infrastructure consists of many fog nodes, including networking components such as routers, switches, gateways, and computational resources like CPUs, storage, and RAM[22,51].
- **Monitoring layer:** This layer is accountable for monitoring the network's overall performance. This aims to empower the fog device and server to make intelligent judgments on the appropriate distribution of resources across many scenarios. This layer may evaluate current resource performance and predict future resource needs by analyzing data load and current resource availability. Furthermore, it must comply with the specified Service Level Agreement (SLA) criteria[22,34].
- **Processing layer:** This layer is responsible for analyzing data and manipulating data as needed. Within this particular layer, we have the option to either transmit the data to the cloud for additional analysis and manipulation or retain it within the fog server for local processing. In addition, this layer possesses the capability to handle faulty or absent data and restore them following processing[22], [34,51].
- **Storage layer:** This layer enables storage virtualization. Storage virtualization is linking many storage devices over a network to serve as a single storage unit. Furthermore, this layer is a precaution to maintain data backups to avoid any negative influence on the data[22,34].
- **Resource management layer:** This layer manages and allocates resources with a focus on energy savings. It can also ensure the resources' reliability and expandability. While cloud computing allows for horizontal scalability, the fog layer may also enable vertical scalability. This layer can also be used to offer synchronization across many fog servers that are running the same application simultaneously. Energy conservation is utilized at this layer to reduce the expense associated with resource use[22,34,51].
- **Security layer:** Similar to any other architectural design, ensuring security is a crucial part of any construction. This layer offers many degrees of security, including message encryption and decryption, authentication, and ensuring the privacy of the fog nodes[22,34].

- **Application layer:** Numerous studies focus on the application of fog computing since its services address certain limitations encountered in VANETs. In fog computing technology, services, processing, and data are centralized at the network edge instead of just in the cloud, allowing location awareness and latency-sensitive services. In vehicular networks, the Internet of Things is facilitated by Fog Computing. Industrial automation and sensor networks require context-aware processing and sensitive delay services[53]. Various applications exhibit sensitivity to delays. These applications can leverage fog architecture due to the proximity of computation and storage capabilities to the edge devices. Real-time traffic monitoring systems and other applications that rely on Augmented Reality (AR) can gain advantages from fog infrastructures[22,34].

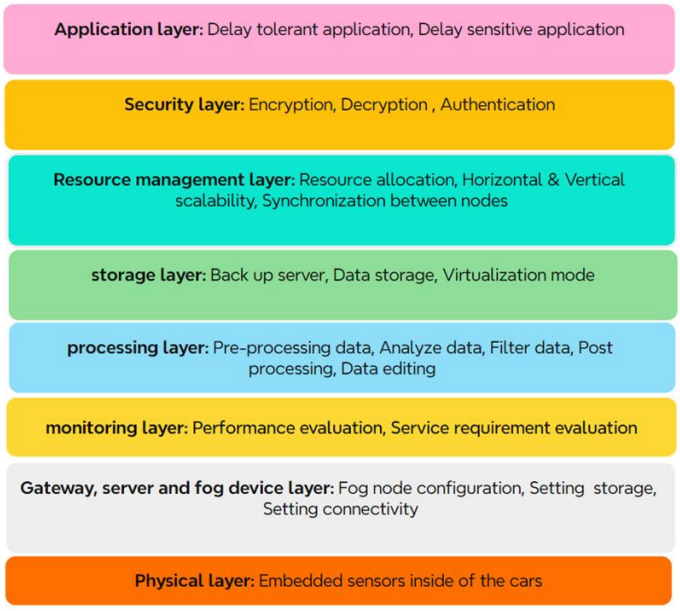

Figure 5: Fog Architecture Layers [34].

3.3 Communication of VANET Enabled by FC

New advancements in IT, such as 5G (5th generation), Wi-Fi, and citizen broadband radio service (CBRS), are satisfying the connectivity needs of FC components that VANETs enable. Now in the works is the deployment of 5G computer networks, which may boost device service speeds to 10-100 Gb/s[25,54].VANETs may be connected to the Internet to enhance travel experiences by offering file downloads and access to social media. Beacon and protection messages are two types of communications utilized in VANETs. Automobiles utilize beacons at 100 ms intervals to convey and announce status alterations to nearby cars. The transmitter broadcasts beacon signals to adjacent vehicles to provide its speed, location, and pseudo-identifier[55,56].

When a vehicle encounters an issue on the road, it broadcasts a Wave Short Message (WSM) to other vehicles. The message payload comprises the vehicle's direction, the timestamp of the message, the vehicle's location, and adjacent road occurrences. Every vehicle in a locality gathers information on the automobiles within its proximity. The vehicles' OBUs are outfitted with IEEE 802.11p and long-term evolution (LTE) cellular technology within heterogeneous VANETs[40,55,56].

The RSUs and OBUs might be designed to function as Fog Computing nodes for data analytics at the network edge. The Fog Hierarchical Deployment Model from the Open Fog Reference Architecture serves as a reference guide, wherein the Mobile Fog Nodes (OBUs) function as advanced applications that primarily collect data from other nodes within the IoT platform. The Static Fog Nodes (RSUs) have two categories of software components: RSU Applications and RSU Service, each with a specific function as outlined below[57]:

1. RSU Applications are containerized programs designed for specialized functions and capable of distribution. They can, for instance, identify traffic abnormalities using local data or gather, analyze, and disseminate information concerning mobility among various nodes.
2. The RSU Service is our fundamental management service. It can be utilized for discovery, lifecycle management, security, or other service implementations.

The fog nodes employed, rather than RSUs, are dispersed along the route. This is mostly due to the superior processing capabilities of the fog nodes compared to the RSUs, which diminishes latency and enhances throughput, as illustrated in Figure 6 [58,55].

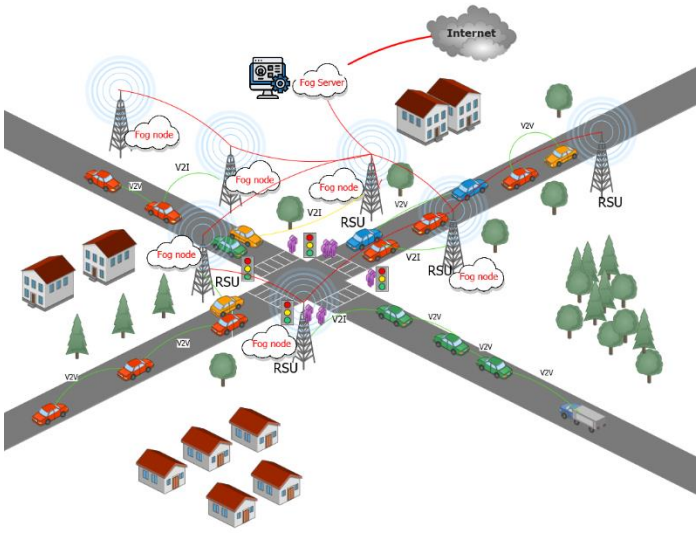

Figure 6: Fog–Based on VANET communication architecture.

Fog facilitates processing, communication, and storage functions. Its proximity to end consumers allows it to deliver services to the system's edge devices. Moreover, it distinguishes itself from other computer models through many features[59]. The main characteristics of fog computing encompass the variety of fog nodes and networks, the extensive size of geo-distributed nodes,

position awareness, the necessity for mobility support, and low latency [51,60,61].

- **Low latency:** This denotes the least duration required to reply, analyze, and execute the computational request. The closeness of fog nodes to edge devices facilitates expedited computation activities and analytical answers[51,59,61].
- **Heterogeneous end-user support:** End-user support is optimized when the requesting IoT device is in proximity to the processing node[51,61].
- **Multi-tenancy:** Denotes the capability of a system wherein several instances access and share a singular instance of the program. These systems are designated as shared systems. The fog platform adopted this because of its dispersed and highly virtualized nature[51,61].
- **Mobility support:** It is a feature that facilitates the registration and deregistration of IoT devices between access points. Mobility support is crucial for mobile IoT systems, as missing or delayed data during device movement can be detrimental. Therefore, it necessitates direct communication between the fog node and the IoT device[51,59,61].
- **Real-time interaction:** Real-time denotes a system that must reply within a designated time range (deadline). This category of applications in fog computing encompasses real-time e-health, traffic transmission, airline operations, and essential industrial process monitoring systems, among others. Furthermore, to ensure quality of service (QoS), fog computing prioritizes real-time transmission over batch processing[51,59,61].
- **Context-awareness:** This function enables fog nodes to acquire knowledge about their networks by retrieving information, facilitating the node's decision-making process[51].
- **Wide geographical distribution:** The architectural architecture of fog computing endows the paradigm with extensive geographical dispersion to guarantee the supply of Quality of Service (QoS)[51,59,61].
- **Interoperability and federation:** Enhance transparency and interoperability in fog computing systems by implementing open standards, enabling third-party systems to execute models and processes via web service requests while simultaneously disseminating findings for utilization by other services[51,59,61].
- **Real-time analytics:** Fog computing's real-time analytics involves collecting, analyzing, and responding to data at the moment of its generation rather than postponing its transmission to a centralized location for processing. This is achieved by placing small, lightweight computing units nearer to the data source at the network's periphery rather than depending on a centralized data center [51,61].

3.5 Advantage of integrating Fog computing in VANET

Integrating fog computing with VANET will yield several benefits, including localized data processing, resource aggregation, cache management, load distribution, and enhanced latency. In fog computing-based VANETs, time-sensitive local data is analyzed using fog edge node technologies, reducing latency. Fog computing facilitates interactions amongst vehicle nodes, significantly enhancing their collaborative efficacy. In Fog computing, infrastructures or facilities providing resources for services at the network's edge are called fog nodes. Fog nodes can function as both Fog servers and Fog edge nodes. Fog servers have enhanced processing and storage capabilities, whereas fog edge nodes can interface with diverse tools, including distinct end devices requiring different protocols[58].

A primary benefit of VFN is its proximity to clients, leveraging optimal choices for vehicle collaboration in service delivery[13,36,52]. Many of the advantages are outlined below.

- **Traffic light systems:** Fog computing and vehicle networks have supplanted traditional physical traffic light systems with virtual traffic signal systems, which are more economical. Furthermore, fog computing facilitates the alleviation of traffic congestion by adjusting traffic signals according to real-time conditions or through vehicular communications that direct cars to less congested routes[51,59].
- **Context-Aware Content Delivery:** The acquisition of real-time data concerning traffic circumstances, vehicle behaviour, network integrity, and similar factors can be enhanced by VANET-enabled FC's FS. VANET, facilitated by FC, enhances content delivery according to user preferences[25,51,59].
- **Latency management:** Latency management pertains to the duration required to reply to, analyze, and execute a computational request. The closeness of fog nodes to edge devices facilitates expedited computational activities and analytical answers. All conceivable approaches must be utilized to mitigate latency, including monitoring and implementing network designs that can eliminate or compel delay reduction. Furthermore, establishing organized nodal collaboration can facilitate efficient latency management. The allocation of jobs and processing between the fog and clients is designed to minimize communication and computational delay[9,51].
- **Data management:** As the quantity of IoT nodes continues to rise, the volume of data is likewise escalating swiftly. This rendered cloud computing and earlier paradigms useless for optimal data management, hence making fog computing advantageous due to its proximity to edge devices[51].
- **Scalability:** It provides scalable solutions by allocating the computational load across several fog nodes, hence averting any one point of overload that may arise in centralized cloud architecture[25,62].
- **Response time:** The reaction time comprises the data delivery duration to and from edge servers, in addition to the processing time within the servers. In comparison to the cloud, the edge servers in VEC are closer to vehicle users. Consequently, the execution time is significantly

reduced, which is particularly advantageous for delay-sensitive applications, such as safety systems[25,63].

- **Energy efficiency:** The optimal utilization of energy is closely linked to the rapid advancement of smart vehicles, which has resulted in an exponential increase in car-related activities, including video streaming and driving. The power requirements of these applications are substantial. Electric cars can enhance these VANET-enabled FC applications by aggregating resources[25,63].
- **Bandwidth:** VANET facilitated by FC is situated considerably nearer to the remote cloud, leading to a marked decrease in bandwidth use during calculations at the network edge in contrast to the backhaul network[25,63].
- **Proximal Service:** Following the analysis of the supplied location and sensing data, VANET facilitated by FC may efficiently administer proximity services, encompassing the dissemination of an HD-Map. The outcome is an enhancement in service quality and the overall user experience across various applications[25].
- **Support for Mobility:** Fog nodes can keep service up even when cars are very mobile since they are adept at handling handoffs between nodes in a smooth manner [64,65].
- **Real-Time Traffic Management:** FC eliminates the lag time associated with CC by processing data locally at RSUs, allowing for real-time traffic analysis and management [41,66].
- **Localized Decision-Making:** FC facilitates localized decision-making essential for autonomous driving and cooperative vehicle behaviors, including platooning and collaborative collision avoidance[25,67].
- **Carpooling:** In the carpooling service, the driver can announce the vehicle's destination and route. To enable potential passengers traveling the same route as vehicles to locate available cars. The objective is to mitigate traffic congestion during peak hours, and car fog can be crucial in managing passenger requests[68,69].
- **Crime detection:** Detecting suspicious activity necessitates systems with substantial storage capacity and computational power. Fog infrastructure can facilitate the identification and examination of suspicious activities and criminal incidents in real-time. Fog computing, through the collection and analysis of substantial data, can deliver a suitable solution to this need with little latency. Consequently, the fog framework is employed for intelligent video surveillance to improve safety and crime prevention cost-effectively[70,71].
- **Emergency Message Dissemination:** The VFC technique is intended to process and disseminate emergency notifications effectively. The strategy carefully identifies fog nodes (vehicles equipped with computing resources) depending on their proximity and availability to the disaster site, hence minimizing delays and improving the overall efficacy of emergency message distribution[20,72].
- **Low Latency and Real-Time Processing:** A key advantage of FC is its capacity to diminish delay markedly. Processing data nearer to the source significantly enhances response times compared to transmitting data to a centralized cloud for processing. This is essential for applications necessitating real-time decision-making and actions, like automated industrial controls, real-time health monitoring systems, or instantaneous data processing for autonomous driving[25,73].

3.6 VANET Service Facilitated by Fog Computing

The subsequent are a few major tasks of the VANET facilitated by FC.

- **Service of Storage:** Automobiles require storage to operate several applications, some of which possess substantial storage demands or necessitate temporary backup. The VF server facilitated this operation by providing storage capacity for the end-user application to operate[5,25].
- **Service of Communication:** In emergencies, internet connectivity is paramount. To circumvent this, VANET-enabled FC provides connectivity via vehicular units, roadside micro base stations, and additional cars[5,25].
- **Service of Computation:** Unused automotive tools may be located in parking lots, along roads, and even within data centers. VANET-enabled FC capitalizes on this opportunity to execute large-scale activities and allocate resources[25].
- **Service of Infotainment and Information:** Besides providing entertainment services like gaming and content caching, VANET enabled by FC can also help convey emergency information. The quality of experience (QoE) for the end users is enhanced by the provision of several services[5,25].
- **Reduction in Processing Delays in Highway Scenario and Urban Scenarios:** The F-RouND framework markedly lowers data processing times. It employs fog computing to improve rogue node identification in VANETs. This framework utilizes the OBUs of all cars in the area, overcoming the shortcomings of earlier approaches that experienced significant processing delays and elevated false positive rates. Fog-IDS employs fog computing to detect rogue nodes utilizing cryptographic methods[74].
- **Resource Utilization:** Fog computing enables the exploitation of idle resources from both mobile and stationary vehicles for compute-intensive applications. This is especially advantageous for resource-constrained vehicles that can delegate their jobs to more proficient nodes, hence improving overall system efficiency[62].
- **Task Offloading:** vehicles may delegate computational duties to roadside units (RSUs) or other vehicles possessing fog computing capabilities. The offloading procedure is crucial when a vehicle does not possess adequate computational resources to perform its responsibilities autonomously[62].
- **Fault Tolerance:** The fog computing architecture improves the reliability of traffic light control systems by mitigating single-point failures. This is essential for preserving traffic flow and safety in urban settings[75].

- **Mobility of fog nodes:** Vehicle fog is a unique computing model that allows moving cars to function as fog nodes alongside stationary ones, allowing them to enter or exit the network at any time[71].
- **Enhanced Security:** Managing sensitive data locally within fog nodes can improve security and privacy by decreasing the volume of data transported over the internet, mitigating exposure to potential cyber threats. Local data processing enables organizations to adhere to data sovereignty and privacy requirements more efficiently by maintaining vital data within certain geographic or jurisdictional borders[5].

3.7 Fog Servers Security

Fog servers, which provide virtualized services and control across geographical regions, may be susceptible to assaults from both internal and external threats. These attacks may encompass man-in-the-middle (MiM) and distributed denial-of-service (DDoS) attacks, in addition to physical assaults resulting from inadequate or absent physical defenses. VFC (Virtual Field Communication) integrates diverse networking infrastructures, presenting security problems. Conventional assaults can be alleviated with the deployment of edge servers. However, DDoS attacks targeting core infrastructure may have little effect. Malicious actors can seize the communication network's control via traffic injection and eavesdropping assaults. Unauthorized gateways can potentially jeopardize the security of fog networks[9,41].

Due to the dynamic topology changes in VEC, vehicles may not fully trust each other. Meanwhile, when the same physical edge servers are allowed to be accessed by different vehicular users, there are issues of security and privacy without a strong protection mechanism[63].

4 Related works and case studies

This survey paper explores different concepts to provide optimized security challenges of Vehicular ad-hoc Networks, and different works in the past have been proposed to identify the potential approaches, use cases, architectures, and the huge benefits brought by the ITS environment in meeting the demands of vertical applications. A summary of existing Fog-based VANET is presented. Surveys focusing on the security of VNs. A detailed survey of different technologies that have been applied to improve security services in VANET and Fog computing environments was presented[15]. The author's in[76] are tackling several crucial inquiries and issues about the security of Vehicular Fog Computing (VFC) systems. They propose a comprehensive threat model that delineates 33 assaults classified into six stride categories: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. This systematic method aids in comprehending the diverse dangers encountered by VFC systems.

In addition to the[77] underscores the considerable security and privacy threats linked to VFC, especially arising from its implementation in open settings such as Vehicular Ad-hoc Networks (VANET). These settings are vulnerable to several threats that might undermine the system's integrity and the security of vehicle communications. Therefore, The [71] examine many security concerns that emerge in vehicular fog networks. Malicious individuals may submit fraudulent reports, resulting in confusion and suboptimal decision-making among users. These include impersonation and Sybil attacks when adversaries generate several identities to exploit the system. Fraudulent communication and message modification attacks entail transmitting erroneous information or altering messages as they traverse nodes, potentially undermining the integrity of the conveyed data. The fluidity of vehicular fog networks affects authentication procedures, as nodes often enter and exit the network. This may result in unauthorized access and exploitation of resources.

The[78] proposed two methodologies for detecting compromised nodes inside the VFC paradigm. The initial approach involves doing a forensic analysis of artifacts from fog nodes that have been identified as exhibiting questionable behavior. Another approach involves employing big data analytics and deep learning algorithms to analyze historical traffic data. Simulation results demonstrate that the analysis of real-time and historical traffic data may alleviate the node compromise attack. The[79] Developed an innovative, secure technique for vehicle-to-vehicle and vehicle-to-edge communications utilizing a probabilistic data structure. This technique not only safeguards communications but also identifies intrusive behaviors. However, its performance deteriorates when vehicle density escalates. In[80], a security protocol for VFC was proposed, emphasizing connection and dependability. A group signature is utilized to administer the vehicular fog group. The client vehicle can utilize group parameters to ascertain the public key of the server vehicle, thereby establishing a symmetric key for subsequent data transfer with the server vehicle.

Both[81] and[82] have suggested fog-based access control methods to facilitate data sharing and access, incorporating encryption and decryption procedures. These established fog-based methodologies have been designed to retrieve data and information resources from centralized settings. Nonetheless, current access control methodologies lack the true context awareness and robustness necessary for developing fog-based Context-Aware Access Control applications when retrieving data from various sources depending on pertinent contextual variables.

To provide effective data security for the data which is transmitted in the vehicular network? The[83] developed a security-oriented authentication paradigm for IoT devices in fog computing, mitigating vulnerabilities using a lightweight methodology, employing post-quantum cryptography, and assuring scalability; nonetheless, the packet loss remains significant. The[84] suggested an innovative cryptographic approach employing AES-GMAC and information dissemination across GF(2w) for safe data management in fog computing. It guarantees secrecy, integrity, and availability. The drawbacks include elevated power usage. Supporting multiple operations with integrity and efficiency based on the shortest integer solution

(SIS) problem[85] created a lattice-based incremental signature scheme for updated secure information transmission in fog computing networks. However, this scheme suffers from high packet loss. In[86] The author introduces LAMAS for fog computing, which primarily focuses on an intelligent mutual authentication mechanism. It guarantees reciprocal authentication, obscures user identity, facilitates effortless server integration, and exhibits enhanced efficiency.

Many of the technologies integrated in VANET the author in[87] are addressing the task of combining 5G technology with Vehicle-to-Everything (V2X) communications to improve vehicle safety, autonomy, and overall road safety. In addition the[88] Focus on addressing the ongoing issues of security, communication dependability, and technological limits in VANET to enhance the safety, efficiency, and effectiveness of intelligent transportation systems. VANET encounters security obstacles due to the growing frequency of cyber-attacks on intelligent vehicles.

Also, the[19] presents a detailed study of VANETs to provide a picture of particular VANETs, security, applications, networking, and challenges. The[44] This paper addresses the question of security challenges in VANETs and the importance of security in the development of VANET applications. It explores the architecture and workings of VANETs, emphasizing the significance of security as a crucial factor in the advancement of a robust VANET environment[42]. Public key cryptography is prioritized to address security problems in VANETs. However, the difficulties of providing certificates to vehicle owners and regularly upgrading them are emphasized, leading to worries about potential data leaks and security breaches. Indeed, Table 1 compares the existing reviews, case studies, and different technologies used to enhance the security of VANETs.

Table 1: Existing review papers in literature.

References	Domain	Contributions	Limitation
[1], 2021	VANET	The paper identifies four main types of authentication and privacy techniques: pseudonym-based, identity-based signature, hashed function-based, and group signature-based, each with its own strengths and weaknesses.	As VANET car numbers increase, security protocols become more complex due to scalability issues, potentially causing weaknesses as the network expands.
[22],2022	VANET	Researchers developed a novel algorithm to improve data processing and transmission efficiency in fog computing for smart city mobility, mitigating delays and latency.	The article focuses on latency reduction but neglects energy consumption, security, and communication costs in fog computing and vehicle networks, which are crucial for practical application.
[9],2022	VFC	The paper underscores the significance of security and privacy in Vehicle-Fog Computing (VFC), outlining the methods necessary for secure data exchange across cars. The emphasis on security is essential for establishing confidence in VFC systems and safeguarding user data.	VFC devices' resource constraints hinder traditional data security methods, necessitating a reduction in cryptographic algorithm complexity for smaller devices, potentially undermining security.
[14], 2021	VANET	The research examines security and privacy needs in Vehicular Ad-Hoc Networks, focusing on resilience against threats and assessing computation and communication costs using evaluation metrics.	The research primarily focuses on identity-based encryption, potentially overlooking other new cryptographic techniques that could offer additional security benefits in VANET contexts.
[15], 2020	VANET	The study proposes a comprehensive integration strategy combining Vehicular Ad hoc Networks, 5G technologies, and blockchain to enhance communication and data transfer among cars, thereby enhancing network reliability and protection.	While the blockchain offers a fault-tolerant mechanism, the efficacy of this attribute may diminish as the network expands. The study emphasizes that consensus methods, such as pBFT, may encounter difficulties in extensive implementations.
[19],2022	VANET	The paper emphasizes the need to guarantee the promptness and accuracy of message transmission in VANETs in order to uphold data security and privacy protection.	The paper may not provide a comprehensive analysis of all security threats for VANETs, as it does not cover specific security protocols or attacks that could enhance VANET security.
[20],2020	VANET	The study explores primary obstacles in distributing emergency messages within	The study lacks strategies to enhance security in emergency message

		VANETs, including broadcast storms, hidden node problems, and packet collisions, laying the groundwork for future research and enhancements.	dissemination systems within vehicular networks. It identifies several security limitations, including susceptibility to attacks, complexity resulting in security gaps, and the absence of robust security measures.
[32],2019	VANET	The important discoveries concerning trust models and the significance of privacy preservation in upcoming VANET applications push for the integration of simulation platforms to improve performance and security assessments.	The paper may not fully address emerging technologies like blockchain, AI, and machine learning in improving security, trust, and privacy in VANETs, but they offer innovative solutions.
[36],2022	V2X	The article explores the security concerns of autonomous vehicles, particularly in the context of 5G technology, and proposes alternative solutions to mitigate their vulnerability to external attacks.	AVs' lack of robust security features like authentication and encryption makes them vulnerable to attacks like DoS and replay, while their LiDAR and RADAR systems may not handle user and data authentication.
[42],2020	VANET	The significance of creating security mechanisms at distinct levels of the protocol stack is prioritized over building countermeasures against particular assaults. The objective of this technique is to improve the overall security of the network.	While this paper addresses numerous security measures created by researchers, it does not go into the scalability and adaptation of these strategies to different VANET setups and scenarios.
[44],2019	VANET	Explores the many categories of security assaults and obstacles encountered by VANETs, enhancing comprehension of the prevailing security concerns in-vehicle networks.	The study primarily analyzes security challenges in VANETs theoretically, highlighting main issues but not delving into specific technological solutions or countermeasures.
[45],2021	VANET	The paper provides a thorough analysis of the 5G architecture, focusing on its potential to address security issues in automotive networks and improve existing security solutions.	The study acknowledges the dynamic nature of security risks in 5G and vehicle networks but acknowledges the need for ongoing adaptation and enhancement of security measures.
[47],2019	VANET	The authors examine the security characteristics, prerequisites, and benchmarks for automotive networks. The authors uncover and expose the existing vulnerabilities in VANET security and emphasize the limitations of current security protocols.	The document criticizes VANET standards for not addressing all necessary security criteria, highlighting that cryptographic methods do not effectively combat cellular network assaults like IP spoofing and DDoS attacks.
[55],2022	VANET	The authors propose a systematic framework for enhancing and advancing VANETs, integrating big data and other technologies, for academics and developers.	The rapid expansion of vehicle edge networks has raised security concerns due to their adaptability and the significant challenge of authentication security.
[57],2019	VANET	The papers propose a hybrid VANET/Fog architecture for real-time data analytics, enhancing urban transportation by detecting traffic abnormalities, road works, and accidents, and providing timely information to users.	The hybrid VANET/Fog architecture, a decentralized model, presents security risks due to conflicting regulations, data interception, privacy concerns, and real-time data analytics interactions.
[58],2021	VANET	The authors aim to create a bilinear pairing-based message authentication mechanism to ensure the integrity of vehicle communications, thereby enhancing trust in the information transferred.	The study explores various attack types, but may not cover advanced ones. It also highlights scalability challenges and reduced communication and computing overhead in a network.

[76],2022	VFC	The paper categorizes attackers based on their abilities and motivations, distinguishing between aggressive and self-serving types, and emphasizing the importance of understanding these motivations for effective security solutions.	The study's literature review is based on existing scientific publications related to VFC, potentially limiting its scope due to the exclusion of broader research in related domains.
[77],2022	VFC	The paper presents various literature-based strategies for identifying and addressing harmful behaviors in Vehicle Freight Controllers (VFCs) to enhance the security architecture of vehicle networks.	The paper addresses security and privacy concerns in vehicular fog contexts, highlighting the lack of comprehensive tools for identifying and mitigating hostile activities in current studies.
[71],2019	VFC	The paper delineates the architectural, security, and privacy prerequisites pertinent to vehicle fog computing. It emphasizes the distinctive issues that emerge in this setting, differentiating them from those in conventional cloud computing and other network types.	The study addresses crowdsourcing assault hazards like impersonation and Sybil attacks but lacks comprehensive solutions or remedies to mitigate these vulnerabilities.
[87],2021	V2X	The study underscores the significance of establishing strong security measures to protect V2X communications by emphasizing possible security risks such as Man-in-the-Middle attacks, Denial of Service attacks, and data manipulation.	The study acknowledges security concerns but lacks a comprehensive analysis of V2X interactions' security methods, potentially hindering the understanding of effective system protection.
[88],2019	V2X	The paper emphasizes the need for a comprehensive strategy to protect the cyber security of ICVs, encompassing hardware, software, communication, and cloud requirements throughout the entire car ecosystem.	The article may not provide a comprehensive overview of all necessary security measures for VANETs or explore specific protocols or implementations for enhanced ICV security.
[48],2018	FC	The authors propose a novel approach using urban buses and fog computing technologies to enhance data collection efficiency and security in smart cities, thereby promoting intelligent city construction.	The research highlights the importance of WPA2 security procedures for data integrity and permission between sensing and fog levels but warns of potential weaknesses in sophisticated attackers and the need for HTTPS for data authorization.
[89],2019	VFNs	The study aims to enhance throughput, minimize latency, optimize load balancing, maximize availability, and ensure reliable performance by integrating fog computing with VANETs.	The paper lacks a comprehensive discussion on the potential problems and constraints of integrating fog computing with VANETs, suggesting a need for a more comprehensive understanding.
[90],2020	VANET	The study introduces a robust Intrusion Detection System (IDS) to effectively combat spoofing in connected EVs, enhancing the security of vehicle communications.	The study uses a probabilistic cross-layer Intrusion Detection System for spoofing in connected electric vehicles but lacks comprehensive cybersecurity solutions, scalability, and practical implementation issues.
[91],2019	VFC	The study evaluates the effectiveness of SDWN controller positioning in dynamic VANET contexts, considering factors like vehicular velocity, network latency, and computing burden.	VANET systems' volatile nature, characterized by rapid vehicle changes, may hinder efficient security protocols, potentially creating vulnerabilities for malicious actors.
[92],2021	VANET	An efficient Clique Searching based Scheduling (CSS) algorithm is developed for the SDN controller to facilitate coding decisions and give directives for collaborative data dissemination. A graph	The CSS algorithm's complexity study suggests scaling issues in extensive networks or high vehicle density. The assessment is limited to specific traffic

		transformation strategy is established to enable the search for viable solutions.	situations and timeframes, lacking a comprehensive benchmark.
[93],2022	VANET	The authors propose deep Q-learning, a method that uses deep neural networks to estimate Q-values, to improve the management of high-dimensional input data, and to enhance learning process stability.	The research highlights security deficiencies in VANETs, including vulnerability to attacks, authentication issues, node risks, inadequate access control, and insufficient detection systems, emphasizing the need for improved security.
[94],2019	VANET	The authors propose a lightweight intrusion detection system using a hybrid optimization algorithm and key distribution establishment to improve authentication and trustworthiness in VANET.	The paper emphasizes that the suggested approach may remain susceptible to undiscovered Denial of Service (DoS) and Smart and Normal Intrusions (SNI) assaults. This signifies that more inquiry is required to improve security protocols against such attacks.
[75],2018	VANET	The research proposes two methodologies to enhance traffic efficiency and protect security, and privacy, using the Computational Diffie-Hellman puzzle and hash collision problem, validated by traffic lights.	The paper's proposed intelligent traffic light management techniques, utilizing fog computing, face challenges in computational Diffie-Hellman and hash collision problems, and may struggle with vehicle validity validation under high vehicle density.
[95],2020	VFC	The proposed trust model employs fuzzy logic to evaluate the precision of event communication, considering sender credibility and expertise, and establishes trust value for automobiles.	The task mapping algorithm faces challenges in adapting to dynamic driving conditions, as it must constantly reevaluate and redistribute jobs based on vehicle progress and availability.
[96],2024	VFC	The authors developed a lightweight authentication technique for VANETs using Elliptic Curve Cryptography (ECC) and Fuzzy-Verifiers to enhance security in three-factor authenticated key agreement protocols.	The document focuses on secure communication between individual cars and fog nodes but neglects group communication, which is crucial for simultaneous communication across multiple vehicles, potentially limiting its usefulness in complex vehicle settings.

5 Security requirements in VANET

Efficient and dependable security procedures are necessary for the safety-related applications of VANET to minimize various assaults. The communications transmitted through these apps must remain unaltered, un-counterfeited, and unexploited by potential attackers, as any breach of these messages might result in life-threatening implications for both drivers and passengers. Only a limited number of studies in the literature specifically address the various security requirements of VANET. Table 3 provides a concise overview of the primary security needs in VANET and their effects on the network. Failure to meet these security criteria can result in many consequences, such as financial, operational, safety, and privacy problems[47].

Vehicles establish communication with one another and with roadside infrastructure via public networks. The information transferred among components of VANETs is vulnerable to security breaches. Hence, it is imperative to safeguard transferred information. The literature outlines the key security needs for vehicle communication, and further upon below[1]. Some security issues with VANETs are as follows.

- **Availability:** The primary problem of VANETs is the availability of the wireless channel for receiving vital communications from vehicles. If an intruder executes a Denial-of-Service Attack (DoS) to disrupt the traffic, it will prevent the transmission of essential information between vehicles, rendering them ineffective. Therefore, it is necessary to have a high level of accessibility for the wireless channel[1]. Providing network services in real-time is the main goal of VANET. It seems like the majority of attacks are aiming to disrupt the availability of resources. Therefore, we need to address the issue of defense against these kinds of assaults[97-99].
- **Data Integrity:** first thing, make sure the messages are getting to their intended destinations. There has to be a system in place to quickly identify and respond to security breaches, such as unauthorized changes made to the network[97]. Integrity is the second most crucial aspect of ensuring secure communication in VANETs. The integrity

of the sent information remains unchanged throughout the communication between automobiles and roadside infrastructure. Put simply, the message received is identical to the one sent by the sender. In the absence of a reliable integrity assurance method, significant repercussions can occur. Thus, guaranteeing integrity is of utmost importance[1,14,99].

Table 2: Security Requirements in VANET.

Security requirement	Communication Paradigm	Impact
Authentication	V2X	Operational, Privacy
Data Confidentiality and responsibility	In-vehicle, V2X	Financial, Privacy
Key distribution	V2I	Operational, Safety, Privacy
Trust management	V2V	Safety, Privacy
Misbehavior	V2V, V2I	Safety, Financial
Availability	V2X	Operational, Financial, Safety
Integrity	V2X	Operational, Financial, Safety
Access control	V2I, V2V	Financial, Safety, Operational
Privacy	V2V, V2P, V2C	Financial, Safety
Location privacy	V2V,V2C	Financial, Safety
Flexibility	V2I ,V2C	Operational, Safety

- **Authentication:** Authentication is the crucial element in ensuring a secure connection. Authentication is a crucial need in VANETs to ensure the security of communication between vehicles. Lack of a secure authentication method between VANET components can result in unauthorized individuals intercepting sent information, leading to potential damage[1,14,98,99].
- **Confidentiality:** Confidentiality is the fourth most significant aspect of security. Encrypting sensitive information is essential in some circumstances to safeguard it against unauthorized access. In VANETs, cars occasionally exchange confidential data, such as in military convoys. To ensure the confidentiality of the sensitive information, it must be transferred in an encrypted manner, hence preventing unauthorized individuals from comprehending the contents of the communications. Data encryption is unnecessary for non-sensitive messages due to the inefficient use of resources[1,98].
- **Non-repudiation:** non-repudiation is a crucial element of secure communication that offers proof of conversation between two parties. Two cars engage in communication and thereafter cannot refute the message that was conveyed between them[1,14,98].
- **Verification of data:** It is necessary to authenticate data sent between V2V, V2I, and I2V. So, Road Side Access Points (RSAP) and cars need to be alerted ahead of time so their identities can be randomly confirmed according to the standards[97-99].
- **Validation:** VANET needs to make sure that no unapproved cars or Road Side Access Points (RSAPs) may use their services. The ability of the network to trace the identification of the vehicle that transmits and receives communications is crucial[97,99].
- **Efficient:** VANET performance may be enhanced by cutting down on processing, delays, and unnecessary overhead[97-99].
- **Access Control:** The primary objective within the wireless channel is to determine the access level of various organizations. There needs to exist a system via which law enforcement agencies can withdraw malevolent cars from communication networks[1,98].
- **Physical Security:** Safeguarding cryptographic credentials from unwanted access is crucial. One way to accomplish this is by implementing tamper-resistant hardware in the vehicle's On-Board Unit (OBU)[1].
- **Forward Secrecy:** The cars in the new group are unable to decrypt communications sent by other members of the group using their key[1].
- **Backward Secrecy:** The departing cars are unable to decrypt communications sent by the newly joined group member using their encryption key[1].
- **Perfect Forward Secrecy:** If the system possesses perfect forward secrecy, it means that even if one of the long-term keys is compromised in the future, no one will be able to compromise the session key that is generated from a set of long-term keys[1].
- **Key Independence:** Backward and forward secrecy is the means via which key independence is attained[1].
- **Unforgeability:** The attacker cannot fake the signature on a message sent by a genuine member. An assailant can use the first message again and fabricate the signature[1].
- **Unlink ability:** The attacker cannot establish a connection between the signature on the message and the actual identification of the corresponding vehicle. The secret information about cars in VANET is concealed from others using the unlinkability characteristic[1].
- **Traceability and Revocation:** If any vehicle is discovered to be engaged in harmful conduct, a trusted authority can track down the true identity of the offending vehicle and subsequently remove it from the VANET[1,14,98].

6 Security Attacks in VANET and Fog-based VANET Environments

Various security assaults, including internal and external threats, target both vehicle terminals and fog nodes in a VANET-fog environment. These attacks can be classified as either active or passive assaults and countermeasures of each attack. Undermining system performance and compromising data integrity. The following are some documented assaults and their repercussions, and Table 3 provides a summary of the VANET and Fog-based VANET attack categorization based on the two factors mentioned above[25].

- **MitM Attack:** An assailant intercepts communication between cars and fog nodes, compromising data integrity and confidentiality to alter traffic flows using MitM assaults. It holds particular significance in a VANET-fog environment due to the sharing of private data among participants. Man-in-the-middle (MitM) attacks can be mitigated by the effective implementation of encryption and appropriate authentication protocols[25,29,77,96,100].
- **Denial of Service (DoS) Attack:** The objective of DoS attacks is to disrupt vehicular networks or fog nodes by inundating them with an excessive volume of requests, hence rendering the service inoperable. This may result in significant interruptions to communication and data processing in a VANET-fog context. Resource management and intrusion detection systems can mitigate this issue[25,29,30,100].
- **Eavesdropping Attack:** Eavesdropping is characterized as the unauthorized eavesdropping of lawful communication between cars and fog nodes, resulting in the potential disclosure of sensitive information, including location data. Utilizing secure communication routes and encryption is crucial in a VANET-fog environment to avert eavesdropping[25,59].
- **Sybil Attack:** In the VANET-fog environment, malevolent nodes may employ several identities to engage in actions that disrupt regular network operations, including erroneous routing decisions and network instability. Vehicle-to-vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications may be affected. It may be addressed by identity verification and digital certificates[25,29,30,59,101].
- **Message Tampering:** This enables an attacker to alter the substance of messages transmitted between nodes and fog nodes, resulting in the dissemination of incorrect or misleading information, which may lead to traffic issues and accidents. Message integrity verification and digital signatures can be utilized to safeguard against tampering[25,51,59].
- **GPS Spoofing:** Attackers may transmit counterfeit GPS signals to automobiles within a VANET-fog environment, leading to inaccurate vehicle positioning and probable navigation complications or collisions. This hazard can be mitigated by evaluating geographical signals (e.g., GPS) and employing redundant locating techniques[25,76,102].
- **Replay Attack:** This is an active attack characterized by the interception and retransmission of legitimate data, hence jeopardizing the recipient's trustworthiness. This may disrupt the synchronization between cars and fog nodes in a VANET-fog scenario. Replay attacks can be mitigated with the implementation of time-stamping and nonce values[25,29,76].
- **Black Hole Attack:** In the context of VANET, the spatial scalability of fog allows malevolent nodes to assert themselves as the optimal route to a target, compelling all other vehicles to transmit packets through them, which are then rejected, so breaking the communication pathway. Consequently, both safe routing protocols and detection techniques guarantee the identification and isolation of black hole assaults[25,102].
- **Wormhole Attack:** The wormhole attack entails an adversary transmitting messages between disparate segments of the network, replaying them, and causing confusion inside routing algorithms. This is disruptive in VANET-fog. Packet leads and geographic routing methodologies help mitigate wormhole assaults[25,43].
- **Jamming Attack:** For instance, assailants may emit disruptive signals between cars and fog nodes, thus obstructing the communication channel's service. Jamming attacks can be mitigated with the implementation of spread spectrum and frequency hopping, alongside the development of jamming detection algorithms[25,59,102].

Attacks Associated with Fog-based Vehicle Ad-hoc Networks. Fog-based VANETs inherit all the vulnerabilities of traditional VANETs while additionally presenting novel attack vectors due to the decentralized and resource-limited characteristics of fog nodes, the security issues encountered by FSs in the VANET-fog environment, and various remedies to alleviate these security concerns. Examples pertinent to Fog-based architectures include[25].

- **Compromised Node Attacks:** This is a risk as attackers may infiltrate fog nodes, therefore gaining unauthorized access to data. This may lead to the collapse of the entire VANET-fog ecosystem, as fog nodes are essential to information management and decision-making. Enhancements to FS security may be achieved by stringent access restrictions, automated intrusion detection systems, and regular security audits[25,68,76,77].
- **DoS attacks on fog Nodes:** May target fog nodes to disrupt the functionality of vehicular networks by preventing them from processing and responding to request traffic. In a VANET-fog scenario, this may result in significant service interruptions. We may implement a system that manages addition and resource allocation, using redundancy to ensure that if one server fails, another can assume its responsibilities[25,77].
- **Data Integrity Attacks:** Any modification of data stored or executed on fog nodes impacts the integrity of the whole VANET-fog system. This may also enhance data integrity; hence, using cryptographic techniques and regular integrity verification is fundamental, and the countermeasure guarantees data integrity using cryptographic methods and routine integrity assessments[25,103].

Table 3: VANET and Fog-Based VANET Attack Classifications.

Type of Attack	attackers from inside or outside	Impact of the Attack	countermeasures
Man-in-middle Attack (MitM)	Outside /Inside Attack	Passive	Encryption and authentication protocols.
DoS Attack	Inside Attack	Active	Resource management, intrusion detection systems.
Eavesdropping Attack	Outside Attack	Passive	Encryption, secure communication channels.
Sybil Attack	Inside Attack	Active	Identity verification, digital certificates.
Message tampering Attack	Inside Attack	Active	Message integrity checks, digital signatures.
GPS spoofing Attack	Outside Attack	Active	GPS signal verification, redundant positioning systems.
Replay Attack	Outside / Inside Attack	Active	Time-stamping, nonce values.
Black hole Attack	Outside Attack	Active	Secure routing protocols, detection and isolation.
Wormhole Attack	Outside / Inside Attack	Active	Packet leashes, geographical routing.
jamming Attack	Outside Attack	Active	Spread spectrum, frequency hop- ping, jamming detection.
Compromised Node Attacks	Outside /Inside Attack	Active	Strong access controls, regular security audits, intrusion detection systems.
DoS attacks on fog Node	Inside Attack	Active	Resource management, redundancy.
Data Integrity Attacks	Outside /Inside Attack	Active	Cryptographic techniques, regular integrity checks.

Vehicular Ad-hoc Network (VANET) is a potential technology for traffic control, enhancing road safety, and providing entertainment systems. The implementation of VANET necessitates establishing confidence among vehicle owners. Trust must be established to engage car owners in the vehicular network; without their active involvement, VANETs cannot be fully realized. Consequently, ensuring security has emerged as a critical concern in VANETs[42]. New technologies, such as fog computing (FC), are necessary to address specific needs like security, resource management, and heterogeneity in vehicular ad-hoc networks (VANET). FC provides computational and storage capabilities at the vehicle's edge, allowing the execution of resource-intensive applications in smart cars while adhering to stringent latency constraints[22,41]. The analysis distinguishes between attacks occurring in a VANET environment and those in a Fog-based VANET environment, emphasizing their distinctions and presenting particular mitigation solutions in Table 4.

Table 4: VANET and Fog-Based VANET Compression based on Impact and Mitigation Strategy.

References	Attack Types	VANET	Fog-based VANET	Impact on Fog-based VANETs	Mitigation Strategy
[25,28,29,41,76,77,100]	Denial of Service (DoS)	✓	✓	A fog node has limited resources, rendering it susceptible to localized denial-of-service attacks that can interrupt real-time services.	Implement rate limiting, traffic filtering, decentralized fog node administration, and redundancy protocols to manage failovers.
[9,25,51,76]	Eavesdropping	✓	✓	Fog nodes locally handle sensitive vehicular data, hence increasing the vulnerability of this data to	Safe routing, data obfuscation, and end-to-end encryption (TLS, IPsec). Connect vehicles to fog nodes

				interception by attackers targeting connections between cars and fog nodes.	securely by utilizing virtual private networks (VPNs).
[29,76,102]	Replay Attack	✓	✓	Fog-based systems may be vulnerable due to its decentralized architecture, wherein local data storage and processing facilitate the potential for replaying outdated messages.	Utilize timestamps, sequence numbers, and nonce-based authentication mechanisms to identify and prevent replayed data.
[28,29,59,76,101]	Sybil Attack	✓	✓	Fog nodes overseeing vehicle clusters may be vulnerable to Sybil attacks, resulting in erroneous routing and resource distribution within the fog framework.	Employ public key infrastructure (PKI), identity-based cryptography, and consensus mechanisms to verify node authenticity.
[43,97]	Wormhole Attack	✓	×	Less prevalent in fog-based VANETs due to limited communication ranges and the localized data processing at fog nodes.	Risk can be reduced in conventional VANETs by using geographic routing, verifying packet timing, and distance-based routing protocols.
[42,59,76]	Resource Exhaustion	×	✓	Attacks that drain fog nodes' CPU, memory, or bandwidth might cause service degradation or system breakdown if the nodes aren't careful.	Utilize resource monitoring tools, dynamic load balancing, rate limitation, and fog node coordination to optimize resource allocation effectively.
[9,30,76,77]	Distributed Denial of Service (DDoS)	×	✓	Fog nodes are especially susceptible to DDoS assaults due to their role as intermediary processing units for several vehicles, and their constrained resources render them easy targets.	Avoid or lessen the impact of distributed denial of service attacks by making use of traffic analysis, fog node cooperation, distributed load balancing, and dynamic resource scaling in your network.
[9,68,96,100]	Man-in-the-Middle (MitM)	×	✓	Fog nodes, because to their closeness to automobiles, are susceptible to interception by attackers who manipulate communication between fog nodes and vehicles, hence jeopardizing data integrity and confidentiality.	Guarantee encryption across all communication tiers (vehicle-to-fog and fog-to-cloud), authenticate every node, and implement integrity tests, such as hash functions, to verify message authenticity.
[25,103]	Data Integrity Attack	✓	✓	Fog nodes may locally process faulty or altered data, thereby compromising decision-making and resulting in dangerous vehicle operations.	Implement hash-based integrity verification, utilize blockchain for immutable data storage, and adopt message authentication codes (MACs).
[59,76,100]	Data Privacy Leak	×	✓	Fog nodes, being in proximity to end users and cars, heighten the danger of privacy breaches resulting	Execute data confidentiality, enforce stringent access control measures, utilize encrypted storage, and adopt

				from inadequate data management or insufficient encryption.	decentralized privacy-preserving techniques.
[25,59]	Compromised Node Attack	×	✓	Malefactors may infiltrate fog nodes, seizing control of the data they handle, resulting in unauthorized access, data manipulation, or network interruption.	Implement secure boot, hardware-based trust modules (TPMs), routine node audits, and multi-factor authentication to safeguard fog nodes against compromise.
[25,59,76]	Jamming Attack	✓	×	Both VANETs and Fog-based VANETs are susceptible to jamming, wherein adversaries interfere with wireless transmission, especially at RSUs or fog nodes.	Utilize spread-spectrum methodologies, frequency hopping, and adaptive communication methods to circumvent damaged frequencies.
[1,28,43,81,104]	Side-channel Attack	×	✓	Fog nodes, owing to their local processing capabilities, may be susceptible to side-channel attacks that use physical attributes like as timing, power consumption, or electromagnetic emissions.	Employ noise injection, include randomization in cryptographic functions, and segregate essential activities within secure contexts.
[76,97]	Routing Attacks	✓	✓	Routing attacks, including black-hole and grey-hole attacks, impede message transmission in both VANETs and Fog-based VANETs, resulting in the redirection or loss of crucial data.	To avoid malicious route manipulation, take use of secure routing protocols, multi-path routing, and trust-based route selection.

Conclusion

This study comprehensively explores security challenges and advancements in fog-enabled Vehicular Ad Hoc Networks (VANETs), emphasizing the integration of Fog Computing (FC) to address privacy, security, and operational challenges inherent in VANETs. By proposing a novel taxonomy, the paper classifies threats, attack vectors, and mitigation strategies, offering a structured framework for understanding and addressing vulnerabilities in fog-based VANET architectures. Key contributions include identifying methods for secure data sharing, real-time authentication, and localized threat mitigation, alongside evaluating emerging security frameworks. The findings highlight Fog Computing's potential to enhance VANET systems by enabling low-latency data processing, improving mobility support, and ensuring localized privacy management. These advancements pave the way for scalable and secure ITS capable of real-time decision-making and robust communication. Practical implications include the development of more resilient architectures that address both current and emerging threats while ensuring compliance with privacy regulations and operational efficiency.

This paper provides valuable insights and actionable recommendations for researchers and practitioners aiming to develop next-generation VANET systems. Future work should focus on refining security mechanisms, exploring the integration of advanced technologies such as AI and blockchain, and addressing the scalability challenges associated with large-scale ITS deployments. While this study provides a solid foundation for understanding and addressing security challenges in fog-enabled VANETs, several avenues for future research remain open. One key area is the integration of advanced technologies, such as artificial intelligence (AI) and machine learning (ML), to develop adaptive security mechanisms capable of predicting and mitigating emerging threats in real time. AI-driven anomaly detection systems and ML-based threat classification models can significantly enhance the security and efficiency of VANETs.

Another promising direction is incorporating blockchain technology to strengthen trust management and data integrity across decentralized VANET environments. Blockchain can provide tamper-proof records for vehicle communications, but its integration poses challenges related to scalability, energy consumption, and latency that require further investigation. Moreover, future research should address scalability and

interoperability challenges in large-scale deployments, particularly in urban environments with high node density and diverse communication protocols. Exploring hybrid architectures that combine centralized and decentralized approaches could offer a balanced solution for managing resource allocation and network performance.

List of abbreviations

Abbreviations	Description	Abbreviations	Description
VANET	Vehicular Ad Hoc Networks	V2V	vehicle-to-vehicle
ITS	intelligent transportation systems	V2I	vehicle-to-infrastructure
RSUs	Roadside Units	V2X	Vehicle–to–everything
OBU	On-Board Unit	MANET	Mobile Ad hoc Network
DSRC	Dedicated Short-Range Communication	GPS	Global Positioning System
IOT	Internet of things	QoS	Quality of Service
FC	Fog Computing	UAVs	Unmanned Aerial cars

References

[1] Jan, S. A. *et al.* A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues. *IEEE Access* **9**, 153701–153726 (2021).

[2] Hidayathunisa, B. & Khader, A. S. A. AUGMENTING THE QUALITY OF EXPERIENCE IN 5G NEXT-GEN VANET ARCHITECTURE IN IOV FRAMEWORK. **09**, (2022).

[3] Xiao, K. *et al.* A Fog Computing Paradigm for Efficient Information Services in VANET. *IEEE Wirel. Commun. Netw. Conf. WCNC* **2019-April**, 1–7 (2019).

[4] Brennand, C. A. R. L. *et al.* Towards a fog-enabled intelligent transportation system to reduce traffic jam. *Sensors (Switzerland)* **19**, 1–29 (2019).

[5] Nazih, O., Benamar, N., Lamaazi, H. & Choaui, H. Toward Secure and Trustworthy Vehicular Fog Computing: A Survey. *IEEE Access* **12**, 35154–35171 (2024).

[6] Menon, V. G. & Prathap, J. Vehicular Fog Computing. *Int. J. Veh. Telemat. Infotain. Syst.* **1**, 15–23 (2017).

[7] Menon, A. *et al.* Measurement of wing deflections in flexible aircraft using the sansec smart sensor. *IEEE Aerosp. Electron. Syst. Mag.* **32**, 14–23 (2017).

[8] Thakur, A. & Malekian, R. Fog Computing for Detecting Vehicular Congestion, an Internet of Vehicles Based Approach: A Review. *IEEE Intell. Transp. Syst. Mag.* **11**, 8–16 (2019).

[9] Keshari, N., Singh, D. & Maurya, A. K. A survey on Vehicular Fog Computing: Current state-of-the-art and future directions. *Veh. Commun.* **38**, 100512 (2022).

[10] Din, S., Paul, A. & Rehman, A. 5G-enabled Hierarchical architecture for software-defined intelligent transportation system. *Comput. Networks* **150**, 81–89 (2019).

[11] Gaba, G. S., Kumar, G., Kim, T. H., Monga, H. & Kumar, P. Secure Device-to-Device communications for 5G enabled Internet of Things applications. *Comput. Commun.* **169**, 114–128 (2021).

[12] Amari, H., Houda, Z. A. El, Khoukhi, L. & Belguith, L. H. Trust Management in Vehicular Ad-Hoc Networks: Extensive Survey. *IEEE Access* **11**, 47659–47680 (2023).

[13] Aljeri, N. Efficient AI and Prediction Techniques for Smart 5G-enabled Vehicular Networks. (2020).

[14] Al-Shareeda, M. A., Anbar, M., Manickam, S., Khalil, A. & Hasbullah, I. H. Security and Privacy Schemes in Vehicular Ad-Hoc Network with Identity-Based Cryptography Approach: A Survey. *IEEE Access* **9**, 121522–121531 (2021).

[15] Arif, M. *et al.* Integration of 5G, VANETs and blockchain technology. *Proc. - 2020 IEEE 19th Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2020* 2007–2013 (2020) doi:10.1109/TrustCom50675.2020.00275.

[16] Hozouri, A., Mirzaei, A., RazaghZadeh, S. & Yousefi, D. An overview of VANET vehicular networks. (2023).

[17] Murtadha, M. K. & Mushgil, B. M. Flexible handover solution for vehicular ad-hoc networks based on software defined networking and fog computing. *Int. J. Electr. Comput. Eng.* **13**, 1570–1579 (2023).

[18] Noorani, N. & Seno, S. A. H. Routing in VANETs based on intersection using SDN and fog computing. *2018 8th Int. Conf. Comput. Knowl. Eng. ICCKE 2018* 339–344 (2018) doi:10.1109/ICCKE.2018.8566352.

[19] Hussein, N. H., Yaw, C. T., Koh, S. P., Tiong, S. K. & Chong, K. H. A Comprehensive Survey on Vehicular Networking: Communications, Applications, Challenges, and Upcoming Research Directions. *IEEE Access* **10**, 86127–86180 (2022).

[20] Ghazi, M. U., Khan Khattak, M. A., Shabir, B., Malik, A. W. & Sher Ramzan, M. Emergency Message Dissemination in Vehicular Networks: A Review. *IEEE Access* **8**, 38606–38621 (2020).

[21] Bhatia, J., Modi, Y., Tanwar, S. & Bhavsar, M. Software defined vehicular networks: A comprehensive review. *Int. J. Commun. Syst.* **32**, 1–22 (2019).

[22] Farooqi, A. M., Alam, M. A., Hassan, S. I. & Idrees, S. M. A Fog Computing Model for VANET to Reduce Latency and Delay Using 5G Network in Smart City Transportation. *Appl. Sci.* **12**, (2022).

[23] Ben Jaballah, W., Conti, M. & Lal, C. Security and design requirements for software-defined VANETs. *Comput. Networks* **169**, 107099 (2020).

[24] Boukerche, A. & De Grande, R. E. Vehicular cloud computing: Architectures, applications, and mobility. *Comput. Networks* **135**, 171–189 (2018).

[25] Al-Mekhlafi, Z. G. *et al.* Coherent Taxonomy of Vehicular Ad Hoc Networks (VANETs)-Enabled by Fog Computing: A Review. *IEEE Sens. J.* **24**, 29575–29602 (2024).

[26] Shafiq, H., Rehman, R. A. & Kim, B. Services and Security Threats in SDN Based VANETs : A Survey. **2018**, (2018).

[27] Zeadally, S., Javed, M. A. & Hamida, E. Ben. Vehicular Communications for ITS: Standardization and Challenges. *IEEE Commun. Stand. Mag.* **4**, 11–17 (2020).

[28] Urooj, S., Lata, S., Ahmad, S., Mehfuz, S. & Kalathil, S. Cryptographic Data Security for Reliable Wireless Sensor Network. *Alexandria Eng. J.* **72**, 37–50 (2023).

[29] Shawky, M. A., Bottarelli, M., Epiphaniou, G. & Karadimas, P. An Efficient Cross-Layer Authentication Scheme for Secure Communication in Vehicular Ad-Hoc Networks. *IEEE Trans. Veh. Technol.* **72**, 8738–8754 (2023).

[30] Al-Shareeda, M. A. & Manickam, S. A Systematic Literature Review on Security of Vehicular Ad-Hoc Network (VANET) Based on VEINS Framework. *IEEE Access* **11**, 46218–46228 (2023).

[31] Anjum, A. & Khan, A. A. Optimized Communication in 5G-Driven Vehicular Ad-hoc Networks (VANETs). (2019).

[32] Lu, Z., Qu, G. & Liu, Z. A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy. *IEEE Trans. Intell. Transp. Syst.* **20**, 760–776 (2019).

[33] Arif, M. *et al.* SDN based communications privacy-preserving architecture for VANETs using fog computing. *Veh. Commun.* **26**, 100265 (2020).

[34] Miri, F. & Pazzi, R. A Comprehensive Survey on the Convergence of Vehicular Social Networks and Fog Computing. (2021).

[35] Fraiji, Y., Ben Azzouz, L., Trojet, W. & Saidane, L. A. Cyber security issues of Internet of electric vehicles. *IEEE Wirel. Commun. Netw. Conf. WCNC* **2018-April**, 1–6 (2018).

[36] Hakak, S. *et al.* Autonomous vehicles in 5G and beyond: A survey. *Veh. Commun.* **39**, 1–34 (2022).

[37] He, Y. *et al.* D2D-V2X-SDN: Taxonomy and Architecture towards 5G Mobile Communication System. *IEEE Access* **9**, 155507–155525 (2021).

[38] Rocha, P. G., Souza, A., Silva, F. A. & Rego, P. A. L. Decision Algorithm for Computational Offloading in Vehicular Fog Computing with Pedestrians. *Proc. 2022 IEEE Conf. Cloud Netw. 2022, CloudNet 2022* 126–130 (2022) doi:10.1109/CloudNet55617.2022.9978821.

[39] Nkenyereye, L. *et al.* Software-defined network-based vehicular networks: A position paper on their modeling and implementation. *Sensors (Switzerland)* **19**, 1–14 (2019).

[40] Cardona, N., Coronado, E., Latre, S., Riggio, R. & Marquez-Barja, J. M. Software-Defined Vehicular Networking: Opportunities and Challenges. *IEEE Access* **8**, 219971–219995 (2020).

[41] Behravan, K., Farzaneh, N., Jahanshahi, M. & Hosseini Seno, S. A. A comprehensive survey on using fog computing in vehicular networks. *Veh. Commun.* **42**, 100604 (2023).

[42] Pavithra, T. & Nagabhushana, B. S. A Survey on Security in VANETs. *Proc. 2nd Int. Conf. Inven. Res. Comput. Appl. ICIRCA 2020* 881–889 (2020) doi:10.1109/ICIRCA48905.2020.9182823.

[43] Arif, M. *et al.* applied sciences and Challenges. *Appl. Sci.* **10**, (2020).

[44] Phull, N. & Singh, P. A review on security issues in VANETs. *Proc. 2019 6th Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2019* 1084–1088 (2019).

[45] Hussain, R., Hussain, F., Zeadally, S. & Lee, J. Y. On the Adequacy of 5G Security for Vehicular Ad Hoc Networks. *IEEE Commun. Stand. Mag.* **5**, 32–39 (2021).

[46] Waheed, A. *et al.* A Comprehensive Review of Computing Paradigms, Enabling Computation Offloading and Task Execution in Vehicular Networks. *IEEE Access* **10**, 3580–3600 (2022).

[47] Hussain, R. Integration of VANET and 5G Security: A review of design and implementation issues. *Futur. Gener. Comput. Syst.* **101**, 843–864 (2019).

[48] Cruz Caminha, P. H. *et al.* SensingBus: Using Bus Lines and Fog Computing for Smart Sensing the City. *IEEE Cloud Comput.* **5**, 58–69 (2018).

[49] Arif, M., Wang, G., Wang, T. & Peng, T. *SDN-based secure VANETs communication with fog computing*. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* vol. 11342 LNCS (Springer International Publishing, 2018).

[50] Mekki, T., Jabri, I., Rachedi, A. & Chaari, L. Software-defined networking in vehicular networks: A survey. *Trans. Emerg. Telecommun. Technol.* **33**, 1–29 (2021).

[51] Das, R. & Inuwa, M. M. A review on fog computing: Issues, characteristics, challenges, and potential applications. *Telemat. Informatics Reports* **10**, (2023).

[52] AB, A., NA, M. & AA, S. Fog Computing for Network Slicing in 5G Networks: An Overview. *J. Telecommun. Syst. Manag.* **07**, (2018).

[53] Renuka, K., Medikonda, PravJoshi, J. & Een. Secured and energy efficient data transmission in SDN-VANETs. *2018 22nd Int. Comput. Sci. Eng. Conf. ICSEC 2018* 1–4 (2018) doi:10.1109/ICSEC.2018.8712714.

[54] Meng, Y., Naeem, M. A., Almagrabi, A. O., Ali, R. & Kim, H. S. Advancing the state of the fog computing to enable 5g network technologies. *Sensors (Switzerland)* **20**, 1–26 (2020).

[55] Mahi, M. J. N. *et al.* A Review on VANET Research: Perspective of Recent Emerging Technologies. *IEEE Access* **10**, 65760–65783 (2022).

[56] Khan, A. A., Abolhasan, M. & Ni, W. 5G next generation VANETs using SDN and fog computing framework. *CCNC 2018 - 2018 15th IEEE Annu. Consum. Commun. Netw. Conf.* **2018-Janua**, 1–6 (2018).

[57] Pereira, J., Ricardo, L., Luís, M., Senna, C. & Sargento, S. Assessing the reliability of fog computing for smart mobility applications in VANETs. *Futur. Gener. Comput. Syst.* **94**, 317–332 (2019).

[58] Soleymani, S. A. *et al.* A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET. *Veh. Commun.* **29**, 100335 (2021).

[59] Ahammad, I. *Fog Computing Complete Review: Concepts, Trends, Architectures, Technologies, Simulators, Security Issues, Applications, and Open Research Fields*. *SN Computer Science* vol. 4 (Springer Nature Singapore, 2023).

[60] Zhi, Y., Fu, Z., Sun, X. & Yu, J. Security and Privacy Issues of UAV: A Survey. *Mob. Networks Appl.* **25**, 95–101 (2020).

[61] Anawar, M. R. *et al.* Fog Computing: An Overview of Big IoT Data Analytics. *Wirel. Commun. Mob. Comput.* **2018**, (2018).

[62] Hamdi, A. M. A., Hussain, F. K. & Hussain, O. K. Task offloading in vehicular fog computing: State-of-the-art and open issues. *Futur. Gener. Comput. Syst.* **133**, 201–212 (2022).

[63] Liu, L., Chen, C., Pei, Q., Maharjan, S. & Zhang, Y. Vehicular Edge Computing and Networking: A Survey. *Mob. Networks Appl.* **26**, 1145–1168 (2021).

[64] Ostrowski, K., Małecki, K., Dziurzański, P. & Singh, A. K. Mobility-aware fog computing in dynamic networks with mobile nodes: A survey. *J. Netw. Comput. Appl.* **219**, 103724 (2023).

[65] Lakhan, A., Ahmad, M., Bilal, M., Jolfaei, A. & Mehmood, R. M. Mobility Aware Blockchain Enabled Offloading and Scheduling in Vehicular Fog Cloud Computing. *IEEE Trans. Intell. Transp. Syst.* **22**, 4212–4223 (2021).

[66] Mao, W., Akgul, O. U., Cho, B., Xiao, Y. & Yla-Jaaski, A. On-Demand Vehicular Fog Computing for Beyond 5G Networks. *IEEE Trans. Veh. Technol.* **72**, 15237–15253 (2023).

[67] Hornik, J., Rachamim, M. & Graguer, S. Fog computing: a platform for big-data marketing analytics. *Front. Artif. Intell.* **6**, (2023).

[68] Hoque, M. A. & Hasan, R. Towards an Analysis of the Architecture, Security, and Privacy Issues in Vehicular Fog Computing. *Conf. Proc. - IEEE SOUTHEASTCON* **2019-April**, (2019).

[69] Li, M., Zhu, L. & Lin, X. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. *IEEE Internet Things J.* **6**, 4573–4584 (2019).

[70] Neto, A. J. V., Zhao, Z., Rodrigues, J. J. P. C., Camboim, H. B. & Braun, T. Fog-based crime-assistance in smart IoT transportation system. *IEEE Access* **6**, 11101–11111 (2018).

[71] Hoque, M. A. & Hasan, R. Towards an Analysis of the Architecture, Security, and Privacy Issues in Vehicular Fog Computing. *Conf. Proc. - IEEE SOUTHEASTCON* **2019-April**, 1–8 (2019).

[72] Ullah, A., Yaqoob, S., Imran, M. & Ning, H. Emergency Message Dissemination Schemes Based on Congestion Avoidance in VANET and Vehicular FoG Computing. *IEEE Access* **7**, 1570–1585 (2019).

[73] George, A. S. Partners Universal International Innovation Journal (PUIIJ) The Impact of IT / OT Convergence on Digital Transformation in Manufacturing Partners Universal International Innovation Journal (PUIIJ). 18–38 (2024) doi:10.5281/zenodo.10969999.

[74] Paranjothi, A. & Atiquzzaman, M. A statistical approach for enhancing security in VANETs with efficient rogue node detection using fog computing. *Digit. Commun. Networks* **8**, 814–824 (2022).

[75] Liu, J. *et al.* Secure intelligent traffic light control using fog computing. *Futur. Gener. Comput. Syst.* **78**, 817–824 (2018).

[76] Klein, T. *et al.* A Threat Model for Vehicular Fog Computing. *IEEE Access* **10**, 133256–133278 (2022).

[77] Nazih, O., Benamar, N., Lamaazi, H. & Chaoui, H. Challenges and future directions for security and privacy in vehicular fog computing. *2022 Int. Conf. Innov. Intell. Informatics, Comput. Technol. 3ICT 2022* 693–699 (2022) doi:10.1109/3ICT56508.2022.9990869.

[78] Huang, C., Lu, R. & Choo, K. K. R. Vehicular Fog Computing: Architecture, Use Case, and Security and Forensic Challenges. *IEEE Commun. Mag.* **55**, 105–111 (2017).

[79] Garg, S. *et al.* Edge Computing-Based Security Framework for Big Data Analytics in VANETs. *IEEE Netw.* **33**, 72–81 (2019).

[80] Yao, Y., Chang, X., Misic, J. & Misic, V. Reliable and Secure Vehicular Fog Service Provision. *IEEE Internet Things J.* **6**, 734–743 (2019).

[81] Yu, Z., Au, M. H., Xu, Q., Yang, R. & Han, J. Towards leakage-resilient fine-grained access control in fog computing. *Futur. Gener. Comput. Syst.* **78**, 763–777 (2018).

[82] Zhang, P., Chen, Z., Liu, J. K., Liang, K. & Liu, H. An efficient access control scheme with outsourcing capability and attribute update for fog computing. *Futur. Gener. Comput. Syst.* **78**, 753–762 (2018).

[83] Roy, K. S., Deb, S. & Kalita, H. K. A novel hybrid authentication protocol utilizing lattice-based cryptography for IoT devices in fog networks. *Digit. Commun. Networks* **10**, 989–1000 (2022).

[84] Vijayakumar, K., Suchitra, S. & Swathi Shri, P. A secured cloud storage auditing with empirical outsourcing of key updates. *Int. J. Reason. Intell. Syst.* **11**, 109–114 (2019).

[85] Wang, F., Wang, J. & Yang, W. Efficient incremental authentication for the updated data in fog computing. *Futur. Gener. Comput. Syst.* **114**, 130–137 (2021).

[86] Hamada, M., Salem, S. A. & Salem, F. M. LAMAS: Lightweight anonymous mutual authentication scheme for securing fog computing environments. *Ain Shams Eng. J.* **13**, 101752 (2022).

[87] Alalewi, A., Dayoub, I. & Cherkaoui, S. On 5G-V2X Use Cases and Enabling Technologies: A Comprehensive Survey. *IEEE Access* **9**, 107710–107737 (2021).

[88] Qiu, M. *Proceedings Smart Computing and Communication*. (2019). doi:10.1007/978-3-030-34139-8.

[89] Khattak, H. A., Islam, S. U., Din, I. U. & Guizani, M. Integrating Fog Computing with VANETs: A Consumer Perspective. *IEEE Commun. Stand. Mag.* **3**, 19–25 (2019).

[90] Kosmanos, D. *et al.* A novel Intrusion Detection System against spoofing attacks in connected Electric Vehicles. *Array* **5**, 100013 (2020).
[91] Khoury, J., Sami, H., Safa, H. & El-Hajj, W. On the use of software defined wireless network in vehicular fog computing environments. *2019 15th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2019* 1198–1203 (2019) doi:10.1109/IWCMC.2019.8766622.
[92] Liu, K. *et al.* Fog Computing Empowered Data Dissemination in Software Defined Heterogeneous VANETs. *IEEE Trans. Mob. Comput.* **20**, 3181–3193 (2021).
[93] Zhang, D., Yu, F. R., Yang, R. & Zhu, L. Software-Defined Vehicular Networks with Trust Management: A Deep Reinforcement Learning Approach. *IEEE Trans. Intell. Transp. Syst.* **23**, 1400–1414 (2022).
[94] Ioualalen, A. Fog computing. *Data Lakes* 171–186 (2020) doi:10.1002/9781119720430.ch8.
[95] Rahman, F. H., Shah Newaz, S. H., Au, T. W., Suhaili, W. S. & Lee, G. M. Off-Street Vehicular Fog for Catering Applications in 5G/B5G: A Trust-Based Task Mapping Solution and Open Research Issues. *IEEE Access* **8**, 117218–117235 (2020).
[96] Awais, S. M. *et al.* Provably secure fog-based authentication protocol for VANETs. *Comput. Networks* **246**, 110391 (2024).
[97] Tanwar, S., Vora, J., Tyagi, S., Kumar, N. & Obaidat, M. S. A systematic review on security issues in vehicular ad hoc network. *Secur. Priv.* **1**, 1–26 (2018).
[98] Hasrouny, H., Samhat, A. E., Bassil, C. & Laouiti, A. VANet security challenges and solutions: A survey. *Veh. Commun.* **7**, 7–20 (2017).
[99] Mahalakshmi, G., -, E. U., Science, N. S. and D. & 2020, undefined. Machine Learning based Feature Selection for Intrusion Detection System in VANET. *Researchgate.Net* (2021).
[100] Roman, R., Lopez, J. & Mambo, M. Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Futur. Gener. Comput. Syst.* **78**, 680–698 (2018).
[101] Benadla, S. & Merad-Boudia, O. R. The Impact of Sybil Attacks on Vehicular Fog Networks. *Proc. - 2021 IEEE Int. Conf. Recent Adv. Math. Informatics, ICRAMI 2021* 1–6 (2021) doi:10.1109/ICRAMI52622.2021.9585965.
[102] Zemmoudj, S., Bermad, N. & Bouallouche-Medjkoune, L. Detection and mitigation of vehicle platooning disruption attacks. *Veh. Commun.* **47**, 100765 (2024).
[103] Mao, Y., You, C., Zhang, J., Huang, K. & Letaief, K. B. A Survey on Mobile Edge Computing: The Communication Perspective. *IEEE Commun. Surv. Tutorials* **19**, 2322–2358 (2017).
[104] Alshudukhi, J. S., Mohammed, B. A. & Al-Mekhlafi, Z. G. An Efficient Conditional Privacy-Preserving Authentication Scheme for the Prevention of Side-Channel Attacks in Vehicular Ad Hoc Networks. *IEEE Access* **8**, 226624–226636 (2020).