IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 16 February 2024, accepted 26 February 2024, date of publication 4 March 2024, date of current version 11 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3371488

SURVEY

Toward Secure and Trustworthy Vehicular Fog Computing: A Survey

OSSAMA NAZIH[1], NABIL BENAMAR[2,3], HANANE LAMAAZI[4], AND HABIBA CHAOUI[1]

[1]National School of Applied Sciences, Ibn Tofail University, Kenitra 14000, Morocco
[2]Moulay Ismail University of Meknes, Meknes 50000, Morocco
[3]School of Science and Engineering, Al Akhawayn University in Ifrane, Ifrane 53000, Morocco
[4]College of Information Technology, United Arab Emirates University, Al Ain, United Arab Emirates

Corresponding author: Ossama Nazih (nazih.ossama@uit.ac.ma)

ABSTRACT The integration of fog computing in vehicular networks has led to significant advancements in road safety, traffic control, entertainment, and comfort services. Vehicular Fog Computing (VFC) emerges as an optimistic solution, offering a pathway to responsive service requests. VFC uses either onboard vehicle computers or vehicles as fog infrastructure between the underlying networks and the cloud, addressing the limitations of centralized data processing in traditional cloud computing. However, VFC faces security vulnerabilities due to the open nature of its deployment. In this survey, we explore the security threats confronting VFC and review existing solutions related to their detection and mitigation capabilities. This paper provides a comprehensive overview of the foundational concept of Fog Computing, VFC architectures, and their critical role in various intelligent computing applications. Moreover, it spotlights the trust and security concerns in deploying VFC and real-time big data analytics within the vehicular environment. This survey identifies pressing issues and outlines potential research directions, offering insights for the research community to address while designing secure VFC architectures.

INDEX TERMS Security, trust, vehicular cloud computing, vehicular fog computing.

I. INTRODUCTION

There is an increasing need for processing and communication resources due to the rapid development of vehicular applications [1]. Therefore, building and deploying rapid and effective solutions for heterogeneous environments is crucial. Similarly, academic and industrial researchers have focused on vehicular ad hoc networks (VANETs) to enhance traffic flow, drastically reduce car accidents, and ensure a safe trip. Dedicated Short-Range Communication (DSRC) allows for single-hop and multi-hop communications between smart vehicles and roadside infrastructure while allowing unrestricted movement on the road. The three primary methods of connection among automobiles in a Vehicular Ad-hoc Network (VANET) are vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and hybrid communication [2]. These connection methods faced many challenges, including Vehicle mobility, limited transmission range, frequently shifting topology, and scalability.

One of the effective solutions to these challenges was the deployment of centralized platforms such as cloud computing with VANET to ensure continuous communication among vehicles while improving their QoS. Vehicular Cloud Computing (VCC) platform helps vehicles communicate, perform complex computations, and share information and communication resources [3]. VCC helps drivers predict traffic, plan the best routes, and improve traffic conditions [4], [5].

Furthermore, it improves the autonomous and intelligent control of vehicles. It reduces the driver's workload to the greatest extent possible while offering passengers a more pleasant trip experience. However, being a centralized paradigm, VCC has several drawbacks. During communication, a large amount of data is transferred to the cloud, requiring a high transmission, processing, and response time suitable for delay-sensitive and real-time applications, especially in mobile environments [6], [7].

To overcome the shortcomings of the centralized platform, opting for distributed solutions was necessary. Fog Computing was proposed as a paradigm that will overcome

The associate editor coordinating the review of this manuscript and approving it for publication was Huan Zhou.

central cloud computing issues [8], [9]. Indeed, the Open Fog Consortium, which has lately issued a few white papers (e.g., [10]), is currently promoting it. A fog is a ''cloud located near the end devices.'' It is a distinctive distributed design that extends the network edge of the usual cloud computing architecture. Fog can process some application components, such as latency-sensitive, delay-tolerant, and computationally intensive applications that can be processed on the network edge and the cloud server. In this regard, a research paper proposes utilizing reverse auctions for efficient resource allocation in mobile cloud-edge. This approach optimizes task offloading, directing computations to the most suitable and cost-effective resources. It enhances edge computing by reducing reliance on centralized servers, ensuring lower latency, and efficiently utilizing vehicular resources. The result is improved overall efficiency and responsiveness in the computing ecosystem [11]. Fog computing provides a reliable, safe, and valuable computing environment that has the potential to transform our driving styles [12]. It enables the efficient use of VANET performance and the support of features required in various real-time applications, such as low latency and high computational capability [13]. It extends VCC features to the network's edge while handling the increasing need for storage, processing, and communication resources [14].

The main goal of this paper is to provide an in-depth overview of the VFC paradigm. It presents the main architecture, possible scenarios, applications, and services. Also, it explores the main challenges in terms of trust, privacy, security, and cyber threats. The paper focuses on existing and emerging concepts such as game theory and artificial intelligence (AI) used to resolve some of the security and privacy solutions. Also, it provides insights into future directions and open challenges to improve VFC systems.

Abbreviations and acronyms for the main terms used in this paper are illustrated in table 1.

TABLE 1. List of abbreviations.

Acronym	Description
VCC	Vehicular cloud computing
VFC	Vehicular Fog computing
FC	Fog Computing
IoT	Internet of Things
DSRC	Dedicated Short-Range Communication
VANET	Vehicular Ad-Hoc Network
RSU	Roadside unit
V2V	Vehicle-to-Vehicle
V2I	vehicle-to-infrastructure
QoS	Quality of Service
LBS	Location-based Service
NaaS	Network as a service
STaaS	Storage as a service
CaaS	Computing as a service
ENaaS	Entertainment as a service
INaaS	Information as a service

A. RELATED SURVEYS

VFC interested several researchers from different fields, who explored the main functionalities and characteristics of fog computing and how their integration into vehicular networks could improve its performance and services through extensive literature reviews. Authors in [15] covered the operational aspects of smart vehicles, vehicular communications, and computational power, focusing less on security and privacy concerns. However, authors in [16] offered an outline of architecture, prospective VFC use cases, and security and privacy issues without providing techniques for identifying and preventing harmful behavior in a VFC. In addition, three main aspects of VFC were emphasized in [17]: VFC design, security, and privacy. Based on the authors' study, there are three categories of research focus: resource allocation, data dissemination, and crowdsourcing. This study also evaluated other metrics, such as latency, QoS, mobility, confidentiality, integrity, non-repudiation, privacy, and location verification. In contrast, there is no focus on solutions based on game theory and emergent technology, such as AI, used to secure the VFC systems.

Table 2 wraps up the existing related surveys discussed in this section.

The surveys, as mentioned earlier, provide a general summary of VFC. They primarily analyze the various architectural approaches to creating a VFC network, the VFC application domain, and associated technological difficulties. On the other hand, the current study proposes a detailed literature analysis that mainly focuses on trust, privacy, and security in VFC networks. It also describes the various methods and improvements suggested in the literature for identifying and preventing harmful actions that damage communication and computation.

B. THE SCOPE OF THIS SURVEY

This paper presents a systematic and comprehensive review of the research studies interested in VFC, with a limited focus on security threats in VFC systems. We investigated the different application domains and possible deployment scenarios. We also discussed the research effort proposed to secure the VFC systems using AI and game theory solutions and highlighted some open research directions.

The main contribution of this paper is summarized as follows:

- Provide a deep study of VFC systems, including VFC architecture, possible scenarios, applications, and services.
- Shed spot on main challenges of VFC in terms of trust, privacy, security, and cyber threats.
- Explore existing and emerging techniques such as game theory and AI used to provide security solutions for VFC.

TABLE 2. Related surveys comparison.

Ref	Scope	Topics					Contribution	Drawbacks	Year
		Architect. Design	Mobility	Security	Privacy	Detect. and Prev.			
[17]	VFC environment	✓	✓	✓	✗	✗	• VFC architecture • Security issues in VFC	• Security solutions in VFC	2019
[15]	VEC environment	✓	✗	✓	✓	✗	• V2V and V2I in VEC • Security and privacy in VEC	• VFC and VEC comparison • VEC security requirements	2019
[16]	Fog Computing in VANET	✓	✓	✓	✗	✗	• Connecting vehicles to VANET • Security and forensics requirements	• Vehicles as Fog nodes • Possible scenarios in VFC • Detection and prevention in VFC	2017
[18]	VFC application	✓	✓	✗	✗	✗	• VFC: Video crowdsourcing as a study case	• Security and privacy challenges • Countermeasures for mitigation in VFC	2018
[19]	Fog Computing in VANET	✗	✗	✓	✓	✗	• Integration of Fog Computing in VANET	• Deployment on vehicles as fog nodes • VFC applications	2017
[20]	VFC challenges	✓	✓	✓	✓	✗	• VFC taxonomy vehicles deployment in VFC	• VFC implementation requirements • Detection and prevention in VFC	2020
[21]	Dissemination of Data in VFC	✓	✗	✓	✗	✗	VCC vs VFC in: • Data Dissemination • Applications • Security threats	• Privacy issues in VFC • Misbehaving detection and prevention solutions	2021
[22]	VFC: implementation and open issues	✓	✓	✓	✗	✗	• Identifies challenges related to VFC: resource allocation, communication protocols, security, energy, and mobility. • Analyzes various task offloading techniques in VFC. • Evaluates strengths and limitations, considering suitability for different scenarios. • Provides insights for improvement and innovation in VFC.	Security and Privacy Concerns: • Briefly addresses, lacks depth. • Ignores privacy-preserving techniques Scalability of VFC: • Inadequate discussion on scalability. • Doesn't address challenges with increasing data volume.	2022
[23]	Task offloading in VFC	✓	✓	✓	✗	✗	• Addresses key challenges: resource allocation, security, energy, etc. • Introduces a structured framework for task offloading understanding. • evaluates techniques, strengths, and limitations for varied scenarios.	• Focused on task offloading; may miss broader insights from a wider scope. • May not include the latest advancements, potentially limiting relevance.	2022
Our survey	VFC: security and trust issues	✓	✓	✓	✓	✓	• VFC global architecture • VFC implementation • VFC scenarios • Security and privacy threats • Detection and prevention in VFC		

- Highlights some open challenges.

The rest of the paper is organized as follows. The concepts of VFC are introduced and described in Section II. Section III highlights the major trust and security concerns in the context of VFC. AI-based and Game theory approaches to secure VFC are presented in Section IV. Finally, section V concludes the paper by discussing open challenges and the future direction of VFC.

II. FROM FOG COMPUTING TO VFC

VFC represents a transformative shift from traditional cloud-centric approaches, extending Fog Computing principles to the vehicular domain. In VFC, parked vehicles serve as a static communication infrastructure, forming a geo-distributed backbone, while moving vehicles engage in dynamic communication models, facilitating both single-hop and multi-hop communication. The hierarchical VFC architecture encompasses layers from Smart Things to Cloud, optimizing resource utilization and supporting real-time applications. By leveraging parked vehicles for connectivity and computation clusters and utilizing moving vehicles for dynamic communication scenarios, VFC addresses challenges unique to vehicular environments, ushering in a paradigm that enhances vehicular communication and computation capabilities at the network's edge [24]. Several VFC assumptions have been proposed in the literature, including vehicular cloudlets (cloudlets transported by moving vehicles) [25], [26], [27], [28], [29]. Hou et al. [30]

provided an example of cloudlet deployment. The authors propose combining the idle computational capacity of nearby vehicles to form a small cloud known as a Jam-Cloud by converting vehicles–particularly parked and slowly moving ones–into cloudlets. In this method, vehicles are viewed as fog users and nodes with underutilized assets that can considerably boost fog resources and increase the probability of processing tasks at the network's edge.

This section highlights various VFC environment elements, including architecture, probable scenarios, applications, and services.

A. VFC ARCHITECTURE

A vast array of designs now illustrates the operations and services of the VFC systems. Indeed, most of these systems are based on the basic multi-layer Fog Computing framework described in [16], with cars acting as fog nodes. VFC extends cloud services to the network's edge by introducing a vehicular fog layer between end-user devices and the cloud layer. Using a decentralized design, VFC can ensure that the requested tasks are communicated with, controlled, stored, and computed at the network's edge. Figure 1 presents a thorough illustration of VFC networks. Mainly as it is shown in figure 2, we illustrate the VFC hierarchical architecture, which is composed of the following four layers:

1) SMART THINGS LAYER

It is the layer that is nearest to the end devices. It mostly consists of several smart things with different CPU types, memory, and operating systems. For instance, sensors, mobile phones, and vehicular smart sensing devices do not participate in vehicular Fog. They will be responsible for sensing and transmitting the gathered data to the upper layer for more processing and computing free spaces [25].

2) MULTI-SERVICE EDGE LAYER

This layer is placed on the network's edge, is multimodal, and supports many protocols, such as DSRC Roadside, Mobile WiFi Offload, Consumer Network, and Electrical Charging Network. The multi-service edge comprises many vehicles [31]: parked and moving vehicles. These vehicles are extensively dispersed between end devices and the cloud and are deployed in different places in the physical environment, such as shopping malls, streets, parks, etc. The end devices are connected to vehicles, benefiting from fog applications and services. These vehicles can accomplish real-time and delay-sensitive applications to transmit and store the received data. Furthermore, the vehicles are connected to the cloud via a core network, where more powerful computing and storage capabilities are achieved [32].

3) CORE NETWORK LAYER

The core network layer must be capable of processing, controlling, and managing huge volumes of network traffic. This layer is in charge of regulating end devices and keeping track of their IP addresses to unify the integration of several devices into a single cooperative network. Various technologies, including cable, wireless, and satellite, have aided this phenomenon. The traffic profile and data types are the major differences between vehicular Fog and conventional core networks [33].

4) CLOUD LAYER

In contrast to conventional VCC architecture, not all computing and storage tasks should be transmitted to the cloud. This layer comprises several powerful computing and storage servers used for heavy computation, analysis, and long-term storage of huge amounts of data. The cloud core modules are quickly planned and controlled based on demand to use the cloud resources effectively. Vehicle fog computing architecture consists of the combination of various network technologies in which end-devices or smart objects are connected to the fog vehicles using wireless access technologies (mainly including WIFI, 3G, 4G, 5G, ZigBee, Bluetooth, etc.) or wired connections [34]. However, fog vehicles are connected using other technologies such as DSRC Roadside, Mobile WIFI Offload, Consumer Network, and Electrical Charging Network, and then linked to cloud computing using an IP core network [35]. In a nutshell, this architecture serves latency-sensitive and real-time applications. It provides better computational and communication services in vehicular environments, such as enhanced route navigation, traffic lights, and optimal scheduling toward a safe road.

B. VFC POSSIBLE FORMATION SCENARIOS

In a VFC network, the vehicle can be mobile or static, creating two main scenarios affecting VFC operations. In the first scenario, the car moves from one place to a specific location. While in the second scenario, the vehicle is not in use and is parked somewhere. Both scenarios deploy specific communication and computation infrastructures that consider their requirements.

1) PARKED VEHICLES

In any urban area, a huge number of parked vehicles are widely geo-distributed on the parking lots (mainly street parking, underground parking, or garages). In this situation, exchanging information between vehicles is not possible due to the stable locations of vehicles over a long period [1].

However, using parked vehicles as a part of communication infrastructure improves connectivity elsewhere. With their features, parked vehicles can communicate with nearby moving vehicles and serve as a static backbone for the network. Integrating parked vehicles as a communication infrastructure can compensate for moving vehicles' disadvantages, such as changing positions and unbalanced space and time distribution. By that, parked vehicles' wide geo-distribution and long-term staying in a specific location can positively impact QoS in vehicular communications and improve the computation of complex tasks [30].

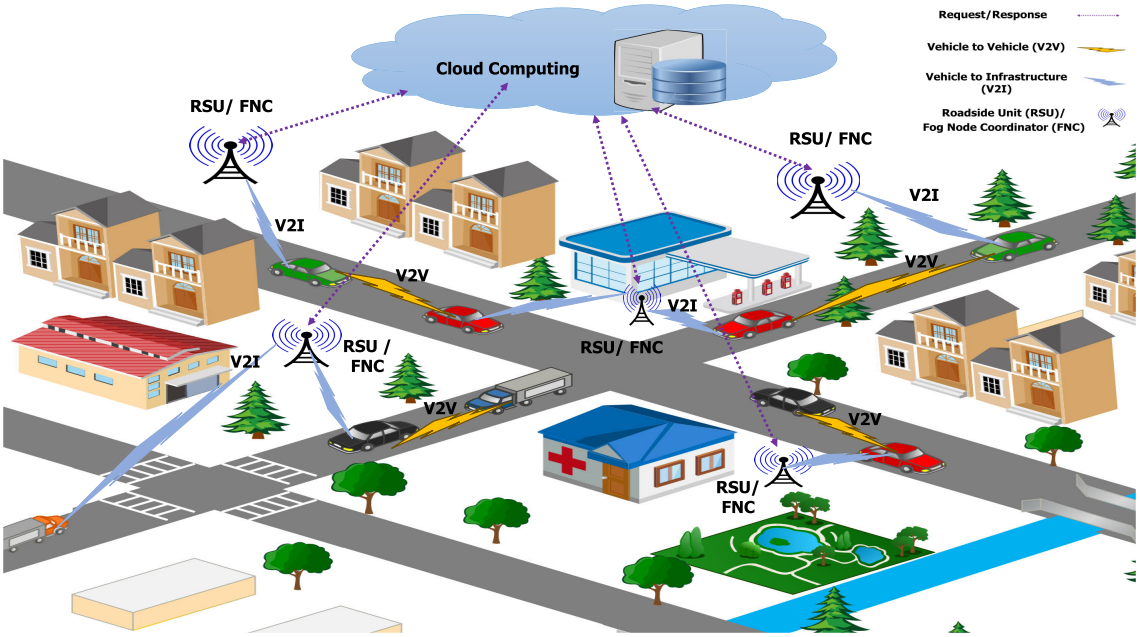


FIGURE 1. VFC global architecture.

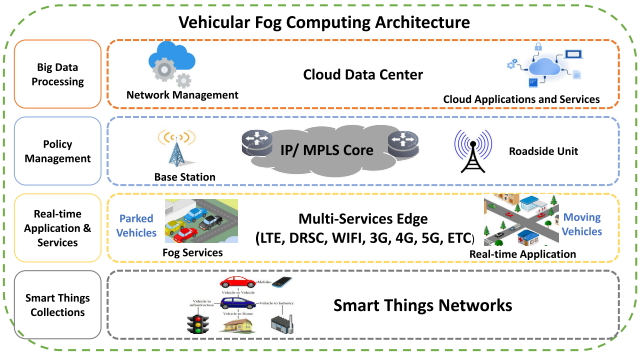


FIGURE 2. The hierarchical architecture of VFC.

As an individual computing resource, vehicles have a very limited computation capacity. VFC can provide powerful computation resources to achieve high computation tasks more efficiently and quickly so that the participating parked vehicles in VFC create small computer clusters and offer ample facilities for various complex computing tasks. Moreover, many realistic scenarios and practical approaches exploit parked vehicles as infrastructure [26], [36].

2) MOVING VEHICLES

Many research studies have been tuned to the VFC, focusing on solving communication and computing problems in a mobile environment where vehicles are deployed as infrastructure. In a moving scenario, we can distinguish two main communication models:

Single-hop communication refers to direct communication between a vehicle and a fixed infrastructure point or another vehicle within range. In an urban environment, single-hop communication can occur through various means such as WiFi, cellular networks, or DSRC systems. Single-hop communication is often used for immediate and local information exchange. For example, a vehicle may communicate with a nearby traffic light or a roadside unit to obtain information about traffic conditions, signal changes, or road hazards. Similarly, vehicles can directly communicate with each other for purposes like cooperative collision avoidance or sharing real-time traffic information [37], [38]. While multi-hop communication enables vehicles to relay messages over longer distances, single-hop communication is essential for immediate and localized information exchange. Both approaches complement each other and contribute to improving network connectivity in urban environments [39].

Authors in [30] take vehicles' VFC multi-hop characteristics and moving features to improve network connectivity. The link between mobility and connectivity in-vehicle networks may be differentiated using knowledge about vehicular speed distribution in space and time domains; this allows for a better awareness of urban communication situations. Moving vehicles were presented as one of the most essential message carriers to send information from one location to another via VFC geo-distribution and local decision-making. Vehicles can operate as communication hubs, linking nearby vehicles and connecting with even more mobile APs [40]. Communication hubs in VFC represent the backbone for sending information to cloud servers; these communication hubs are the main networking component that forms Fog Computing power. It achieves its goal by utilizing local computational and communication resources rather than sending all information to the cloud servers. It involves local decision-making and geo-distribution features, unlike the

VCC system, which needs to transmit a huge amount of data between mobile APs and remote servers. VFC shows higher efficiency, lesser delay, and lower cost when utilizing geo-related vehicles [40], [41]. Regarding computation, moving vehicles, particularly slow-moving vehicles, are an important solution to serve computation tasks in VFC temporarily. Vehicles jammed around an intersection of streets can also achieve tasks cooperatively by sharing their resources during their travels. In the case of infrastructure damage, vehicles can be connected through V2V communications [18], where integrating a remote cloud is unnecessary. Vehicles rely on their computing capabilities and create local mobile cloudlets to carry out computational tasks and satisfy the computation demands of individual vehicles. This paradigm turns the congestion situation into valuable and useful computational power. According to [3], the involving elements of the architectural support of this kind of VFC infrastructure can be processed in 3 steps, as follows:

1) Initially, a chosen vehicle will attempt to establish a VFC environment by getting initial authorization from the VFC trusted authority.
2) Following receipt of a successful authorization and the presence of a sufficient number of vehicles, the designated broker will ask the area-connected vehicles to establish a VFC.
3) Finally, computing resources will be pooled to form a vast VF computing entity resembling a conventional fog server. In this sort of moving vehicle situation, traffic lights must be rearranged across a wide area, and vehicles must be motivated utilizing game-based and AI-based incentive mechanisms to form numerous VCs [42], [43].

C. APPLICATIONS AND SERVICES

Drivers can access various real-time applications through the application and services layer, including fuel feedback, health detection, and environmental monitoring [44]. It provides the user with various services, including connectivity, information, data processing and storage, and entertainment. The several services that VFC offers are shown in figure 3.

1) NETWORK AS A SERVICE (NaaS)

The ability of vehicular fog nodes to connect to the cloud is their most striking characteristic. The vast majority of automobiles lack Internet access. Clients with Internet access might offer this service to other clients in need. Many underutilized resources, such as mobile device networks or other fixed infrastructure, can be shared on the road to provide Internet connectivity for interested individuals. Customers who agree to share their resources must publicize such information among existing nodes in nearby areas that can serve as Internet access points [45].

2) STORAGE AS A SERVICE (STaaS)

Due to limited capacity and high storage charges, many clients request additional storage resources. Vehicles with a significant storage capacity can offer storage as a service in VFC [46]. As a result, users can run programs that demand a significant amount of storage and use the additional terabytes of storage as a short-term backup, boosting the availability and dependability of data or peer-to-peer applications over time [47], [48].

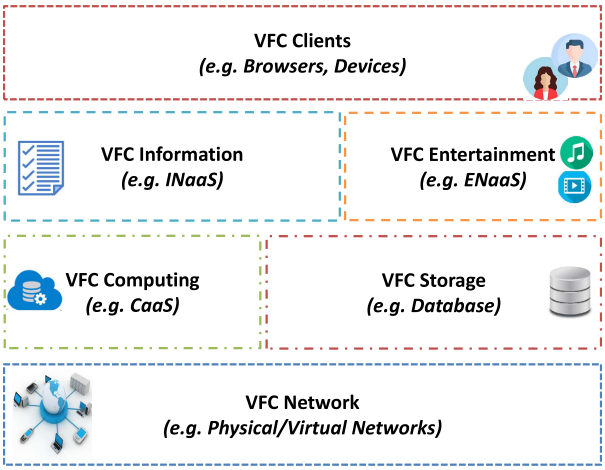


FIGURE 3. VFC applications and services.

3) COMPUTING AS A SERVICE (CaaS)

Most automobiles are stored in garages, parking lots, or driveways daily for several hours. The huge potential processing capability of these parked cars is underutilized. VFC allows clients who wish to improve the processing power of their devices and conduct enormous computing operations to gather the underused computing capabilities of parked vehicles as a new service [49].

4) INFORMATION AS A SERVICE (INaaS) AND ENTERTAINMENT AS A SERVICE (ENaaS)

A driver's choice may be influenced by the state of the roads, warning signs, and emergency information, to name a few [50]. IaaS offers this information type, which is mostly employed to guarantee safe automotive operation. To make users' days as delightful as possible, entertainment as a business offers them advertisements, films, and commercials [51].

III. TRUST AND SECURITY IN VFC

In the multifaceted domain of VFC, security considerations span various facets, from authentication and identity management to access control, trust management, policy integration, secure-service management, privacy, data protection, and organizational security management. Existing research categorizes security and trust issues in VFC into six fundamental requirements, providing a comprehensive framework to address vulnerabilities. Notably, trust emerges as a pivotal element in safeguarding VFC against malicious nodes and security risks, prompting the exploration of diverse trust models tailored to VFC's unique challenges.

Indeed, the deployment of the VFC system must examine various security challenges that it may meet to assure high-quality communication while maintaining an atmosphere of trust. This section will discuss the security issues related to VFC implementation and highlight mitigation solutions.

A. OVERVIEW OF THE EXISTING VFC WORKS

Computing technologies can be found in multi-domain settings, where each domain has its security, privacy, and trust requirements and the opportunity to use various interfaces, processes, and semantics. Security risks might be data-dependent, where malicious behavior is provided by malfunctioning sensors, or context-aware, where the external environment produces malicious behavior.

The current study's main goal is to explore the various security vulnerabilities in VFC domains while categorizing them into six major entities:

We classify security and trust issues of these researches into six requirements:

1) (R1): Authentication and Identity Management,
2) (R2): Access Control,
3) (R3): Trust Management and Policy Integration,
4) (R4): Secure-Service Management,
5) (R5): Privacy and Data Protection and
6) (R6): Organizational Security Management.

Many studies present strategies for securing VFC systems. According to Soleymani et al. [52], trust is critical to every security system. Thus, trust models can significantly prevent VFC against malicious nodes and other security risks. Furthermore, establishing trustworthiness in VANETs is crucial because a fog vehicle is regarded as the most important component. After all, it is responsible for maintaining end-user secrecy and anonymity. The collection of interactions between participants or nodes that make up trust in VFC Building trust inside the VFC is a challenging problem, though, as many VFC applications include multi-hop routing with several vehicles, RSUs, service providers, and communication channels. Trust models in VFC can be divided into three types [53]:

1) Vehicles or Entity-based trust models.
2) Data-based trust models.
3) Hybrid trust models that focus on analyzing both the entity and the data.

Each model computes trust in VFC differently and has varied properties that can be useful in various scenarios and with various VFC applications. Data-based models may be more accurate in assessing trust than entity-based ones. Entity-based models, for example, can be an excellent solution for dealing with sparse traffic. On the other hand, data-based models would not perform efficiently and could be affected depending on interactions because there is a limited possibility for two cars to meet again (Wu et al., [54]).

B. TRUST MANAGEMENT IN VFC

In VFC systems, building trust between entities is made possible through trust management. It highlights the methods and best practices that help build confidence. Trust becomes particularly important when dealing with sensitive data, such as health-related data, because the information provided is so personal.

Many trust models have demonstrated usefulness in various fields, such as autonomous agents in multi-agent systems [55]. Meanwhile, multiple traits, like dynamic topology and vehicle scalability, which are crucial factors to consider in VFC, can affect their effectiveness. Therefore, creating the best trust model for VFC is vital.

In the VFC use case, three primary models can be used: Trust-middleware, collusion deception, and region-based trust models. The Trust middleware model solves distrust problems by providing a standalone layer dedicated to supporting security considerations [56]. It can also be used as an intermediary between the Internet of Healthcare Things (IoHT) devices and the cloud to ensure privacy compliance [57]. It can also be used to assess and enforce compliance with Organization for Economic Cooperation and Development (OECD) privacy principles, which are widely recognized guidelines for protecting personal data.

However, in the collusion deception model, If a witness rates another vehicle several times or incorrectly, a malevolent node, for example, uses the same key K to encrypt the message to the requesting vehicle, which ignores all communications encrypted with that key. The rogue node occasionally could take others' keys [58]. The collusion trust model addresses the issue of preserving privacy in a content-based publish-subscribe scheme within fog computing. The primary focus is protecting user privacy and preventing potential collusion attacks, where multiple fog nodes could combine their resources or data to violate privacy.

The last model is the region-based trust model, which considers various physical devices located in multiple locations with various communication unique types and connection topologies in the Fog. Fog nodes can still offer customers localized processing for a quicker response [59]. Figure 4 illustrates the three models used for managing trust in a VFC environment [44].

C. SECURE-SERVICE MANAGEMENT IN VFC

In the dynamic landscape of VFC, a game-changing reputation-based service provisioning system unfolds. Authors in [60], introduce a thorough evaluation of service providers, incorporating service history, performance metrics, and user feedback. Beyond authentication measures, the system enables secure service discovery, allowing users to make informed choices based on reputation scores. It establishes stringent service-level security policies, ensuring providers adhere to top-tier data privacy practices. Notably, the system's dynamic reputation-updating mechanisms

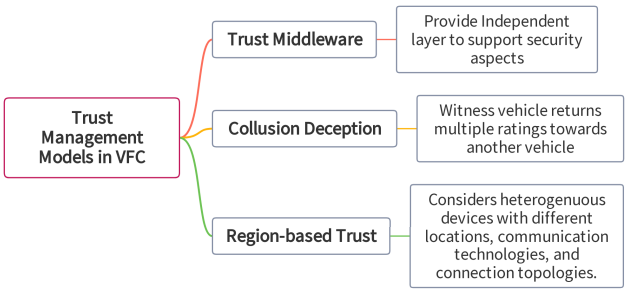


FIGURE 4. Trust management models in VFC.

ensure real-time relevance, empowering users to confidently navigate the Fog and choose reliable and trustworthy services in this ever-evolving narrative.

Indeed, integrating Blockchain in VFC played a vital role in efficiently securing services in VFC [61]. Thanks to its decentralized nature, Blockchain helped to enhance the system's security, protecting data and transactions from unauthorized access. Encrypted communication protocols secure information exchange, and access controls permit only authenticated entities to access computing resources, reducing the risk of security breaches. Implementing secure Service Level Agreements (SLAs) increases reliability while enforcing security requirements. Smart contracts further optimize resource allocation, ensuring efficient use of computing resources and addressing security challenges in VFC [62].

Also, The authors in [63] propose a framework that incorporates reputation-based prioritization and resource allocation techniques in the context of vehicular fog computing. By considering the reputation of vehicles based on their past behavior and performance, the framework prioritizes resource allocation to more trustworthy and reliable vehicles. It also leverages predictive analytics to estimate future resource requirements, enabling proactive and optimized resource allocation. The framework specifically focuses on the unique challenges of vehicular networks and aims to enhance resource management, reduce latency, and improve overall system efficiency. The empirical evaluations and results provided in the paper support the effectiveness of the proposed techniques in the vehicular fog computing domain.

D. PRIVACY PRESERVATION IN VFC

Since vehicular fog nodes may acquire sensitive data about end-user identities, smart grids, or positions, privacy preservation in the VFC is far more difficult than in the core network. An attacker can access the vehicular network by exploiting a poorly protected VF node. Once within the network, the attacker can mine and abuse the user's private data shared across entities [64].

1) LOCATION PRIVACY PRESERVATION

Guaranteeing vehicle privacy also entails ensuring vehicle identity. Most of the time, the genuine identities of the vehicles are replaced with pseudonyms. Vehicles regularly change pseudonyms to avoid being traced indefinitely. However, because of the significant growth in the number of vehicles, pseudonym management, including pseudonym formation, distribution, and revocation, has become a priority. First, pseudonyms have been managed in centralized platforms, which requires high computational resources and time. However, deploying a pseudonym management system at the network edge (e.g., fog/edge computing) helped produce, disseminate, and revoke pseudonyms faster, improving the vehicle location privacy and decreasing the communication overhead [65]. Also, the vehicles can change their pseudonyms while keeping their location anonymous from outsiders using the Cryptographic MIX-Zones (CMIX) deployed at the crossroads level [66]. Every vehicle inside a mixed zone is given a symmetric key by the Road Side Unit (RSU), and when inside the zone, these vehicles use this key to encrypt all messages. Furthermore, the vehicle can dynamically manage their keys to protect their privacy, where the users can use a pseudo-ID to conceal their real identities while registering for a location-based service (LBS) [67]. The service session key can be quickly and effectively updated to achieve forward, backward, and collision prevention. Also, the vehicles can improve their privacy by interrupting the heartbeat message delivery when a speed threshold is reached. This method is called ''SLOW'' which stands for ''silence at low speeds''), allowing a synced period for vehicles to switch their pseudonyms [68].

2) OTHER DATA PRIVACY PRESERVATION

In the context of Fog Computing, Wang et al. present a privacy-preserving content-based PS system with differential privacy (PCP). The PCP can protect users' privacy and the PS system's functioning and resist collusion threats [58]. Most privacy-preserving information-gathering techniques only permit data aggregation for homogeneous IoT devices. They cannot combine data from hybrid IoT devices into one in some real-world IoT applications. Lu et al. provide LPDA, a lightweight privacy-preserving data aggregation technique for Fog Computing-enhanced IoT. The suggested LPDA stands out for its use of homomorphic Parlier encryption, the Chinese Remainder Theorem, and one-way hash chain techniques to combine hybrid IoT device data into one, as well as a filter intruding bogus data at the network's edge [69]. Another security model for protecting medical big data privacy in a healthcare cloud using a fog computing facility and pairing-based cryptography is proposed in [70]. Data theft incidences are thus acknowledged as one of the riskiest breaches of security of data related to health care in the cloud, particularly the electronic medical record (EMR), which must be accommodated in enormous data storage in the healthcare cloud, according to [70]. Also, the authors in [71] offer a privacy-preserving protocol for improving security in vehicle crowd sensing-based road surface condition monitoring systems employing Fog Computing-based certificateless aggregate sign-encryption (CLASC) to ensure privacy, confidentiality, and integrity. Wang et al. provide a secure and privacy-preserving navigation strategy based on fog-based

VANETs that employ vehicular spatial crowdsourcing. Thus, unlike models that use a trusted authority (TA), a trustworthy and public agency (TPA) might identify the driver who submits incorrect traffic information. Nobody, not even TA, can connect a vehicle's navigation inquiry with its identity [72]. Lin et al. have also invented GSIS, a conditional privacy-preserving protocol for VANETs. They employed a brief collaborative signature for signing the messages delivered by cars, ensuring signers' anonymity and matching the anonymity and traceability conditions of VANETs deployment [73]. Weimerskirch and Westhoff presented a protocol that permits nodes with no extra knowledge to re-recognize themselves when they encounter them again. Their method ensures the utmost privacy while maintaining immutable and non-migrable identities [74].

In table 3, we illustrate all the proposed solutions for privacy preservation in VFC.

E. ORGANIZATION SECURITY MANAGEMENT IN VFC

The primary contribution of a secure crowd-sensing protocol for the fog-based vehicular cloud is establishing robust organizational security management in VFC. It is achieved by implementing secure data collection mechanisms, safeguarding against unauthorized access and tampering [71]. Privacy preservation measures, including anonymous communication and data aggregation, protect individuals' and vehicles' privacy. Access control mechanisms regulate data and service management, ensuring only authorized entities access resources. Secure Service Level Agreements (SLAs) define and enforce security requirements for reliable services. The protocol also ensures secure resource management, optimizing allocation to prevent unauthorized usage and resource wastage, thereby promoting efficient utilization of computing resources in a VFC environment [34].

After establishing robust organizational security management with a secure crowd-sensing protocol for the fog-based vehicular cloud, another key contribution lies in enhancing security, privacy, and fairness in vehicular crowd-sensing. It involves implementing secure data collection, privacy preservation, access control mechanisms, confidentiality, and regulated data management. Additionally, the system employs secure data aggregation techniques and promotes fairness and accountability among participants [75].

F. ATTACKS IN VFC

Fog vehicles are frequently used in open environments like VANETs, making them susceptible to attacks that could damage the system [76]. Information such as the speed and position of the cars is essential for data transfer in vehicular networks because most applications in the vehicular system depend on information about the current traffic situation, emergency warnings, accidents, congestion avoidance, etc. The location information in the vehicular network must be validated using different devices such as radar, GPS, etc. The algorithm eliminates the improbable spots if the vehicles do not have such equipment [77]. The tamper-proof GPS device is one of the most effective solutions for safeguarding vehicle position. New threats in VFC have not previously occurred and have had no substantial impact in other contexts, such as vehicular clouds [78]. Thus, many security approaches advocated for VCC have been difficult to implement in VFC due to various flaws. Here is a summary of some of the attacks that put VFC's security at risk:

1) MAN IN THE MIDDLE ATTACKS

Most fog vehicles cannot establish secure communication protocols due to insufficient resources. An eavesdropper can sniff or intercept messages among fog vehicles in a man-in-the-middle attack [79]. Indeed, the authors in [80] employ traffic analysis to identify patterns and detect anomalies that may indicate the presence of a Man-in-middle attack (MITM). By monitoring network traffic and comparing it against normal patterns, the system can identify suspicious behaviors that suggest an attacker's presence. In addition to detection, the paper suggests a reactive prevention mechanism to mitigate the impact of MITM attacks. When an attack is detected, the system can block or divert malicious traffic to prevent further damage or unauthorized access.

2) AUTHENTICATION-RELATED ATTACKS

Authentication is one of the main problems that VFC is currently dealing with. Numerous approaches are offered to deal with this problem, but none provide a complete resolution. It is not advised to rely on a remote authentication server for this activity, especially as the VFC paradigm emphasizes the new capabilities rather than sending the data to the remote servers [81], [82]. Indeed, the Authors in [83] introduce a certificateless authentication scheme, where vehicles and fog nodes can establish secure communication without needing traditional public key infrastructure (PKI) certificates. It eliminates the requirement for certificate management and associated overhead, making the authentication process more efficient.

Also, in [84], the ANAA-Fog scheme has been suggested as an anonymous authentication mechanism designed for 5G-enabled VFC. This approach enhances security and privacy by allowing vehicles to authenticate themselves and their data while maintaining anonymity. The scheme employs symmetric and asymmetric encryption, secure hash functions, anonymous credentials, and revocation mechanisms to ensure vehicular communication's integrity, confidentiality, and anonymity in 5G-enabled fog computing systems.

3) AVAILABILITY-RELATED ATTACKS

One of the features of VFC is that consumers can use its services at any time. When a fog vehicle sustains damage, a related mechanism should promptly redirect consumers to another nearby node. However, the huge number of geographically dispersed vehicles presents a significant challenge [85].In this regard, the authors, in [86], contribute

TABLE 3. Privacy preservation in VFC.

Ref	Proposed Model	Execution				Improvement
		Network Edge	Road	Vehicle	Physical Server (PS)	
[65]	Fog Computing-based Pseudonym Management	✓				- Enhance location privacy - Reduce overhead
[66]	Cryptographic Mix-zones (C-MIX)		✓			- Ensure location privacy - Encrypt shared message inside
[67]	Dynamic privacy preservation Key management (DIKE)			✓		- Requires authentication to join the service - Mask identity during the session - Protect service content
[68]	Silent at Low Speeds (SLOW)			✓		- Synchronizing the change of pseudonyms
[58]	Privacy-preserving content-based scheme (PCP)				✓	- Ensure the privacy preservation of users - Resist the collusion of attacks
[69]	Lightweight Privacy-preserving Data Aggregation (LPDA)	✓				- Support data aggregation for Hybrid IoT devices - Early filter injected false data - Use homomorphic Parlier encryption
[71]	Fog Computing-based Certificate Less Aggregate Sign-encryption (CLASC)		✓			- Provides privacy, confidentiality, and integrity
[72]	A Secure and Privacy-Preserving Navigation Scheme			✓		- Trace the identity of the driver who reports false traffic information
[73]	Secure and Privacy-Preserving Protocol (GSIS)	✓				- Use a short group signature to sign the messages sent by vehicles

by proposing an optimized VFC scheme to efficiently process and disseminate emergency messages. The scheme strategically selects fog nodes (vehicles with computing resources) based on their proximity and availability to the emergency scene, minimizing delays and enhancing the overall effectiveness of emergency message dissemination.

4) DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS

A DDoS attack is one of the most difficult security concerns since it is used to flood a target with bogus traffic. In the context of vehicular Fog, deploying fog vehicles as bots to launch many meaningless service requests simultaneously causes more harm than traditional DDoS. As a result, vehicular fog nodes cannot handle many queries simultaneously, and Many services may become unavailable over an extended period [87]. The authors in [88] leverage fog computing to deploy an anomaly detection mechanism closer to IoT devices and edge networks. By placing detection modules at fog nodes, the framework identifies and mitigates attacks near their source, reducing the impact on the IoT network and improving response times. This approach enhances the scalability and efficiency of DDoS prevention in IoT environments. Indeed, utilizing fog computing to deploy DDoS mitigation closer to IoT devices can enhance network performance by filtering malicious traffic at the source and reducing the impact of attacks on the IoT network [89].

In table 4, we illustrate the Existing attacks that may threaten VF nodes and the whole VF network. We have classified those attacks based on six security aspects: Confidentiality, integrity, availability, authenticity, privacy, and delivery time.

G. ACCESS CONTROL IN VFC

VFC raises several security and privacy problems, mostly regarding resource and service access. In conventional structures, subjects are assigned identities. These identities are presented to the system during user identification and validated during authentication. Thus, assigning and confirming IDs for every VF node in an urban area with a randomly shifting number of vehicles is impractical.

S. Salonikias presents an Attribute-Based Access Control (ABAC) system, an access control (AC) method based on attributes, defined as name-value pairs carrying information on objects, subjects, and context. These context

characteristics make ABAC implementations context-aware, making them an ideal candidate for ITS applications where context impacts the whole system behavior [99].

In traditional computer systems, the reference monitor is frequently incorporated with the secured objects or implemented in a centralized place that receives inquiries for distributed objects, such as Cloud Computing [100]. However, both techniques are challenging in a dynamic and dynamically distributed ITS system like Fog Computing, where AC choices are made in real-time. However, both approaches are impractical in a dynamic and distributed ITS environment like Fog Computing, where access control requires real time decisions.

C. Dsouza et al. propose a policy-based resource AC in Fog Computing to promote secure cooperation and interoperability among multiple user-requested resources. They demonstrated the applicability and utility of their technique by implementing a VFC idea in various use-case scenarios [101]. They suggested a VFC environment, a heterogeneous distributed architecture designed to enable real-time communication between smart systems and commuters. They also actively track traffic behaviors to allow for traffic preemption and safe commuter redirection.

H. SECURE COMMUNICATIONS IN VFC

Mainly, secure communications in VFC can be divided into two types [64]: ***Inter*** and ***Intra*** constrained-IoT/VF nodes communications. The attackers in the VFC can send bogus messages, such as wrong information, to the network during the communication process [52]. These components proved the need for an effective and adaptable end-to-end security technique for VFC communications, capable of dealing with unstable network connections and achieving security settings appropriate for various applications. To ensure the confidentiality and integrity of data, Hu et al. [6] indicate the use of lightweight encryption or masking algorithms during communications from VFC to the cloud. When sending data from the VANET to the cloud, the authors of [12] illustrate that secure communication should be resilient and flexible in a resource-constrained vehicular fog context. Fang et al. create a lightweight, secure routing protocol AODV (SAL-SAODV) in the VFC based on source anonymity to improve security design and communication performance [102]. Also, Wang et al. introduce the anonymous and secure aggregation scheme (ASAS) in Fog Computing, which is a scheme to assure data confidentiality when transporting data from edge devices to the cloud using bilinear pairings and the Castagnos-Laguillaumie cryptosystem approach [103].

I. OTHER TRUST AND SECURITY ISSUES IN VFC

Other trust and security issues, including service availability, can appear in the VFC system. A denial of service (DOS) can be produced when several VF nodes request the same service simultaneously [104]. It requires the development of new defense systems that protect VFC services from this kind of attack while preserving resource consumption [105].

Securing data shared among many vehicular positions, such as orchestration between parked fog vehicles and moved fog vehicles, is also one of the major critical issues that can occur in the VFC system [106]. New security service provisioning models should also be suggested to correctly recommend security services with a crowd-sensing-enabled mechanism in the VFC system [107].

IV. AI AND GAME THEORETIC-BASED SOLUTIONS FOR SECURITY AND PRIVACY IN VFC

Embark on a journey through the dynamic landscape of VFC, where security and privacy challenges find innovative solutions at the intersection of Game Theory and Artificial Intelligence (AI). This exploration unravels strategic game-based approaches and AI-powered solutions, showcasing the synergy that fortifies VFC against cyber threats. From pseudonym-changing games to decentralized blockchain applications, this narrative provides a concise yet comprehensive overview of the transformative power of combining strategic games with intelligent algorithms. However, various solutions have been proposed to address these security threats and maintain VFC security, privacy, and trust.

A. GAME THEORETIC-BASED APPROACHES FOR SECURITY AND PRIVACY IN VFC

With the increase in cyber-security attacks, game theory has become a useful tool for answering security and privacy issues for reliable network communication [108], [109], [110]. Game theory is the formal study of conflict and cooperation among several stakeholders, and it is used whenever the actions of multiple individuals are interdependent. Individuals, groups, businesses, or any combination of these entities may act as agents. The notion of game theory gives a vocabulary for developing, structuring, analyzing, and comprehending strategic scenarios. Security games are a type of game that investigates the interplay between malicious attackers and defenders. Security game techniques are commonly employed to forecast attacker behavior as a foundation for formal decision-making.

One of the most important things in VFC implementation is deploying an incentive mechanism to ensure efficient and secure data transmission. Dealing with the selfishness problem by encouraging nodes to participate in data forwarding and protecting the privacy of vehicle users is needed. Several research projects have been carried out and tested to promote cooperation and save the privacy of vehicle users.

A vehicle in VFC sends out safety and entertaining messages regularly, which can potentially expose the vehicle's position [111]. To solve this issue, the vehicles can hide their identities using substituted pseudonyms [65], [67], [112].

Vehicles may play a pseudonym-changing game to decide whether to alter their pseudonyms while meeting in social hotspots [30].

The suggested approach allows vehicles to communicate and maintain their privacy. Numerical findings reveal

TABLE 4. Existing attacks in VFC.

Ref	Attack Type	Severity						Threat
		Confidentiality	Integrity	Availability	Authenticity	Privacy	Delivery time	
[90]	Eavesdropping					✓		Unauthorized interception of communication between vehicles and fog nodes, leading to potential privacy breaches
[87]–[89], [91]	Distributed Denial of Service (DDoS)	✓					✓	Deliberate disruption of fog computing services, causing vehicles to lose access to resources or delay task offloading
[77], [92], [93]	Sybil Attack	✓						Malicious nodes impersonate multiple identities to gain control or influence over the fog computing network
[94], [95]	Data Tampering		✓					Unauthorized modification or alteration of data exchanged between vehicles and fog nodes, leading to inaccurate results or malicious actions
[96]	Replay Attack				✓			Captured data packets are replayed by an attacker to deceive fog nodes or vehicles.
[79], [80]	Man-in-the-Middle (MITM)		✓					An attacker intercepts and relays communication between vehicles and fog nodes, potentially altering the data in transit.
[97]	Malware Injection		✓	✓				Injecting malicious code or malware into fog nodes or vehicles to disrupt services or steal data.
[97]	Traffic Analysis	✓	✓					Attackers analyze traffic patterns to gain insights into vehicle behavior or sensitive information.
[97]	Identity Spoofing				✓			Attackers impersonate legitimate vehicles or fog nodes to gain unauthorized access.
[98]	Insider Attacks		✓	✓		✓	✓	Malicious actions carried out by authorized entities, such as fog node operators or compromised vehicles.

that the proposed pseudonym method outperforms existing pseudonym management schemes regarding vehicle location privacy while communication overheads are decreased. However, there was no consideration of vehicle mobility, which makes the efficiency of the proposed solution in a dynamic environment unknown [113].

Furthermore, authors in [114] have considered three types of attacks, namely Sybil attacks, tampering message attacks, and packet loss profits attacks [115], [116], and three aspects of privacy, namely data, social attributes, and transaction privacy. Indeed, the authors presented an incentive-based data forwarding technique to increase message transmission efficiency in IoV while protecting vehicle users' private information. It is divided into three modules: location prediction, message processing, and node incentive protection. First, a vehicle movement model for position prediction is created. Following that, a trajectory dataset is extracted. A vehicle similarity computation approach based on moving trajectory, where vehicle groups with high similarity are discovered, is also proposed [117].

The data privacy is then protected by a mechanism called privacy-aware task allocation and data aggregation (PTAA), which is based on a crowd-sensing model with the help of fog nodes. In the IoV, a Robin Steiner bargaining game is used to cope with the selfishness of the node.

As a result, the vehicles show competitiveness in defending against attacks while guaranteeing a user's privacy. However, this study should be investigated and tested in different scenarios, such as the parked scenario [30]. Similarly, authors in [116] develop a bargaining-based approach to managing a vehicle's reputation (DREAMS). It considers reputation query, reputation computation, reputation manifestation, network monitoring, and information record [117], where vehicle users with low reputation values are misbehaving nodes, and the SPs cannot serve them.

V2X communication technology, which uses the mm-wave frequency spectrum, accelerates this technology with huge bandwidth and beamforming. This approach decreases mutual interference and enhances network performance. However, content caching is difficult due to limited local storage and high data transmission costs. The authors in [118] proposed a route segmentation model for mm-Wave V2X communication using evolutionary game theory and developed centralized and distributed algorithms for the evolutionary content cache game. In vehicular Fog, the suggested evolution algorithm directs vehicles to use the ESS for content storage.

Centralized computation offloading poses security threats. A decentralized approach using blockchain technology enables transparent, verifiable, and traceable network activities in computation offloading. Network entities are introduced, and interactive smart contract operations are designed to minimize user payments. The Stackelberg game framework solves the optimal smart contract design problem, demonstrating high security and efficiency guarantees [78].

Also, the authors in [119] look into VFC scenarios where clients offload computation to nearby edge or fog computing nodes, such as moving vehicles. The authors emphasize decentralized multi-agent decision-making in an unknown game, where each agent does not know the game's

composition or opponents. Using an uncoupled learning rule, they generalize the decentralized decision-making method for multi-agent instances. The multi-agent approach detects and reacts to unpredictable offloading cost variations.

Also, the authors in [120] likely aim to address issues related to efficient computation offloading in dynamic vehicle networks, considering both computational task allocation and network resources. The research may provide a novel strategy for maximizing the performance of such networks in terms of computation offloading and resource allocation by applying Contract-Stackelberg to motivate VF nodes with idle resources for cooperation.

Similarly, the authors in [121] propose a game theory-based approach that enables verifiable and fine-grained data management in VFC. It addresses the challenge of managing large-scale data generated by vehicles while maintaining data privacy and integrity. Indeed, they design a game model that captures the interaction between vehicles and fog nodes, considering both the privacy concerns of the vehicles and the resource limitations of the fog nodes.

B. AI-BASED APPROACHES FOR SECURITY AND PRIVACY IN VFC

The authors in [122] introduce perception reaction time (PRT), which indicates the time of safety-related applications and reflects road efficiency and security. Similarly, a VFC platform called oneVFC, through the aggregation of resources from nearby vehicle fog nodes and ITS infrastructure, is proposed [123]. In this sense, oneVFC uses oneM2M, an IoT middleware standard for achieving interoperability across heterogeneous machine-to-machine (M2M) and IoT systems in areas such as smart health and smart farming. The oneVFC platform is tested for AI/DL-based ITS applications in AI-based model exploitation and training. Another hybrid approach, fuzzy reinforcement learning (FRL), was proposed in [124]. The approach combines fuzzy logic (FL) and reinforcement learning (RL) to deal with task-offloading problems in VFC. It was utilized in smart settlements located near rural roads. Indeed, this combination of FL and RL has been used to speed the identification of possible fog vehicles with idle resources while lowering overall energy usage and average reaction time while protecting fog vehicle privacy.

Furthermore, the authors in [125] develop a new V2V partial computation offloading scheme based on deep reinforcement learning (DRL) and evaluate the service availability of surrounding vehicles regarding idle computer resources and vehicle mobility. Based on the actor-critic paradigm, they created an algorithm that determines service vehicle selection, task segmentation, and computational resource allocation in both the task vehicle and the service vehicle.

The authors in [126] discuss major challenges when providing intelligence and computation capabilities to vehicular networks. These challenges arise due to the rapidly changing network dynamics, high mobility, and high reliability with rigorous security requirements that characterize modern vehicular networks. They have studied vehicular fog architecture implementation, considering the deployment of resource allocation and task offloading using deep learning algorithms.

Also, the authors in [127] treat the computational offloading problem as a Markov decision process (MDP) while accounting for the time-varying computing capacity of a dynamic fog server and unpredictable communication channel properties in the vehicular network. The proposed solution is an RL-based approach called FedOVe for determining an optimal association among RSUs and fog servers to optimize energy consumption for RSUs and load balancing for fog servers formed with vehicles with idle computing resources.

Also, the authors in [128] propose an online learning (real-time learning) approach, described as an advice-based learning approach. In this approach, an RSU that has previously learned about the performance of the cars in its coverage area uses that knowledge to advise a neighboring RSU that lacks the experience to make appropriate assignment selections. This method was tested in a moving vehicle scenario to compare it to the case where no advice is shared between RSUs about the vehicles' ability to offload idle resources.

Another contribution of multi-agent reinforcement learning for cooperative edge caching in the Internet of Vehicles (IoV) is leveraging artificial intelligence to optimize edge caching in vehicular fog computing. By employing multi-agent reinforcement learning, vehicles collaboratively make caching decisions based on local observations, enhancing the efficiency and effectiveness of edge caching in the IoV [129]. This AI-based approach facilitates intelligent decision-making, optimizing caching policies through learning from interactions with the environment and other vehicles. It ensures efficient resource utilization by dynamically adapting to traffic patterns, content popularity, and vehicle movements, leading to reduced latency and improved data availability. Furthermore, the approach exhibits scalability and adaptability, enabling effective caching decisions as the number of vehicles in the IoV increases [130].

In table 6, we summarize the AI-based research works for assessing security and efficiency in a VFC environment.

V. OPEN CHALLENGES

This section introduces some major challenges and potential future research directions in cybersecurity and trust in VFC, such as trust and certificate revocation management, Cryptography, malware, and intrusion detection [131], [132].

In terms of trustworthiness, Vehicles in VFC may misbehave by sending faulty information, sharing it with untrustworthy entities, or withholding it selfishly. Adopting a trusted third-party model for secure communication between VF nodes and end-users is crucial to address this issue. Considering the regional nature of the vehicular environment and users' assigned roles is also important [59]. Region-based trust management can handle join/leave requests, and users can be selected based on assigned roles through

TABLE 5. Summary of game theoretic-based approaches in VFC.

Ref	Main contribution	Game Model	VFC aspects			Advantages	Drawbacks
			Incentive Mechanism	Computation Offloading	Security		
[117]	Focuses on reputation management for security and efficiency in VEC	Bargaining	✗	✗	✓	Enhances trust and collaboration among vehicular network participants	Lack of incentive mechanism to mitigate selfish behavior of VF nodes
[118]	Proposes an evolutionary game approach for optimizing content caching using mm-wave communication using ESS solution	Evolutionary	✓	✗	✗	Captures dynamic behavior and adapts to changing network conditions	Challenges in convergence and sensitivity to initial conditions
[78]	Addresses security through Blockchain and smart contracts for parked vehicle-assisted fog computing	Stackelberg	✓	✓	✓	Provides tamper-resistant data storage and automates interactions and Stackelberg-based smart contract	Blockchain's computational overhead and scalability concerns for real-time applications
[119]	Generates a decentralized decision-making method based on a repeated unknown game to solve task offloading problem in VFC	Repeated Unknown	✗	✗	✓	Encourages cooperation over time and suits resource allocation scenarios	Challenges in addressing uncertainties in the unknown game model for real-world adoption
[120]	Generates a contract-based incentive scheme to push VF nodes to cooperate in solving resource allocation problem	Stackelberg	✓	✓	✗	Encourages cooperation over time and suits resource allocation scenarios	Challenges in addressing uncertainties in the unknown game model for real-world adoption
[121]	Generates a contract-based incentive scheme to push VF nodes to cooperate in solving resource allocation problem	A three players	✓	✓	✓	Uses strategic decision-making for data analysis and privacy-preserving techniques to protect sensitive information.	Complexity of ensuring scalability in large-scale environments.

TABLE 6. Summary of research works of AI-based models in VFC.

Ref	VFC aspects			AI model			contributions and features
	Architect. Design.	Resource Alloc.	Security	ML	DL	RL	
[123]	✓	✓	✗	✓			• Design of a VFC-based platform that supports AI in the context of IoV • Real-time AI interference • Efficient resource management
[124]	✗	✓	✓			✓	• Combination of fuzzy logic with RL to perform uncertain conditions of VFC • Energy-Efficient Task Offloading • Energy Efficiency improvement for vehicular applications
[125]	✗	✓	✓		✓	✓	• Conception of a Computation Offloading approach for VFC using DRL and V2V communications • Latency and Energy Optimization • Adaptability to Vehicular Mobility and Network Conditions
[126]	✓	✓	✓		✓		• Combining DL with V2X communication in the called Deep-Vfog • Enabling AI-driven decision-making in V2X communication scenarios • Latency Reduction and Real-Time Response • Energy Efficiency Enhancement
[127]	✓	✓	✓		✓		• Suggesting a federated learning algorithm for computation offloading in a VFC environment • Enhancing privacy preservation for Fog vehicles • Promoting adaptability and scalability
[128]	✓	✓	✗	✓			• proposing new task assignment approach to VF nodes with minimal delay • developing a neighbor advice mechanism to choose the most suitable VF nodes • deploying a called advice-based learning as an online learning approach

verification and authorization strategies, and detecting any policy violation. However, these solutions may not fully protect against insiders, necessitating improvements in trust management models. Currently, the research focuses on developing Certificate Revocation List-based (CRL) solutions to control the trust [133]. It relies on revoking, before the estimated expiry date, a list of digital certificates that have been issued by certificate authorities (CA). After revocation, these certificates remain untrusted. This technique is still under development and not widely deployed in VFC. Another challenge for VFC security, privacy, and non-traceability is Key distribution management. However, models for periodically switching certificates, pseudonym distribution, and short-duration keys are not yet defined [134]. Critical

issues in the VFC system, such as key size, protocols, and authentication delays, are still under study. Furthermore, Developing efficient anti-malware frameworks or intrusion detection systems (IDS) is a critical problem for VFC systems, enhancing network security from malicious activity or policy violations in different communication modes (V2V, V2I, or both). Research is needed for responses to intrusions based on cost-sensitive models, game theory, and proactive tactics [135].

VI. CONCLUSION

VFC has emerged due to emphasizing better utilization of vehicle resources and enhancing intelligent transportation networks. This novel paradigm enables more efficient collaboration among vehicles, significantly reducing data transfer time and network communication stress. This technology additionally meets the requirements of new real-time or latency-sensitive applications. The present research discussed VFC in terms of hierarchical architecture, characteristics, security risks, and countermeasures. The significant security gaps that must be addressed in future research have been identified. To summarize, vehicular fog benefits vehicular networks more than vehicular clouds. Several concerns must be addressed to guarantee that the security requirements are met.

REFERENCES

[1] H. Shah-Mansouri and V. W. S. Wong, "Hierarchical fog-cloud computing for IoT systems: A computation offloading game," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3246–3257, Aug. 2018.

[2] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[3] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *J. Netw. Comput. Appl.*, vol. 40, pp. 325–344, Apr. 2014.

[4] I. Ahmad, R. M. D. Noor, I. Ali, and M. A. Qureshi, "The role of vehicular cloud computing in road traffic management: A survey," in *Future Intelligent Vehicular Technologies* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 185. Cham, Switzerland: Springer, 2017, doi: 10.1007/978-3-319-51207-5_12.

[5] P. Liu, R. Wang, J. Ding, and X. Yin, "Performance modeling and evaluating workflow of ITS: real-time positioning and route planning," *Multimedia Tools Appl.*, vol. 77, no. 9, pp. 10867–10881, May 2018.

[6] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: Architecture, key technologies, applications and open issues," *J. Netw. Comput. Appl.*, vol. 98, pp. 27–42, Nov. 2017.

[7] A. Boukerche and R. E. De Grande, "Vehicular cloud computing: Architectures, applications, and mobility," *Comput. Netw.*, vol. 135, pp. 171–189, Apr. 2018.

[8] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A comprehensive survey on fog computing: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 416–464, 1st Quart., 2018.

[9] M. Ran and X. Bai, "Vehicle cooperative network model based on hypergraph in vehicular fog computing," *Sensors*, vol. 20, no. 8, p. 2269, Apr. 2020.

[10] *IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing*, IEEE Standard 1934-2018, pp. 1–176, Aug. 2018, doi: 10.1109/IEEESTD.2018.8423800.

[11] H. Zhou, T. Wu, X. Chen, S. He, D. Guo, and J. Wu, "Reverse auction-based computation offloading and resource allocation in mobile cloud-edge computing," *IEEE Trans. Mobile Comput.*, vol. 22, no. 10, pp. 6144–6159, Oct. 2023.

[12] M. Mukherjee, L. Shu, and D. Wang, "Survey of fog computing: Fundamental, network applications, and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1826–1857, 3rd Quart., 2018.

[13] F. Bonomi, "The smart and connected vehicle and the Internet of Things," in *Proc. Workshop Synchronization Telecommun. Syst.*, 2013.

[14] Y. Xiao and C. Zhu, "Vehicular fog computing: Vision and challenges," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 6–9.

[15] S. Raza, S. Wang, M. Ahmed, and M. R. Anwar, "A survey on vehicular edge computing: Architecture, applications, technical issues, and future directions," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–19, Feb. 2019.

[16] C. Huang, R. Lu, and K. R. Choo, "Vehicular fog computing: Architecture, use case, and security and forensic challenges," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 105–111, Nov. 2017.

[17] M. A. Hoque and R. Hasan, "Towards an analysis of the architecture, security, and privacy issues in vehicular fog computing," in *Proc. SoutheastCon*, Apr. 2019, pp. 1–8.

[18] C. Zhu, G. Pastor, Y. Xiao, and A. Ylajaaski, "Vehicular fog computing for video crowdsourcing: Applications, feasibility, and challenges," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 58–63, Oct. 2018.

[19] V. G. Menon and J. Prathap, "Vehicular fog computing: Challenges applications and future directions," *Int. J. Veh. Telematics Infotainment Syst. (IJVTIS)*, vol. 1, no. 2, pp. 15–23, 2017.

[20] T. Mekki, I. Jabri, L. Chaari, and A. Rachedi, "A survey on vehicular fog computing: Motivation, architectures, taxonomy, and issues," in *Web, Artificial Intelligence and Network Applications—WAINA* (Advances in Intelligent Systems and Computing), vol. 1150, L. Barolli, F. Amato, F. Moscato, T. Enokido, and M. Takizawa, Eds. Cham, Switzerland: Springer, 2020, doi: 10.1007/978-3-030-44038-1_15.

[21] N. Gaouar and M. Lehsaini, "Toward vehicular cloud/fog communication: A survey on data dissemination in vehicular ad hoc networks using vehicular cloud/fog computing," *Int. J. Commun. Syst.*, vol. 34, no. 13, p. e4906, Sep. 2021.

[22] N. Keshari, D. Singh, and A. K. Maurya, "A survey on vehicular fog computing: Current state-of-the-art and future directions," *Veh. Commun.*, vol. 38, Dec. 2022, Art. no. 100512.

[23] A. M. A. Hamdi, F. K. Hussain, and O. K. Hussain, "Task offloading in vehicular fog computing: State-of-the-art and open issues," *Future Gener. Comput. Syst.*, vol. 133, pp. 201–212, Aug. 2022.

[24] W. Mao, O. U. Akgul, B. Cho, Y. Xiao, and A. Ylä-Jääski, "On-demand vehicular fog computing for beyond 5G networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 12, pp. 15237–15253, Dec. 2023.

[25] Z. Ning, J. Huang, and X. Wang, "Vehicular fog computing: Enabling real-time traffic management for smart cities," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 87–93, Feb. 2019.

[26] Y. Zhang, C.-Y. Wang, and H.-Y. Wei, "Parking reservation auction for parked vehicle assistance in vehicular fog computing," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3126–3139, Apr. 2019.

[27] S.-S. Lee and S. Lee, "Resource allocation for vehicular fog computing using reinforcement learning combined with heuristic information," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10450–10464, Oct. 2020.

[28] J. Klaimi, S.-M. Senouci, and M.-A. Messous, "Theoretical game approach for mobile users resource management in a vehicular fog computing environment," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 452–457.

[29] O. Nazih, N. Benamar, and A. Addaim, "An incentive mechanism for computing resource allocation in vehicular fog computing environment," in *Proc. Int. Conf. Innov. Intell. Informat., Comput. Technol. (3ICT)*, Dec. 2020, pp. 1–5.

[30] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, "Vehicular fog computing: A viewpoint of vehicles as the infrastructures," *IEEE Trans. Veh. Technol.*, vol. 65, no. 6, pp. 3860–3873, Jun. 2016.

[31] Y. Lai, F. Yang, L. Zhang, and Z. Lin, "Distributed public vehicle system based on fog nodes and vehicular sensing," *IEEE Access*, vol. 6, pp. 22011–22024, 2018.

[32] M. A. U. Rehman, M. Salah ud din, S. Mastorakis, and B.-S. Kim, "FoggyEdge: An information-centric computation offloading and management framework for edge-based vehicular fog computing," *IEEE Intell. Transp. Syst. Mag.*, vol. 15, no. 5, pp. 78–90, Sep./Oct. 2023.

[33] D. C. Binwal, R. Tiwari, and M. Kapoor, "Modeling and optimization of vehicular fog network towards minimizing latency," *Mobile Netw. Appl.*, 2023, doi: 10.1007/s11036-023-02197-5.

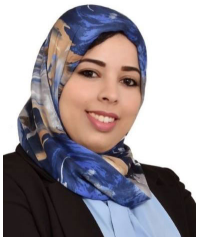
[34] L. Nkenyereye, S. M. R. Islam, M. Bilal, M. Abdullah-Al-Wadud, A. Alamri, and A. Nayyar, "Secure crowd-sensing protocol for fog-based vehicular cloud," *Future Gener. Comput. Syst.*, vol. 120, pp. 61–75, Jul. 2021.
[35] L. Zhang and J. Li, "Enabling robust and privacy-preserving resource allocation in fog computing," *IEEE Access*, vol. 6, pp. 50384–50393, 2018.
[36] F. H. Rahman, A. Y. M. Iqbal, S. H. S. Newaz, A. T. Wan, and M. S. Ahsan, "Street parked vehicles based vehicular fog computing: TCP throughput evaluation and future research direction," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 26–31.
[37] I. W. Ho, S. C. Chau, E. R. Magsino, and K. Jia, "Efficient 3D road map data exchange for intelligent vehicles in vehicular fog networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3151–3165, Mar. 2020.
[38] J. Li, C. Natalino, D. P. Van, L. Wosinska, and J. Chen, "Resource management in fog-enhanced radio access network to support real-time vehicular services," in *Proc. IEEE 1st Int. Conf. Fog Edge Comput. (ICFEC)*, May 2017, pp. 68–74.
[39] M. M. Hussain and M. M. S. Beg, "CODE-V: Multi-hop computation offloading in vehicular fog computing," *Future Gener. Comput. Syst.*, vol. 116, pp. 86–102, Mar. 2021.
[40] Z. Deng, Z. Cai, and M. Liang, "A multi-hop VANETs-assisted offloading strategy in vehicular mobile edge computing," *IEEE Access*, vol. 8, pp. 53062–53071, 2020.
[41] L. Liu, M. Zhao, M. Yu, M. A. Jan, D. Lan, and A. Taherkordi, "Mobility-aware multi-hop task offloading for autonomous driving in vehicular edge computing and networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2169–2182, Feb. 2023.
[42] Y. Sun and N. Zhang, "A resource-sharing model based on a repeated game in fog computing," *Saudi J. Biol. Sci.*, vol. 24, no. 3, pp. 687–694, Mar. 2017.
[43] Y. Sun, F. Lin, and N. Zhang, "A security mechanism based on evolutionary game in fog computing," *Saudi J. Biol. Sci.*, vol. 25, no. 2, pp. 237–241, Feb. 2018.
[44] O. Nazih, N. Benamar, H. Lamaazi, and H. Chaoui, "Challenges and future directions for security and privacy in vehicular fog computing," in *Proc. Int. Conf. Innov. Intell. Informat., Comput., Technol. (ICT)*, Nov. 2022, pp. 693–699.
[45] V. B. Souza, M. H. Pereira, L. H. S. Lelis, and X. Masip-Bruin, "Enhancing resource availability in vehicular fog computing through smart inter-domain handover," in *Proc. GLOBECOM IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–6.
[46] S. Arif, S. Olariu, J. Wang, G. Yan, W. Yang, and I. Khalil, "Datacenter at the airport: Reasoning about time-dependent parking lot occupancy," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 11, pp. 2067–2080, Nov. 2012.
[47] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *J. Netw. Comput. Appl.*, vol. 84, pp. 38–54, Apr. 2017.
[48] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote data checking for network coding-based distributed storage systems," in *Proc. ACM Workshop Cloud Comput. Secur. Workshop*, Oct. 2010, pp. 31–42.
[49] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Fog computing: A platform for Internet of Things and analytics," in *Big Data and Internet of Things: A Roadmap for Smart Environments*. Berlin, Germany: Springer, 2014, pp. 169–186.
[50] F.-J. Ferrández-Pastor, H. Mora, A. Jimeno-Morenilla, and B. Volckaert, "Deployment of IoT edge and fog computing technologies to develop smart building services," *Sustainability*, vol. 10, no. 11, p. 3832, Oct. 2018.
[51] N. Chen, Y. Yang, T. Zhang, M.-T. Zhou, X. Luo, and J. K. Zao, "Fog as a service technology," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 95–101, Nov. 2018.
[52] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales, M. K. Khan, and S. Goudarzi, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619–15629, 2017.
[53] Q. Alriyami, A. Adnane, and A. K. Smith, "Evaluation criterias for trust management in vehicular ad-hoc networks (VANETs)," in *Proc. Int. Conf. Connected Vehicles Expo (ICCVE)*, Nov. 2014, pp. 118–123.
[54] Y. Wu, F. Meng, G. Wang, and P. Yi, "A Dempster–Shafer theory based traffic information trust model in vehicular ad hoc networks," in *Proc. Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun. (SSIC)*, Aug. 2015, pp. 1–7.
[55] D. Jelenc, R. Hermoso, J. Sabater-Mir, and D. Trcek, "Decision making matters: A better way to evaluate trust models," *Knowl.-Based Syst.*, vol. 52, pp. 147–164, Nov. 2013.
[56] E. Onica, P. Felber, H. Mercier, and E. Rivière, "Confidentiality-preserving Publish/subscribe: A survey," *ACM Comput. Surv.*, vol. 49, no. 2, pp. 1–43, Jun. 2017.
[57] A. M. Elmisery, S. Rho, and D. Botvich, "A fog based middleware for automated compliance with OECD privacy principles in Internet of Healthcare Things," *IEEE Access*, vol. 4, pp. 8418–8441, 2016.
[58] Q. Wang, D. Chen, N. Zhang, Z. Ding, and Z. Qin, "PCP: A privacy-preserving content-based publish-subscribe scheme with differential privacy in fog computing," *IEEE Access*, vol. 5, pp. 17962–17974, 2017.
[59] T. D. Dang and D. Hoang, "A data protection model for fog computing," in *Proc. 2nd Int. Conf. Fog Mobile Edge Comput. (FMEC)*, May 2017, pp. 32–38.
[60] C. Tang and H. Wu, "Reputation-based service provisioning for vehicular fog computing," *J. Syst. Archit.*, vol. 131, Oct. 2022, Art. no. 102735.
[61] X. Liu, W. Chen, Y. Xia, and C. Yang, "SE-VFC: Secure and efficient outsourcing computing in vehicular fog computing," *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 3, pp. 3389–3399, Sep. 2021.
[62] M. Kong, J. Zhao, X. Sun, and Y. Nie, "Secure and efficient computing resource management in blockchain-based vehicular fog computing," *China Commun.*, vol. 18, no. 4, pp. 115–125, Apr. 2021.
[63] M. I. Khattak, Y. Hui, A. Ahmad, and A. Khan, "RPRA: Reputation-based prioritization and resource allocation leveraging predictive analytics and vehicular fog computing," *Ad Hoc Netw.*, vol. 155, Mar. 2024, Art. no. 103401.
[64] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293–19304, 2017.
[65] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 8, pp. 2627–2637, Aug. 2018.
[66] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *Proc. ACM Workshop Wireless Netw. Intelligent Transp. Syst. (WiN-ITS)*, Vancouver, BC, Canada, 2007. [Online]. Available: http://infoscience.epfl.ch/record/109437
[67] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–139, Mar. 2012.
[68] L. Buttyan, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: A practical pseudonym changing scheme for location privacy in VANETs," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Oct. 2009, pp. 1–8.
[69] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.
[70] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, "A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography," *IEEE Access*, vol. 5, pp. 22313–22328, 2017.
[71] S. Basudan, X. Lin, and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing," *IEEE Internet Things J.*, vol. 4, no. 3, pp. 772–782, Jun. 2017.
[72] L. Wang, G. Liu, and L. Sun, "A secure and privacy-preserving navigation scheme using spatial crowdsourcing in fog-based VANETs," *Sensors*, vol. 17, no. 4, p. 668, Mar. 2017.
[73] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.
[74] A. Weimerskirch and D. Westhoff, "Zero common-knowledge authentication for pervasive networks," in *Proc. Int. Workshop Sel. Areas Cryptography*, vol. 3006, M. Matsui and R. J. Zuccherato, Eds. Berlin, Germany: Springer, 2003, doi: 10.1007/978-3-540-24654-1_6.
[75] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 146–152, Jun. 2017.
[76] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: A review of current applications and security solutions," *J. Cloud Comput.*, vol. 6, no. 1, p. 19, Dec. 2017.
[77] S. Benadla and O. R. Merad-Boudia, "The impact of Sybil attacks on vehicular fog networks," in *Proc. Int. Conf. Recent Adv. Math. Informat. (ICRAMI)*, Sep. 2021, pp. 1–6.

[78] X. Huang, D. Ye, R. Yu, and L. Shu, "Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 2, pp. 426–441, Mar. 2020.
[79] K. Bhargavi and S. G. Shiva, "Man-in-the-middle attack explainer for fog computing using soft actor critic Q-learning approach," in *Proc. IEEE World AI IoT Congr. (AIIoT)*, Jun. 2022, pp. 100–105.
[80] F. Aliyu, T. Sheltami, and E. M. Shakshuki, "A detection and prevention technique for man in the middle attack in fog computing," *Proc. Comput. Sci.*, vol. 141, pp. 24–31, Jan. 2018.
[81] X. Duan, Y. Guo, and Y. Guo, "Design of anonymous authentication scheme for vehicle fog services using blockchain," *Wireless Netw.*, vol. 30, no. 1, pp. 193–207, Jan. 2024.
[82] Z. G. Al-Mekhlafi, M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, A. Alreshidi, M. Alazmi, J. S. Alshudukhi, M. Alsaffar, and T. H. Rassem, "Efficient authentication scheme for 5G-enabled vehicular networks using fog computing," *Sensors*, vol. 23, no. 7, p. 3543, Mar. 2023.
[83] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "ECA-VFog: An efficient certificateless authentication scheme for 5G-assisted vehicular fog computing," *PLoS ONE*, vol. 18, no. 6, Jun. 2023, Art. no. e0287291.
[84] B. A. Mohammed, M. A. Al-Shareeda, S. Manickam, Z. G. Al-Mekhlafi, A. M. Alayba, and A. A. Sallam, "ANAA-fog: A novel anonymous authentication scheme for 5G-enabled vehicular fog computing," *Mathematics*, vol. 11, no. 6, p. 1446, Mar. 2023.
[85] M. Y. Darus and K. A. Bakar, "Review of congestion control algorithm for event-driven safety messages in vehicular networks," *Int. J. Comput. Sci. Issues (IJCSI)*, vol. 8, no. 5, p. 49, 2011.
[86] A. Ullah, S. Yaqoob, M. Imran, and H. Ning, "Emergency message dissemination schemes based on congestion avoidance in VANET and vehicular FoG computing," *IEEE Access*, vol. 7, pp. 1570–1585, 2019.
[87] T. Klein, T. Fenn, A. Katzenbach, H. Teigeler, S. Lins, and A. Sunyaev, "A threat model for vehicular fog computing," *IEEE Access*, vol. 10, pp. 133256–133278, 2022.
[88] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, "A DDoS attack mitigation framework for IoT networks using fog computing," *Proc. Comput. Sci.*, vol. 182, pp. 13–20, Jan. 2021.
[89] D. K. Sharma, T. Dhankhar, G. Agrawal, S. K. Singh, D. Gupta, J. Nebhen, and I. Razzak, "Anomaly detection framework to prevent DDoS attack in fog empowered IoT networks," *Ad Hoc Netw.*, vol. 121, Oct. 2021, Art. no. 102603.
[90] M. Arif, G. Wang, and V. E. Balas, "Secure VANETs: Trusted communication scheme between vehicles and infrastructure based on fog computing," *Stud. Informat. Control*, vol. 27, no. 2, pp. 235–246, Jan. 2019.
[91] H. Amari, W. Louati, L. Khoukhi, and L. H. Belguith, "Securing software-defined vehicular network architecture against DDoS attack," in *Proc. IEEE 46th Conf. Local Comput. Netw. (LCN)*, Oct. 2021, pp. 653–656.
[92] L. J. Vinita and V. Vetriselvi, "Impact of Sybil attack on software-defined vehicular fog computing (SDVF) for an emergency vehicle scenario," in *Inventive Communication and Computational Technologies* (Lecture Notes in Networks and Systems), vol. 383, G. Ranganathan, X. Fernando, and Ã. Rocha, Eds. Singapore: Springer, 2023, doi: 10.1007/978-981-19-4960-9_61.
[93] S. Benadla, O. R. Merad-Boudia, S. M. Senouci, and M. Lehsaini, "Detecting Sybil attacks in vehicular fog networks using RSSI and blockchain," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 3919–3935, Dec. 2022.
[94] F. Dewanta and M. Mambo, "BPT scheme: Establishing trusted vehicular fog computing service for rural area based on blockchain approach," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1752–1769, Feb. 2021.
[95] Q. Kong, L. Su, and M. Ma, "Achieving privacy-preserving and verifiable data sharing in vehicular fog with blockchain," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 4889–4898, Aug. 2021.
[96] F. Dewanta and M. Mambo, "A mutual authentication scheme for secure fog computing service handover in vehicular network environment," *IEEE Access*, vol. 7, pp. 103095–103114, 2019.
[97] H. Lamaazi, "Cyber security for edge/fog computing applications," in *Cyber Security for Next-Generation Computing Technologies*. Boca Raton, FL, USA: CRC Press, 2024, pp. 177–189.
[98] T.-Y. Wu, X. Guo, Y.-C. Chen, S. Kumari, and C.-M. Chen, "SGXAP: SGX-based authentication protocol in IoV-enabled fog computing," *Symmetry*, vol. 14, no. 7, p. 1393, Jul. 2022.
[99] N. Dan, S. Hua-Ji, C. Yuan, and G. Jia-Hu, "Attribute based access control (ABAC)-based cross-domain access control in service-oriented architecture (SOA)," in *Proc. Int. Conf. Comput. Sci. Service Syst.*, Aug. 2012, pp. 1405–1408.
[100] B. Lampson, M. Abadi, M. Burrows, and E. Wobber, "Authentication in distributed systems: Theory and practice," *ACM Trans. Comput. Syst. (TOCS)*, vol. 10, no. 4, pp. 265–310, 1992.
[101] C. Dsouza, G.-J. Ahn, and M. Taguinod, "Policy-driven security management for fog computing: Preliminary framework and a case study," in *Proc. IEEE 15th Int. Conf. Inf. Reuse Integr.*, Aug. 2014, pp. 16–23.
[102] W. Fang, W. Zhang, J. Xiao, Y. Yang, and W. Chen, "A source anonymity-based lightweight secure AODV protocol for fog-based MANET," *Sensors*, vol. 17, no. 6, p. 1421, Jun. 2017.
[103] H. Wang, Z. Wang, and J. Domingo-Ferrer, "Anonymous and secure aggregation scheme in fog-based public cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 712–719, Jan. 2018.
[104] M. T. Saqib and M. A. Hamid, "FogR: A highly reliable and intelligent computation offloading on the Internet of Things," in *Proc. IEEE Region Conf. (TENCON)*, Nov. 2016, pp. 1039–1042.
[105] Y. Bi, "Neighboring vehicle-assisted fast handoff for vehicular fog communications," *Peer-Peer Netw. Appl.*, vol. 11, no. 4, pp. 738–748, Jul. 2018.
[106] Z. Miao, C. Li, L. Zhu, X. Han, M. Wang, X. Cai, Z. Liu, and L. Xiong, "On resource management in vehicular ad hoc networks: A fuzzy optimization scheme," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, May 2016, pp. 1–5.
[107] S. Jiang, J. Liu, Y. Zhou, and Y. Fang, "FVC-Dedup: A secure report deduplication scheme in a fog-assisted vehicular crowdsensing system," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 4, pp. 2727–2740, Jul./Aug. 2022, doi: 10.1109/TDSC.2021.3069944.
[108] D. Cuong, N. H. Tran, and C. S. Hong, "Game theory for cyber security and privacy," Tech. Rep., May 2017.
[109] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacsar, and J. P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv. (CSUR)*, vol. 45, no. 3, pp. 1–39, 2013.
[110] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 472–486, 1st Quart., 2013.
[111] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 1, pp. 93–105, Jan. 2016.
[112] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 1st Quart., 2015.
[113] W. Zhang and G. Li, "An efficient and secure data transmission mechanism for Internet of Vehicles considering privacy protection in fog computing environment," *IEEE Access*, vol. 8, pp. 64461–64474, 2020.
[114] N. W. Lo and H. C. Tsai, "Illusion attack on VANET applications—A message plausibility problem," in *Proc. IEEE Globecom Workshops*, Nov. 2007, pp. 1–8.
[115] O. Nazih, N. Benamar, and M. Younis, "An evolutionary bargaining-based approach for incentivized cooperation in opportunistic networks," *Int. J. Commun. Syst.*, vol. 33, no. 9, pp. 1–17, Jun. 2020.
[116] L. Mendiboure, M.-A. Chalouf, and F. Krief, "Edge computing based applications in vehicular environments: Comparative study and main issues," *J. Comput. Sci. Technol.*, vol. 34, no. 4, pp. 869–886, Jul. 2019.
[117] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2017.
[118] W. Kim, "Evolutionary game for content cache in a mm-wave-based vehicular fog," *Electronics*, vol. 9, no. 11, p. 1794, Oct. 2020.
[119] B. Cho and Y. Xiao, "A repeated unknown game: Decentralized task offloading in vehicular fog computing," 2022, *arXiv:2209.01353*.
[120] Y. Li, B. Yang, H. Wu, Q. Han, C. Chen, and X. Guan, "Joint offloading decision and resource allocation for vehicular fog-edge computing networks: A contract-stackelberg approach," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 15969–15982, Sep. 2022.
[121] Z. Seyedi, F. Rahmati, M. Ali, and X. Liu, "Verifiable and privacy-preserving fine-grained data management in vehicular fog computing: A game theory-based approach," *Peer-Peer Netw. Appl.*, pp. 1–22, Dec. 2023.

[122] X. Chen, S. Leng, K. Zhang, and K. Xiong, "A machine-learning based time constrained resource allocation scheme for vehicular fog computing," *China Commun.*, vol. 16, no. 11, pp. 29–41, Nov. 2019.
[123] K.-H. Phung, H. Tran, T. Nguyen, H. V. Dao, V. Tran-Quang, T.-H. Truong, A. Braeken, and K. Steenhaut, "OneVFC—A vehicular fog computation platform for artificial intelligence in Internet of Vehicles," *IEEE Access*, vol. 9, pp. 117456–117470, 2021.
[124] S. Vemireddy and R. R. Rout, "Fuzzy reinforcement learning for energy efficient task offloading in vehicular fog computing," *Comput. Netw.*, vol. 199, Nov. 2021, Art. no. 108463.
[125] J. Shi, J. Du, J. Wang, and J. Yuan, "Deep reinforcement learning-based V2V partial computation offloading in vehicular fog computing," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2021, pp. 1–6.
[126] M. Rihan, M. Elwekeil, Y. Yang, L. Huang, C. Xu, and M. M. Selim, "Deep-VFog: When artificial intelligence meets fog computing in V2X," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3492–3505, Sep. 2021.
[127] V. Sethi and S. Pal, "FedDOVe: A federated deep Q-learning-based offloading for vehicular fog computing," *Future Gener. Comput. Syst.*, vol. 141, pp. 96–105, Apr. 2023.
[128] Z. Rejiba, X. Masip-Bruin, and E. Marín-Tordera, "Computation task assignment in vehicular fog computing: A learning approach via neighbor advice," in *Proc. IEEE 18th Int. Symp. Netw. Comput. Appl. (NCA)*, Sep. 2019, pp. 1–5.
[129] Y. Hou, Z. Wei, R. Zhang, X. Cheng, and L. Yang, "Hierarchical task offloading for vehicular fog computing based on multi-agent deep reinforcement learning," *IEEE Trans. Wireless Commun.*, early access, Aug. 21, 2023, doi: 10.1109/TWC.2023.3305321.
[130] H. Zhou, K. Jiang, S. He, G. Min, and J. Wu, "Distributed deep multi-agent reinforcement learning for cooperative edge caching in Internet-of-Vehicles," *IEEE Trans. Wireless Commun.*, vol. 22, no. 12, pp. 9595–9609, Dec. 2023.
[131] T. Wang, J. Zeng, M. Z. A. Bhuiyan, H. Tian, Y. Cai, Y. Chen, and B. Zhong, "Trajectory privacy preservation based on a fog structure for cloud location services," *IEEE Access*, vol. 5, pp. 7692–7701, 2017.
[132] P. Zhang, Y. Kong, and M. Zhou, "A novel trust model for unreliable public clouds based on domain partition," in *Proc. IEEE 14th Int. Conf. Netw., Sens. Control (ICNSC)*, May 2017, pp. 275–280.
[133] A. Alrawais, A. Alhothaily, B. Mei, T. Song, and X. Cheng, "An efficient revocation scheme for vehicular ad-hoc networks," *Proc. Comput. Sci.*, vol. 129, pp. 312–318, Jan. 2018.
[134] M. Bousselham, N. Benamar, and A. Addaim, "A new security mechanism for vehicular cloud computing using fog computing system," in *Proc. Int. Conf. Wireless Technol. Embedded Intell. Syst. (WITS)*, 2019, pp. 1–4.
[135] I. Corona, G. Giacinto, and F. Roli, "Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues," *Inf. Sci.*, vol. 239, pp. 201–225, Aug. 2013.

OSSAMA NAZIH received the master's degree from the National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco, in 2017, where he is currently pursuing the Ph.D. degree in mathematics and computer science. His research interests include resource allocation and resource management in VFC using game theory as a modelization approach.

NABIL BENAMAR received the master's and Ph.D. degrees from Moulay Ismail University, Meknes, Morocco, in 2001 and 2004, respectively. He is currently a Professor in computer science with the School of Technology, Moulay Ismail University, and an Adjunct Faculty Member of computer science with Al Akhawayn University, Ifrane, Morocco. He is the author of several journal articles and IETF standard documents. His research interests include future-generation networks, autonomous driving, the IoT, and TinyML. He is a member of the Tiny Machine Learning Open Education Initiative (TinyMLedu). He is also serving as an Associate Editor for IEEE Access journal and the *Journal of King Saud University—Computer and Information Sciences* (IF 8.8). He is a TPC Member of highly-ranked IEEE Flagship Conferences (GLOBECOM, ICC, PIMRC, and WCNC). He served as the Chair for the IEEE MenaComm'20 Conference and a member of the Organizing Committee for IEEE WCNC'2019 and IWCMC'23. He is an expert in internet governance. He was an ISOC Ambassador to IGF (2012 and 2013), a Google panelist in the first Arab-IGF, an ISOC Fellow to IETF'89&92&95&99&103, and an ICANN'50&54 Fellow. Among his international commitments, he is currently serving as the Chair for the Task Force for Arabic Script IDNs, a team of people working on the implementation of the Arabic script in the DNS root zone. He is also chairing the UASG measurement WG promoting the universal acceptance of all valid domain names and e-mail addresses.



HANANE LAMAAZI received the Ph.D. degree in computer sciences and networks from Moulay Ismail University, Meknes, Morocco, in 2018. From 2019 to 2022, she was a Postdoctoral Fellow with the Center for Cyber-Physical Systems, Khalifa University of Science and Technology, United Arab Emirates. She is currently an Assistant Professor with the College of Information Technology, United Arab Emirates University. Her research interests include the Internet of Things (IoT), RPL routing protocol, edge computing, crowdsensing, cybersecurity, and risk management. She is a TPC member at different scientific conferences. She is acting as an active reviewer of several highly reputed scientific journals. She was a guest speaker at several conferences.

HABIBA CHAOUI has been a Professor of Higher Education for 14 years, since 2009. She was the Leader of the Research Team "Data Analysis and Information Security." She occupied many roles at Ibn Tofail University, where she is the Director of Studies Head with the Department of Computer Science, Logistics, and Mathematics, and a Coordinator of the Research Master's Program in "Information Systems Security" and the MUS (University Specialized Masters) Program in "Mobile Technologies and Security."