Towards an Analysis of the Architecture, Security, and Privacy Issues in Vehicular Fog Computing

Mohammad Aminul Hoque and Ragib Hasan
SECRETLab, Department of Computer Science
University of Alabama at Birmingham
Birmingham, AL 35294, USA
{mahoque, ragib}@uab.edu

***Abstract*—The vehicular fog is a relatively new computing paradigm where fog computing works with the vehicular network. It provides computation, storage, and location-aware services with low latency to the vehicles in close proximity. A vehicular fog network can be formed on-the-fly by adding underutilized or unused resources of nearby parked or moving vehicles. Interested vehicles can outsource their resources or data by being added to the vehicular fog network while maintaining proper security and privacy. Client vehicles can use these resources or services for performing computation-intensive tasks, storing data, or getting crowdsource reports through the proper secure and privacy-preserving communication channel. As most vehicular network applications are latency and location sensitive, fog is more suitable than the cloud because of the capability of performing calculations with low latency, location awareness, and the support of mobility. Architecture, security, and privacy models of vehicular fog are not well defined and widely accepted yet as it is in its early stage. In this paper, we have analyzed existing studies on vehicular fog to determine the requirements and issues related to the architecture, security, and privacy of vehicular fog computing. We have also identified and highlighted the open research problems in this promising area.**

***Keywords*-Fog Computing; Vehicular Fog; Vehicular Cloud; Vehicular Network; Cloud Computing; Security; Privacy.**

I. Introduction

Modern vehicles are equipped with enormous computation and storage capabilities. They can perform a considerable amount of complex calculations and process the large amount of data generated from its sensors and GPS. Along with these improvements, the concept of vehicular networks is becoming popular. We posit that in near future, vehicles will be more interconnected and will increasingly share their resources to perform computation quickly and efficiently. For example, according to Gartner, 250 million cars will be connected to vehicular networks by 2020 [1]. With the emergence of capabilities, many systems related to vehicles, such as navigation, traffic management, and other location-aware systems will also become more intelligent. However, to implement these smart systems in real life in large scale, a lot of real-time data will be required to be processed to gain correct situational awareness. To achieve this, a large number of vehicles need to participate in the vehicular network and the massive amount of data generated from these vehicles need to be processed very quickly. Furthermore, vehicles need to perform tasks such as image processing and sensor data reading to make driving decisions continuously. For these cases, any kind of delay is not acceptable in the decision-making process as this may potentially lead to wrong decisions on the road.

Vehicular cloud computing is an attractive solution for these issues [2], [3]. In urban areas, a lot of vehicles are parked in parking areas during work hour. As a result, their storage and computation resources remain idle. Vehicular cloud computing is an idea to outsource these unused resources over the internet. User vehicles can access and use those resources through a wireless network for performing calculations, storing data, or offloading any application. Unfortunately, this approach does not give a real-life solution to the latency constraint as a lot of data is sent back and forth to a remote cloud server through the wireless network. There are several other issues with vehicular cloud paradigm such as it does not support mobility and location-awareness to serve the nearby vehicles.

Vehicular fog computing has been introduced recently to address these problems. Fog is a relatively new computing paradigm which was first presented by CISCO back in 2012 [4]. It is another computing layer between cloud and end devices which lies closer to the edge. Main idea behind fog is to perform the calculations at the edge of the network on the data received from edge devices and only send the summary to the cloud instead of sending the whole amount of data. Vehicular fog is using the idea of fog with vehicular networks where it will be generated on-the-fly using idle computation and storage resources of vehicles situated inside the vehicular network. Vehicular fog can be useful not only in processing the sensor data, crowdsourcing, or traffic management, but also in streaming and real-time applications where low latency and location awareness are required [5]. Currently, there is no widely accepted and well-defined architecture of the vehicular fog network. Researchers have proposed different architectural design keeping focus on various aspects such as the purpose of vehicular fog network, security & privacy, incentive model, quality of the service, and implementation of the system. As the architecture is still in its infancy, security and privacy issues have not been discussed extensively. It may deceptively seem that vehicular fog has similar security and privacy issues as

978-1-7281-0137-8/19/$31.00

other networks, but there are some issues which are entirely vehicular fog centric. Though fog can be considered as a low scale cloud situated in the edge of the network, it will have several unique security and privacy issues along with traditional problems of the cloud due to its nature. To give the researchers in this field a clear idea of the security issues in vehicular fog, we have analyzed the state-of-the-art research on vehicular fog architectures, security, and privacy. Based on our analysis, we have identified the requirements, issues, and open problems of vehicular fog network.

Contribution: The contributions of this paper are summarized below:

1) We have provided a high-level survey on the architecture, security, and privacy of vehicular fog computing.
2) We have identified the architectural, security and privacy requirements, and challenges in vehicular fog computing.
3) Finally, we have analyzed the contributions of existing works to discover research gaps and thereby identify open problems.

Organization: The rest of the paper is organized as follows: Section II contains details of vehicular fog and its architecture. Section III is about architecture, security, and privacy requirements and issues. Section IV includes an evaluation of the existing system based on several criteria. Section V highlights the open problems as we end with conclusions in section VI.

II. Vehicular fog and applications

A. Conceptual Overview

Vehicular fog is a particular type of fog computing system which is formed on-the-fly by using the underutilized resources of vehicles in close proximity. Interested vehicles can outsource their unused onboard unit (OBU) resources to nearest vehicular fog network or can work as the source of crowdsourcing information in exchange for some incentive. User vehicles can use those resources or services on demand for various purposes such as processing the sensor data, getting crowdsourcing or crowdsensing reports, and offloading applications or tasks. There is usually a controller node in this architecture which is responsible for maintaining the available resources and assigning them according to requirements of the requests. Controller node is also responsible for ensuring the security and privacy of the whole architecture. Figure 1 gives an overview of vehicular fog computing architecture.

Potential services of vehicular fog computing are listed as follows:

Information as a service: Vehicular fog network can work as the source of many real-time scenarios such as traffic congestion, road surface condition, and many important events or emergency situations [6].

Entertainment as a service: Vehicular fog architecture can be used for video streaming or computation intensive gaming services where it works as entertainment as a service.

Storage as a service: Vehicles have a lot of storage capabilities in its onboard device. Especially for parked vehicles, this storage capability is completely unused. These storages can be outsourced to meet the requirements of other client vehicles to run applications or tasks which require a higher amount of storage.

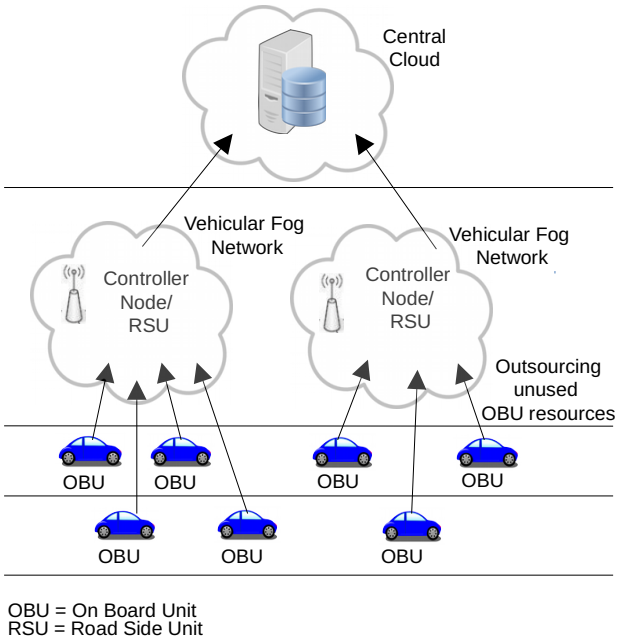

Fig. 1: Vehicular Fog Architecture

Computation as a service: A huge amount of onboard computation power remains unused during several hours each day when vehicles are parked. This computation power can be outsourced to vehicular fog network and can be used by the vehicles who need more computation resources for performing complex tasks.

B. Potential Applications of Vehicular Fog Computing

Occurance reporting: Accidents on the road is a very common incident. Vehicular fog can inform about the accident and possible congestion in quick time to proper authority and other potential users of the road. This can also help to find out who is responsible for the accident. Again, the parked vehicles which are connected as fog nodes in vehicular fog network can report any nearby vehicle theft incident.

Resource outsourcing: Underutilized or unused resources of a vehicle are outsourced to the vehicular fog network. For example, parked vehicles can let their resources to be used by other vehicles on demand.

Traffic management: One of the potential usages of vehicular fog architecture is traffic management. A vehicle can report its speed, location, sensor reports and video to the nearest vehicular fog network. Available fog resources can analyze this data, and a further decision can be taken from that by the traffic control management system. This is a highly latency-sensitive use case, and a vehicular fog is suitable in this case to deliver the decision quickly [5].

Vehicular crowdsourcing: Crowdsourcing is sending data to fog network to get better situational awareness by analyzing the data. Crowdsourcing data may come from video, sensors,

or GPS of participating vehicles. There are several proposed use cases for vehicular crowdsourcing using vehicular fog architecture. Zhu *et al.* [7] proposed a scheme of video crowdsourcing. Authors of [8] talked about some applications of vehicular crowdsourcing such as parking navigation, road surface monitoring, and traffic collision reconstruction. Other research on vehicular crowdsourcing includes the navigation scheme [9], route sharing [10], and road surface monitoring [11].

Carpooling: Carpooling is broadcasting the destination and route of a vehicle so that people willing to go the same way can find each other. The goal is to reduce the congestion of vehicles during peak hour. Vehicular fog can be useful in this context. Authors of [12] proposed a privacy-preserving carpooling scheme named FICA in vehicular fog computing using blockchain technology.

Driving Assistance: Vehicles can outsource the sensor, GPS, and video data to fog network for analyzing and get the instruction about the next decision very quickly. Also, fog network can inform the vehicles about accidents and congestion on routes towards the destination. According to this information, drivers can adjust their routes. There are several navigation schemes available based on GPS, such as google maps. But they take some time to update the system and give information about accidents and congestion. But vehicular fog will work faster in these cases.

Here, we have discussed only a limited number of use cases of vehicular fog. However, this paradigm can be used with any latency sensitive and location-aware system.

III. Architecture, Security, and Privacy of Vehicular Fog

As vehicular fog is a relatively new computing paradigm, the security and privacy issues are mostly unexplored. Here, we present several architectural, security, and privacy issues of vehicular fog computing. First, we will discuss the architectural, security, and privacy requirements and then we will continue with issues and potential defenses or mitigation strategies.

A. Architecture, Security and Privacy Requirements

1) Architectural requirements:

Low latency: To implement the vehicular fog network in a large scale traffic management system, all the calculation results should be available in very short time. So, low latency is one of the primary architectural requirements in a vehicular fog computing system.

Better quality of service: Quality of service largely depends on how quickly and correctly the vehicular fog network can respond to the query, computation or other service requests. So the tasks should be assigned to the available resources in such a way that can satisfy the delay requirements of heterogeneous applications and make proper use of variable computation resources. The architecture should make sure the maximum and efficient use of available resources.

Incentive/pricing model: Vehicular fog architecture should have a proper incentive model depending on the computation capability or resource availability of a vehicle which is willing to join as fog node. This is necessary to make people interested in letting their vehicle used in vehicular fog network as server fog node or source of crowdsourcing.

Mobility of fog nodes: One of the significant properties that differentiates vehicular fog from the other computing paradigms is the mobility of server fog nodes. Here, moving vehicles can join as fog nodes along with the stationary nodes (such as parked vehicles). Due to mobility, the moving vehicles can go out or join a fog network at any time. Even this may happen while performing a computation or any other task. So, the vehicular fog architecture should consider all the different scenarios for both moving and stationary vehicles.

2) Security requirements:

Confidentiality: Confidentiality is very important in vehicular fog computing. [13] [5] No one in the middle should intercept the message or data sent by any vehicle or vehicular fog entity before the receiver receives it. Any such unauthorized access should be detected and prevented [5]. Public or symmetric key encryption can be implemented to achieve the required confidentiality.

Integrity: Any message passed within vehicular fog network should not be modified or tampered by any third party or malicious entity. To ensure integrity, any change in the message should be detected along with the specific change. [13] [5]

Authentication: Every time a server fog node joins the vehicular fog network, it should be authenticated. There should also be an authentication system for the client vehicles who request for services to the vehicular network.

Location validation: To take part in vehicular crowdsourcing or crowdsensing, a vehicle must be present in that location. Validation of the location should be performed so that no vehicle can pretend that they are present in that place without actually being presented there and gain money in this fraudulent way.

Authorization and access control: After getting into the vehicular fog network, an entity must be authorized and have access to perform an action. Proper access control mechanism should be implemented to prevent unauthorized activity.

Non-repudiation: Non-repudiation should be implemented so that a user can verify the sender of any message and the sender cannot deny after sending a message. [13] Here, the message may be application offloading request or result, data for crowdsensing or crowdsourcing, etc.

Availability: The service of vehicular fog network should be available all the time. There should be proper protection mechanism against availability attacks such as denial of service.

Reliability: We must handle reliability of services of vehicular fog structure such as correctness of computation, the capability of storage, and correctness of crowdsourcing reports. [13]

Forensics: Forensics is always a major challenge. Forensic analysis is difficult to perform in cloud computing as well as fog computing. There should be a proper way to find out the evidence of an incident from the components or resources of participating vehicles.

3) Privacy requirements:

Vehicle information privacy: During crowdsourcing or application offloading, related information about the vehicle need to be sent to the vehicular fog network such as registration information or vehicle health. But these information must be kept private and should not be intercepted or revealed to any malicious entity.

Personal information privacy: Personal information of the driver such as name and driving license information should not be revealed in the vehicular fog network.

Location privacy: Current location and destination route information of participating vehicles should be preserved so that nobody can intentionally follow a vehicle.

B. Architecture, Security, and Privacy Issues

1) Architectural issues:

Fight with latency and quality of service: There is a trade-off between latency and quality of service as both of them are related to each other. Any communication or computation overhead will increase the latency. For example, cryptographic solutions are needed to ensure privacy and security. But they will add some computation overhead and thus increase latency, which will eventually reduce the quality of service.

Optimization of resource allocation: The available resources must be allocated optimally among the entities who request for services. Allocating the available resources optimally is a challenge because the resources and requirements will be heterogeneous. Zhu *et al.* [14] proposed a scheme named Fog Following Me which optimizes latency and quality by designing task allocation algorithm in vehicular fog computing. They have formulated a joint optimization problem by considering latency, quality loss, and fog capacity of both the stationary and mobile fog nodes. Lin *et al.* [15] provided another resource allocation optimization solution where the bandwidth is allocated optimally in vehicular fog network.

Optimization of application offloading: In a vehicular fog network there will be heterogeneous delay requirements in different offloaded applications. Some task will ask results in very short time and some will allow little more time. Again, the computation and storage resources of fog server vehicles will vary. The limited service area of a fog server and high mobility of vehicles make the task even harder. So, optimizing the task distribution among available resources is a huge challenge.

Application migration: Due to the high mobility of fog nodes, task migration is an obvious thing in vehicular fog architecture. Migration can be required in several scenarios. If a server fog node goes out of the range of the network while performing a calculation or some other task, then the controller of the fog network needs to reassign the task to some other available resource. Again, a user vehicle may go out of the fog network after offloading a task which is yet to finish. In that case, the task needs to be migrated to another vehicular fog network which comes along the route of that vehicle. Not only the task should be migrated to another available and capable node, but also this migration process should be performed smoothly for the better quality of service. For a smooth and seamless transition, the whole process can be started earlier than the required moment. Memon *et al.* [16] proposed a machine learning based task handover mechanism for vehicular fog environment.

2) Security and Privacy Issues:

Preserving privacy of information: Different privacy attacks are possible in vehicular fog scheme. Attackers can extract information about vehicles such as speed, location, health, and destination from offloaded data to vehicular fog network. Also, the attacker may follow a particular vehicle based on the data it provides. Here, the attacker may be any curious entities such as fog providers, vehicles or external attackers.

To mitigate this issue, any information about the identity of the vehicle cannot be revealed while using vehicular fog network. One possible solution is to anonymizing the identity of participating vehicles. Kang *et al.* [17] designed a scheme named p3 for vehicular fog which is a context-aware and privacy-preserving pseudonym scheme. Data aggregation is also discussed as a potential solution proposed by some research works. Kong *et al.* [18] proposed a verifiable and privacy-preserving querying scheme on data aggregation.

Authentication and authorization: Vehicular fog network topology always changes due to the mobility of fog nodes. A fog node may join or leave the network any time and it makes the authentication problem much harder. A lot of misuses may occur if proper authentication is not performed. In vehicular crowdsourcing, malicious users may send false reports to make the users confused and eventually make wrong decisions. Crowdsensing attacks can be divided into impersonation attacks and sybil attacks. Again, improper authentication may lead to the bogus message and message alteration attacks [19]. In bogus message attack, the user sends wrong information through the network. If proper authenticity of the information is not justified, it will lead to giving erroneous results to the users. Message alteration attack is modifying the message when passing through a node. This is a direct attack on message integrity.

Unauthorized access may lead to some potential issues. An unauthorized fog node may enter into the network pretending to be some other user and use the service where the system will eventually charge the infected user.

Obstacles: In the vehicular network, trust establishment is performed by observing the behavior of neighboring nodes and passing messages with them. But if there are obstacles between them, then None Line Of Sight (NLOS) situation occurs [20]. This will eventually hamper the trust establishment as the communication and monitoring process will be disturbed.

Availability and man-in-the-middle attacks: A fog node can be compromised to an attacker and may become unavailable to serve. Also, a fake user can request a lot of resources to make the vehicular fog structure out of the resources. Again, an attacker can intercept or change a message through man-in-the-middle attack in vehicular fog network.

IV. Analysis and Comparison of Existing Schemes

We have divided the existing research works into three sections based on the scope. Those scopes are: architectural design, resource allocation & application offloading, and crowdsourcing & data dissemination. All the research works are evaluated based on the architectural and security requirements discussed earlier. Specific criteria that we considered for evaluation are latency and Quality of Service (QoS), the mobility of fog nodes, authentication, authorization, confidentiality, integrity, non-repudiation, and location validation. We see that most of the research work either proposed an architectural design or tried to solve security and privacy issues. However, there are some research works which introduced privacy-preserving architectural designs that covered both architectural and security requirements. Table I gives the overview of existing research works on vehicular fog which are evaluated based on the above criteria.

A. Vehicular fog architectural designs

Hou *et al.* [21] have proposed vehicular fog infrastructure design by considering both parked and moving vehicles. They have considered latency, quality of service, and mobility of fog nodes but did not propose anything related to security of the infrastructure.

Huang *et al.* [5] analyzed architecture, use case, security, and forensic challenges in vehicular fog computing. They have also discussed a potential compromise attack on fog based traffic control system. Some countermeasures against the attack have also been proposed. One of them is an evidence-based forensic approach which is observing abnormal behavior of vehicles or nodes. Another countermeasure is traffic based analysis approach where historical traffic data is analyzed to detect deviation from normal behavior using big data analytics and deep learning algorithms.

Yao *et al.* [13] proposed reliable and secure vehicular fog service provision by designing three-layered architecture with a trusted authority (TA) in the top, RSUs in the middle and vehicles in the bottom layer. TA controls all the vehicular fog structures (VFS) where each VFS is constructed centering one RSU. They considered the mobility of fog nodes and solved the security and privacy issues such as reliability, confidentiality, integrity, and non-repudiation with cryptographic solutions. Here, privacy, location verification, and authorization or access control were not considered.

Wei *et al.* [22] designed a vehicular fog framework for crowdsourcing based road surface condition monitoring. They ensured privacy by imposing anonymity and forward privacy. Cryptographic solutions also provide authentication, integrity, and non-repudiation. But authors did not consider the issues about latency, mobility, location validation, and authorization or proper access control.

B. Resource allocation & application offloading

Zhu *et al.* [23] proposed a scheme named Folo which is basically a latency and quality optimized task allocation scheme in vehicular fog computing. This paper has considered both the stationary and mobile fog nodes. Considering latency, quality loss, and fog capacity, authors have formulated a joint optimization problem. The problem has been presented as a bi-objective minimization problem, where there is a trade-off between latency and quality loss. A dynamic task allocation (DTA) framework was proposed where initially the client vehicle discovers the fog nodes within its communication range by broadcasting one-hop prob messages through DSRC. Then client vehicle sends task offloading request which is finally assigned to a fog node by zone head after running the task allocation algorithm. Authors did not consider the security aspects in this scheme.

Lin *et al.* [15] proposed an optimized bandwidth allocation scheme in vehicular fog network. They mainly focused on the latency, quality of service, and mobility. But this is not a privacy-preserving scheme, so it doesn't meet the security and privacy related criteria.

Wang *et al.* [24] proposed an application aware offloading policy considering both heterogeneous application delay requirements and availability of variable computation resources (dynamic topology of vehicular networks). A priority queuing system is applied to model the VFCS to achieve efficient offloading using the semi markov decision process (SMDP). Authors have considered public service vehicles, such as buses, as the fog servers as they have relatively fixed routes and time schedules. These server buses can extend the link duration with the requester if the relative mobility matches. The center of VFCS is called computing scheduler (CS). A fog server is assigned by the CS upon request and result is returned to the CS and then sent back to requester. It has proposed to send low priority tasks to send remote cloud server if no resource is available. This paper has also considered the incentive/pricing model such as if departure rate increases, then reward decreases.

Klaimi *et al.* [25] proposed a scheme for resource management with available heterogeneous resources and quality of service requirements. Authors have claimed that the approach doesn't introduce much overhead and hence latency & QoS is not hampered. This scheme has met all the security requirements except authorization and non-repudiation.

Wang *et al.* [26] designed a contract-based resource allocation framework to reduce the latency by designing an effective incentive mechanism to attract nearby vehicles to participate. As the quality of service and quality of expectation can be hampered during the peak time, authors have designed a well-structured contract of incentive and broadcast the contracts to let the interested vehicle choose the favorable one to maximize the payoff.

C. Crowdsourcing & data dissemination

PROS [10] is a privacy-preserving route-sharing scheme. Here authors considered different related attacks such as group affiliation attack, member impersonation attack, and unlimited participation attack and proposed the scheme to mitigate those attacks. This scheme meets all the security criterion except non-repudiation and location verification.

TABLE I: Analysis of Existing Research on Vehicular Fog Systems

Scope	Paper/ Scheme	Major Contribution	Criteria								
			Latency & QoS	Mobility	Authentication	Authorization	Confidentiality	Integrity	Non-repudiation	Privacy	Location Verification
Architectural Design	Hou *et al.* [21]	Proposed a vehicular fog infrastructure design considering both parked and moving vehicles.	✓	✓	×	×	×	×	×	×	×
	Huang *et al.* [5]	Analyzed architecture, use case, security, and forensic challenges in vehicular fog computing.	×	×	✓	✓	✓	✓	✓	×	×
	Yao *et al.* [13]	Proposed a reliable and secure vehicular fog service provision by designing a three-layered architecture.	✓	✓	✓	×	✓	✓	✓	×	×
	Wei *et al.* [22]	Designed a vehicular fog crowdsourcing framework ensuring privacy by imposing anonymity and forward privacy.	×	×	✓	×	✓	✓	✓	✓	×
Resource Allocation & Application Offloading	Chao *et al.* [23]	Proposed a latency and quality of service optimized task allocation scheme for vehicular fog computing.	✓	✓	×	×	×	×	×	×	×
	Zhu *et al.* [14]	Proposed a latency and quality of service balanced task allocation scheme for vehicular fog computing.	✓	✓	×	×	×	×	×	×	×
	Lin *et al.* [15]	Designed an optimized bandwidth allocation scheme for vehicular fog network.	✓	✓	×	×	×	×	×	×	×
	Memon *et al.* [16]	Proposed a machine learning based task handover mechanism for vehicular fog environment.	✓	✓	×	×	×	×	×	×	×
	Wang *et al.* [24]	Proposed application aware offloading policy considering heterogeneous delay requirements and availability of variable computation resources.	✓	✓	×	×	×	×	×	×	×
	Klaimi *et al.* [25]	Designed a scheme for managing resources with different quality of service requirements and availability of heterogeneous resources.	✓	✓	×	×	×	×	×	×	×
	Wang et al. [26]	Designed a contract-based resource allocation framework for latency reduction with an effective incentive mechanism.	✓	✓	×	×	×	×	×	×	×
Crowdsourcing & data dissemination	PROS [10]	This is a privacy preserving route sharing scheme where authors considered different attack scenarios and designed the scheme to prevent these attacks.	×	×	✓	✓	✓	✓	×	✓	×
	Zhu *et al.* [7]	Authors have analyzed applications, feasibility, and challenges of vehicular fog based video crowdsourcing by performing simulations.	✓	✓	×	×	×	×	×	×	×
	Soleymani *et al.* [19]	Designed a model for ensuring correctness of crowdsourced data.	×	✓	✓	✓	✓	✓	×	×	✓
	REPTAR [27]	REPTAR is a scheme designed to transmit and process the sensing data.	✓	✓	×	×	×	×	×	×	×
	Kong *et al.* [18]	Designed a privacy-preserving and verifiable crowdsourcing querying scheme based on data aggregation.	×	×	✓	✓	✓	✓	✓	✓	×
	Ullah *et al.* [28]	Proposed an emergency message dissemination scheme based for vehicular fog computing and VANET based on congestion avoidance scenario.	×	×	×	×	✓	✓	✓	✓	×
	Ni *et al.* [8]	Authors have analyzed several schemes for maintaining security and privacy in vehicular crowdsensing.	×	×	✓	✓	✓	✓	✓	✓	×
	Wang *et al.* [9]	Designed a secure navigation scheme using different cryptographic algorithms.	×	×	✓	×	✓	×	×	✓	×
	FICA [12]	Proposed privacy-preserving carpooling scheme for vehicular fog computing using blockchain technology.	✓	×	✓	×	✓	✓	×	✓	✓
	DFCV [29]	Designed a scheme for dynamic fog which will be generated on-the-fly, incremented, and destroyed depending on the necessity of communication.	✓	✓	×	×	×	×	×	×	×
	Basudan *et al.* [11]	Designed privacy-preserving road surface condition monitoring system by vehicular crowdsensing using vehicular fog computing.	✓	×	✓	×	✓	✓	×	✓	×

Zhu *et al.* [7] examined applications, feasibility, and challenges of vehicular fog based video crowdsourcing. They have performed simulation in SUMO and VenisLTE using dedicated short-range communication (DSRC) and LTE technologies. Here, DSRC is responsible for data transmission between client vehicles and client fog nodes. On the other hand, LTE is used to send data from vehicular fog node to cellular fog node. Authors have found several issues such as interference in communication, service interruption, and resource management. This is a study based on architectural feasibility and does not contain security related discussions.

Soleymani *et al.* [19] proposed a trust model to ensure correctness of received data as well as overcoming the interruption caused by obstacles between the nodes. Authors have considered mobility and all security & privacy aspects except non-repudiation.

REPTAR [27] is a scheme to transmit and process sensing data where authors have considered latency, quality of service, and mobility but did not discuss the issues related to security.

Kong *et al.* [18] proposed a verifiable and privacy-preserving querying scheme on data aggregation. Here, data is disseminated from roadside units upon querying. Here the road side units work as fog storage devices. In this scheme, multiple data requests are aggregated by encrypting with homomorphic Pilier Cryptosystem, and individual requests are recovered later without knowing vehicle identity.

Ni *et al.* [8] proposed some schemes for maintaining security and privacy in vehicular crowdsensing. One scheme is secure tasking and reporting by proxy re-encryption and searchable encryption. Others are privacy preserving navigation scheme by obtaining anonymous credentials and finally secure and deduplicated crowdsensing.

Wang *et al.* [9] proposed a navigation scheme which ensures security and privacy. Authors used some cryptographic algorithms such as Elgamal encryption algorithm, AES, group signatures, and anonymous credentials to implement the system. This scheme ensures authentication, confidentiality, and privacy.

DFCV [29] is a scheme for dynamic fog which will be generated on the fly, incremented and destroyed depending on the necessity of communication. This scheme mainly focuses on resource utilization, lower latency, and packet loss.

Except the research works on vehicular fog system focusing on different scopes, some works are directly dedicated to security enhancement. These works have focused on specific security and privacy issues and proposed solutions of them.

Lin *et al.* [30] proposed a secure and privacy-preserving communications scheme in vehicular networks named GSIS. The scheme provides security, privacy, and traceability based on group and identity-based signature techniques.

Kang *et al.* [17] proposed a context-aware and privacy-preserving pseudonym scheme named p3 for vehicular fog network. The three-layered architecture works together to change the pseudonym based on context by managing and distributing the pseudonyms through proper communication protocols. Though the scheme provides privacy for participating vehicles, it is not clear how well the introduced overhead will suit with vehicular fog structure and how the vehicles will be charged or given incentive for their participation.

V. Open problems in vehicular fog

We have identified several open problems of vehicular fog computing based on our analysis of existing research. Table II gives a summary of the highlighted open problems. Details of the open problems are discussed below.

Mobility model for the vehicles: The mobility model for vehicular fog computing paradigm is not well defined [21]. As the vehicles move with varying speed, the distance between them changes continuously. Also, a fog node may go out of the range of vehicular fog network even while performing a task. Moreover, speed of the vehicle may be so high that it may be inefficient to consider it as server fog node. Also, there should be some protocols and management mechanisms to connect the moving or parked vehicles with vehicular fog networks. How these situations will be handled is not clear yet.

Capacity analysis and managing resources: Better algorithms and protocols are needed to analyze the capacity of vehicular fog structure properly. Capacity analysis is essential for task allocation and recomposition problems as well as managing the resources efficiently.

Scaling: Usage of the vehicular fog network will not be same all around the day. During peak hours, the task offloading requests and other resource requirements will be higher. So, it will be challenging to scale the vehicular fog system according to the demand. There may be some time periods when enough storage or computation resource will not be available due to a lack of participant vehicles as server fog nodes. In that case, how the requests will be handled needs more research attention.

System implementation: Vehicular fog and its various components are still bound in theoretical discussions. The system implementation details need more research focus.

Pricing and incentive model: No proper incentive and pricing model have been designed for vehicular fog. An incentive model is necessary to attract vehicles with underutilized and unused resources to take part. Incentive model should reflect the amount and quality of available resources of the interested vehicle. Again, user vehicles need to pay for using the services of vehicular fog. Wang *et al.* [26] proposed an incentive model for contract based resource allocation. Wang *et al.* [24] proposed another incentive model along with optimized application offloading mechanism where incentive amount increases if departure rate decreases and vice versa. However, more research is needed in this context.

Security and forensics: From our analysis of existing research, we have observed that security and forensics issues are not discussed extensively in vehicular fogs. Most of the security and privacy issues can be solved by using cryptographic solutions but they will add some computation overhead. So the feasibility of using cryptographic solutions needs more research attention. A few research works have focused on security and privacy issues, but forensics issues are still mostly unexplored.

Interference in communication: During peak hour, there may be a lot of vehicles in a vehicular fog network. Therefore, the

TABLE II: Summary of open problems

Problem	Summary
Mobility model	Need proper protocols for entering and leaving vehicular fog network.
Capacity analysis & managing resources	Need better algorithms and protocols for real time capacity analysis and resource management.
Scaling	Proper scaling has to be done based on usage of resources in different times of a day.
System implementation	Actual system or prototype implementation of vehicular fog has not been done yet.
Pricing & incentive model	Pricing and incentive models are needed to be designed based on the resources used or outsourced.
Security & forensics	Proper security protocols and forensic analysis schemes are required for the participating vehicles.
Interference in communication	Increasing number of communication channels in vehicular fog network may result into interference.

number of V2V communication channel will rise, and as a result, vehicular interference will increase packet loss rate [7]. How this packet loss rate can be decreased is a potential research area in vehicular fog.

VI. Conclusion

The vehicular fog is an exciting prospect for latency-sensitive and location-aware applications and systems in close proximity. This can be formed on-the-fly by using the underutilized and unused resources of both parked and moving vehicles. While it can help to solve a lot of problems that the traditional vehicular clouds cannot solve, there are still a lot of research questions that must be explored. We have analyzed the requirements of vehicular fog in this paper and identified the architectural, security, and privacy challenges. We have also presented the open problems in this domain so that researchers can focus their attention on solving such problems.

Acknowledgments

This research was supported by the National Science Foundation through awards DGE-1723768, ACI-1642078, and CNS-1351038.

References

[1] Gartner, "The future of connected cars." [Online]. Available: http://www.gartner.com/newsroom/id/2970017

[2] M. Abuelela and S. Olariu, "Taking vanet to the clouds," in *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*. ACM, 2010, pp. 6 – 13.

[3] S. Olariu, M. Eltoweissy, and M. Younis, "Towards autonomous vehicular clouds," *EAI Endorsed Transactions on Mobile Communications and Applications*, no. 1, pp. 1–11, 2011.

[4] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *MCC workshop on Mobile cloud computing*. ACM, 2012, pp. 13–16.

[5] C. Huang, R. Lu, and R. Choo, "Vehicular fog computing: Architecture, use case, and security and forensic challenges," in *IEEE Communications Magazine*, vol. 55. IEEE, 2017, pp. 105–111.

[6] M. Sookhak, R. Yu, Y. He, H. Talebian, N. S. Safa, N. Zhao, M. K. Khan, and N. Kumar, "Fog vehicular computing: Augmentation of fog computing using vehicular cloud computing," in *IEEE Vehicular Technology Magazine*, vol. 12. IEEE, 2017, pp. 55–64.

[7] C. Zhu, G. Pastor, Y. Xiao, and A. Ylajaaski, "Vehicular fog computing for video crowdsourcing: Applications, feasibility, and challenges," in *IEEE Communications Magazine*, vol. 56. IEEE, 2018, pp. 58–63.

[9] L. Wang, G. Liu, and L. Sun, "A secure and privacy-preserving navigation scheme using spatial crowdsourcing in fog-based vanets," vol. 17. Sensors, 2017.

[8] J. Ni, A. Zhang, X. Lin, and S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," in *IEEE Communications Magazine*, vol. 55. IEEE, 2017, pp. 146–152.

[10] M. Li, L. Zhu, Z. Zhang, X. Du, and M. Guizani, "Pros: A privacy-preserving route-sharing service via vehicular fog computing," in *IEEE Access*, vol. 6. IEEE, 2018, pp. 66 188 – 66 197.

[11] S. Basudan, X. Lin, and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing," in *IEEE Internet of Things Journal*, vol. 4. IEEE, 2017, pp. 772 – 782.

[12] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," in *IEEE Internet of Things Journal*. IEEE, 2018.

[13] Y. Yao, X. Chang, J. Misic, and V. B Misic, "Reliable and secure vehicular fog service provision," in *IEEE Internet of Things Journal*. IEEE, 2018.

[14] C. Zhu, G. Paster, Y. Xiao, and A. Yale-Jaeaeski, "Fog following me: Latency and quality balanced task allocation in vehicular fog computing," in *2018 15th Annual IEEE Internation Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 2018.

[15] F. Lin, Y. Zhou, G. Pau, and M. Collotta, "Optimization-oriented resource allocation management for vehicular fog computing," in *IEEE Access*, vol. 6. IEEE, 2018, pp. 69 294 – 69 303.

[16] S. Memon and M. Maheswaran, "Using machine learning for handover optimization in vehicular fog computing," 2018.

[17] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 19. IEEE, 2018, pp. 2627–2637.

[18] Q. Kong, R. Lu, M. Ma, and H. Bao, "A privacy-preserving and verifiable querying scheme in vehicular fog data dissemination," in *IEEE Transactions on Vehicular Technology*. IEEE, 2018.

[19] 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 fuzzy logic in vehicular ad hoc networks with fog computing," in *IEEE Access*, vol. 5. IEEE, 2017, pp. 15 619–15 629.

[20] O. Abumansoor and A. Boukerche, "Towards a secure trust model for vehicular ad hoc networks services," in *2011 IEEE Global Telecommunications Conference - GLOBECOM 2011*. IEEE, 2011.

[21] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, "Vehicular fog computing: A viewpoint of vehicles as the infrastructure," in *IEEE Transactions on Vehicular Technology*, vol. 65. IEEE, 2016, pp. 3860–3873.

[22] J. Wei, X. Wang, N. Li, G. Yang, and Y. Mu, "A privacy-preserving fog computing framework for vehicular crowdsensing networks," in *IEEE Access*, vol. 6. IEEE, 2018, pp. 43 776 – 43 784.

[23] C. Zhu, J. Tao, G. Pastor, Y. Xiao, Y. Ji, Q. Zhou, Y. Li, and A. Yla-Jaaski, "Folo: Latency and quality optimized task allocation in vehicular fog computing," in *IEEE Internet of Things Journal*. IEEE, 2018.

[24] Z. Wang, Z. Zhong, and M. Ni, "Application-aware offloading policy using smdp in vehicular fog computing systems," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2018.

[25] J. Klaimi, S.-M. Senouci, and M.-A. Messous, "Theoretical game approach for mobile users resource management in a vehicular fog computing environment," in *2018 14th International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2018.

[26] Y. Wang, C. Xu, Z. Zhou, H. Pervaiz, and S. Mumtaz, "Contract-based resource allocation for low-latency vehicular fog computing," in *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2018.

[27] B. Wang, Z. Chang, Z. Zhou, and T. Ristaniemi, "Reliable and privacy-preserving task recomposition for crowdsensing in vehicular fog computing," in *2018 IEEE 87th Vehicular Technology Conference*. IEEE, 2018.

[28] A. Ullah, S. Yaqoob, M. Imran, and H. Ning, "Emergengy message dissemination schemes based on congestion avoidance in vanet and vehicular fog computing," in *IEEE Access*, vol. 7. IEEE, 2018, pp. 1570 – 1585.

[29] A. Paranjothi, M. S. Khan, and M. Atiquzzaman, "Dfcv: A novel approach for message dissemination in connected vehicles using dynamic fog," 2018.

[30] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications," in *IEEE Transactions on Vehicular Technology*, vol. 56. IEEE, 2007, pp. 3442 – 3456.