Wireless Pers Commun (2015) 83:1131–1158
DOI 10.1007/s11277-015-2442-y

A Paradigm Shift from Vehicular Ad Hoc Networks to VANET-Based Clouds

Rasheed Hussain · Zeinab Rezaeifar · Heekuck Oh

Published online: 27 February 2015

Abstract Vehicular ad hoc network (VANET) is expected to improve our driving experience through enhanced safety, security, robustness, and infotainment. Nevertheless, despite considerable amount of research, VANET did not make it, at least not on a full scale, to the deployment stage because of many issues including security and privacy. However it is speculated that in the future high-end vehicles, on-board computation, communication, and storage resources will be under-utilized. Therefore, recently a new paradigm shift from conventional VANET to vehicular cloud computing was envisioned. This paradigm shift was realized through merging VANET with revolutionary cloud computing. Clearly cloud computing is one of today's tempting technology areas due, at least partially, to its virtualization and cost-effectiveness. However, to date the potential architectural framework for VANET-based cloud computing has not been defined so far. To fill this gap, in this paper, first we put forth the taxonomy of VANET based cloud computing and then define a communication paradigm stack for VANET clouds. Additionally we divide VANET clouds into three architectural frameworks namely vehicular clouds (VC), vehicles using clouds (VuC), and hybrid vehicular clouds (HVC). Each proposed framework provides particular set of services depending upon the underlying communication paradigm. To understand our proposed framework well, we also propose a novel use-case service of the VANET-based cloud namely traffic information dissemination through clouds. In the proposed scheme, vehicles moving on the road are provided with fine-grained traffic information by the cloud as a result of their cooperation with the cloud infrastructure. Vehicles share their frequent mobility dynamics with the cloud and cloud in turn provides them with long range traffic information based on their current and

R. Hussain · Z. Rezaeifar · H. Oh (✉)
Department of Computer Science and Engineering, Hanyang University, ERICA Campus, Sa 3-dong, Sangnok-gu, Ansan, Gyeonggi 426-791, South Korea
e-mail: hkoh@hanyang.ac.kr

R. Hussain
e-mail: rasheed@hanyang.ac.kr

Z. Rezaeifar
e-mail: zeinab.rezaiefar@gmail.com

near-future locations. Our simulation results show that the traffic information dissemination through cloud is feasible and the vehicles receive above 83 % of the traffic information from clouds through gateways in worst-case scenarios (i.e. extensive dense traffic) and above 90 % traffic information in average case scenarios. Finally we also outline the unique security and privacy issues and research challenges in VANET clouds.

Keywords VANET · Cloud computing · VANET clouds · Security and privacy · VANET cloud architecture · Traffic information dissemination

1 Introduction

Until fairly recently, it was a foreseen dream to connect the fleet of consumer vehicles on the road in a way where vehicles can talk to each other and exchange information. The basic idea of vehicular ad hoc network (VANET) is to take the widely adopted and inexpensive wireless local area network (WLAN) technology, with a few tweaks, and install it on vehicles for cooperative communication. However if it was so simple just to migrate the existing technology from simple WLAN to vehicles, research community including academia and consortia would never produce remarkable results after gigantic amount of brainstorming [1]. Nevertheless, despite the remarkable research results achieved in VANET, security and privacy issues have been the root cause of, at least in part, keeping the stakeholders at the bay from investing in VANET deployment. The complete deployment of VANET is still rapidly ahead and its success and adaptation in end-users (drivers), consumers, and governments will depend on viable security solutions, quality of services, and consumers' satisfaction [2–5]. One of the many goals of VANET is to support traffic safety and make the driving experience more safe, comfortable, and infotainment-rich. In VANET, vehicles and road-side units (RSUs), i.e., network nodes, will be equipped with on-board computation and communication modules to enable fruitful communication among them. Abstractly, there are two kinds of communication paradigms in VANET called vehicle-to-vehicle (V2) and vehicle-to-infrastructure (V2I) communication paradigms [6, 7]. V2 communication paradigm is also called '*Zero Infrastructure*' because the communication pattern is fully ad hoc and no additional infrastructure is needed. On the other hand, V2I communication paradigm demands static and/or mobile road-side infrastructure installed beforehand. These communication paradigms offer a rich set of tools to drivers and administrators of transportation system to avoid environmental hazards, for instance black ice on the pavement, highway turbulence, and approaching ambulance, to name a few.

According to statistics from US Department of Transportation (DoT) in 2008, a staggering amount of roughly $75 billion are lost in worker productivity and around 8.4 billion gallons of fuel is wasted [8]. Let alone, half of all congestion events occurred because of highway incidents rather than because of rush hours which is a common perception [9]. Looking at these statistics, the need for new infrastructure such as VANET is essential. Apart from the fact that these statistics could be driving force for VANET deployment, the community of researchers and academia anticipate that the surge in VANET technology is poised to have a huge societal impact. A number of vehicle manufacturers, government agencies, and standardization agencies around the globe have already spawn their research resources to VANET. The examples include Networks-on-Wheels, Car-2-Car

Communication Consortium, the Vehicle Safety Communication Consortium, Honda's Advanced Safety Vehicle Program, and many more [10].

US Federal Communication Commission (FCC) has allocated a rich 75 MHz of spectrum (5.850–5.925 GHz band) for the exclusive use of Dedicated Short Range Communication (DSRC) also known as WAVE 802.11p [11]. It has been pointed out that the allocated bandwidth exceeds far more than the requirements for VANET safety applications [12]. Therefore the surplus bandwidth opened the doors for new opportunities for investors, developers, and automobile industry, to enrich VANET services for the consumers. In other words, plethora of applications can be developed for VANET by utilizing the excess bandwidth, ranging from traffic safety to all kinds of infotainment systems on the wheels [12].

Cloud computing has changed the computation and communication mindset by decoupling computational assets from physical infrastructure thereby enabling virtualization [13]. The main motive of the cloud computing is to make sure the availability of "*exactly what you need and when you need*". Since with the advancements in technology, internet is high-speed and has low cost than before, it would be better if it is utilized for more than just browsing. Another reason is that the advancements in parallel and distributed computing compel the application developers and industry to utilize the internet. Cloud computing is very appealing to the business startups with low upfront and virtually no maintenance cost. This computing paradigm offers new opportunities for developers and infrastructure providers at par. Until very recently, having virtually unlimited resources at very low affordable cost was just a dream, but cloud computing made it reality and there are many players in the market providing cloud services like Amazon, Microsoft, and Google.

Recently Olariu et al. [14] envisioned the idea of vehicular clouds by taking traditional VANET to the clouds [12]. The driving force behind their idea of vehicular clouds is that in the near future, huge vehicular fleets on our roadways, streets and parking lots will be recognized as abundant and under-utilized computational and communication resources. These resources could be used elsewhere that could earn a comparable revenue as well. The cloud computing environment fits to the scenario where the excess of the resources can be rented out. Though Olariu et al. [14] for the first time proposed the idea of vehicular clouds, they did not discuss the potential structural and architectural framework for vehicular clouds.

1.1 Our Contributions

In this paper we put forth the architectural taxonomy of future VANET clouds based on the services provided by the technology. We also propose the potential architectural frameworks for different types of cloud scenarios in VANET. It is to be noted that this work is the extended version of a poster that appeared in IEEE CloudCom 2012 [15] where we, for the first time proposed the signatory VANET-based cloud architectures. Additionally, here we also discuss the unique challenges from architectural, security, and privacy standpoint in VANET clouds. We believe that the proposed framework will cover the existing resource-rich cloud infrastructure and VANET, and enable VANET to merge with cloud computing paradigm. Moreover to argue on the feasibility of the proposed architectures, we also outline a novel traffic information dissemination mechanism through cloud infrastructure in VANET as a use-case of our proposed framework. The proposed traffic information dissemination through cloud leverages the preestablished VANET architecture where every vehicle shares its frequent mobility information with neighbor vehicles as well as with the cloud infrastructure through gateways. The cloud on the other hand, after processing the received coarse-grained information from the vehicles through gateways, constructs fine-grained traffic information and shares it with the vehicles on the road in the form of small segments based on the current near-future location of the subscriber vehicles. The structure of the rest of the paper is organized as follows. Section 2 summarizes the state of the art regarding VANET, cloud computing, and vehicular clouds. We provide the readers with a bird's view of VANET and cloud services as a baseline for our proposed architecture in Sect. 3. Section 4 presents our proposed VANET clouds architectures. In Sect. 5, we discuss our proposed use-case for the VANET-based clouds framework. Section 6 outlines the research, security, and privacy challenges in VANET clouds following by concluding remarks and future directions in Sect. 7.

2 Related Work

In this section we discuss the state of the art regarding VANET and its successor VANET clouds from design, applications, security and privacy standpoint. To have a better understanding of the previous work carried out, we divide this section into three sub-sections. In first and second subsections we outline the research carried out in the field of standalone VANET and cloud computing, respectively. In the last sub-section we outline the state of the art regarding vehicular clouds.

2.1 VANET

Hartenstein and Laberteaux [16] carried out an extensive survey on VANET covering infrastructural aspects. Besides, implementation, performance, and research challenges have been discussed in [7]. Moreover, design and architectural issues are outlined in great detail by Papadimitratos et al. in [17]. The full deployment of VANET is still underway, since its success and adaptation in end-users (drivers), consumers, and governments is bounded by tangible and viable security solutions. Due to security and privacy challenges, the momentum of advancements in VANET has been impeded. Nevertheless, enormous research has been carried out to deal with security and privacy issues in VANET [2–5]. The problem in hand is to secure the operations of VANET by designing protocol suits that will mitigate the attacks and thwart deviations from the implemented protocol to a possible extent. The standalone security requirements for VANET are *authentication, message integrity, message confidentiality, non-frameability, non-repudiation, user and location privacy*, and *conditional anonymity* [2]. It is worth noting that the set of requirements may vary depending upon the types of messages. For instance, in Cooperative Awareness Applications (CAA), where cooperative awareness information is exchanged among the vehicles in the vicinity, there is no reason to encrypt the information.[1] Privacy issues in VANET have been discussed in detail in [4] and many privacy preserving schemes have been proposed [18, 19].

The services offered by VANET are not limited to collision warning, non-safety applications such as traffic congestion and routing information, but also include value-added services such as high-speed tolling, mobile infotainment, internet-on-the-road, movies-on-

[1] This argument is true only for insiders. In order to deal with the outsider attackers, the information must be made secure against different attacks launched by the outsiders such as content manipulation and profilation.

demand, and IPTV [20]. Nonetheless the ephemeral nature of VANET and mobility concerns pose many challenges for the research community.

2.2 Cloud Computing

Cloud computing is considered to be a business model rather than a technology. In [21], the authors carried out a state of the art survey answering the question whether cloud computing will stay or is it one of the hyped subjects that inevitably will be forgotten in the next couple of years. Most of the techno-market players such as Google, Amazon, and Microsoft are accelerating their pace in cloud computing by providing services to their users. Due to the motive of cloud computing, it seems very attractive to the end-user for variety of reasons. For instance the end-users do not need to worry about the shortage and management of resources [13]. Nevertheless, as to the other networks, security and privacy is a nightmare to cloud computing as well. Zhou et al. [22] carried out a brief survey about security and privacy issues in cloud computing covering the very aspects of security such as availability, confidentiality, data integrity, control, and audit. Besides, they also discussed the privacy issues in detail including legal issues and multi-location issues. Zeng and Cavoukian [23] proposed cloud computing architecture from privacy standpoint and they embedded the privacy into design by following '*privacy by design*' approach. Storage security is another hot issue in cloud computing these days. Bessani et al. [24] proposed a scheme to remedy the storage security problem in cloud computing through the encryption, encoding, and replication of the data on diverse clouds which led them to a cloud-of-clouds. Cachin et al. [25] surveyed well-known cryptographic tools for providing integrity and consistency for data stored in clouds, and discussed recent research in cryptography and distributed computing addressing the aforementioned problems.

2.3 Combination of VANET and Cloud Computing

Fairly recently, Olariu and his colleagues envisioned combining VANET with cloud computing [12, 14]. They proposed Autonomous Vehicular Clouds (AVC) offering potential applications to VANET users. The authors also briefly discussed research challenges in the vehicular clouds. Abuelela et al. [12] suggested to take conventional VANETs to the cloud and envisioned that in future, the under-utilized VANET resources could be utilized by combining VANET with cloud computing [14]. Taking a step ahead, Bernstein et al. [26] proposed a Platform as a Service (PaaS) model for mobile vehicular domain with possible potential applications. Yan et al. [27, 28] outlined the security and privacy challenges in vehicular clouds. They discussed the challenges resulted by the features of vehicular clouds, e.g. authentication of highly mobile vehicles and the complexity of trust relationships among multi-players caused by intermittent short range communication.

Nonetheless, the infant vehicular clouds still needs rigorous research insights to make it to the deployment phase. One of the main advantages of VANET-based clouds is that, no additional infrastructure is needed for deployment since the infrastructure is already there. Olariu et al. did not propose any solid framework for vehicular clouds. They carried their work mostly from applications standpoint. Recently Yu et al. [29] addressed the resource management issue in VANET by integrating it with cloud computing. They divided the VANET-based clouds into vehicular cloud and road-side cloud. Yu et al. mainly focused on the Virtual Machine (VM) migration issue, which we think might not be needed if the architecture is re-considered. Moreover, RSU deployment is already a daunting challenge in VANET, leaving the RSU cloud questionable. They also cover a specific range of applications under the umbrella of VANET-based clouds whereas we aim to abstract that limitation. Another recent work has been done by Whaiduzzaman et al. [30] where they surveyed the emergent vehicular clouds. They covered the previous works carried out regarding vehicular clouds[2] and emphasized on the applications that are offered by this business model/technology.

Our contribution is different from the aforementioned authors. We put forth a solid taxonomy of the VANET clouds based on the types of applications and modes of communication. Moreover we define different architectural frameworks for VANET cloud based on the vehicular-based cloud computing taxonomy. The basic idea of our proposed scheme can be found in the poster version [15], whereas here we extend the preliminary version to a more elaborated version with technical depth. It is, to the best of our knowledge, first approach to take the vision of Olariu and his co-workers, a step further towards VANET based cloud computing. For the ease of understanding, we outline a novel use-case of our architectural framework where private cloud infrastructure provides the subscriber vehicles with fine-grained traffic information as a result of cooperation from the vehicles to the cloud infrastructure in the form of frequent mobility information. More precisely vehicles share their coarse-grained mobility information with neighbors and with cloud infrastructure. The cloud after processing the coarse-grained information, constructs fine-grained traffic information of the road segments and disseminates the fine-grained traffic information to the subscriber vehicles based on their locations.

3 VANET and Cloud Computing: A Bird's View

In this section we outline the bird's view of standalone VANET and cloud computing technologies which will serve as baseline for our proposed scheme.

3.1 VANET Architecture, Framework, and Services

VANET leverages vehicles as mobile nodes moving on the road and stationary RSUs installed on the road side and/or hot spots (for instance in an intersection of a cross-road). The main players in VANET are management entities, certification authorities, revocation authorities, and end users (vehicular nodes). Keeping in mind the advancements in vehicular technology, it is sepculated that in the near future, high-end and middle-end vehicles will be equipped with rich set of computational, communication, and storage resources. VANET employs architecture-less communication among the vehicular nodes and infrastructure-based communication between vehicles and RSUs. The results from these communications are fed to safety and non-safety applications. For instance, CAA leverages scheduled beacon messages that contain speed, location, heading, and lane information of the originating node. CCA uses this information from the vehicles in the vicinity to construct traffic view ahead of the vehicle. Besides, important decisions have to be made depending upon the information from these beacons. Apart from beacons, critical warning messages are of paramount importance in VANET that enable the drivers to make timely decision in critical scenarios such as an accident on the freeway or traffic jam in rush hours. These timely warning messages can enable VANET applications to suggest alternate routes for the driver. Cooperative Adaptive Cruise Control (CACC) is another

[2] The terms ‘VANET-based clouds’ and ‘vehicular clouds’ are used interchangeably in this paper and both the terms refer to the merging of VANET and cloud computing.

important application of VANET which mainly emphasizes on maneuver control while driving [31]. From applications point of view, several industry and governments consortiums are striving to identify different kinds of VANET safety applications (and related technologies) that will provide the greatest safety benefits. These organizations include Crash Avoidance Metrics Partnership (CAMP) [32] which is the joint collaboration of vehicle companies like BMW, DaimlerChysler, Ford, GM, Honda, Nissan, Toyota, and Volkswagen. Another such organization is Car2Car Communication Consortium (C3).

3.2 Cloud Services

Needless to say that cloud computing is becoming a well-known buzzword for the last decade. Generally cloud computing refers to both services accessed via, and delivered through, the vast universe of internet in a seemless manner, and the hardware and system software in remote datacenters that provide those services. The beauty of virtualization in cloud computing is attracting large businesses to migrate to cloud environments. Nevertheless this migration is not yet abrupt and still large corporations are testing the waters with small projects. The main concern of these corporations is the control over cloud. As far as the motivation for migration is concerned, it is important to realize that most of the issues are essentially old problems in new settings. For instance offshore outsourcing must guarantee certain security primitives such as data integrity, data security, and privacy etc. Chow et al. [33] believe that integrity of the cloud infrastructure is ensured through the use of trusted computing.

Cloud computing is also known as ‘*utility computing*’ which is based on ‘*pay-as-you-go*’ service [13]. The scenario can be easily compared with our daily life, where we use gas and electricity in our homes as much as we need and at the end of the month we pay for exactly what we have used, neither more nor less. Cloud computing environment offers rich amount of resources ranging from offshore storage to offshore infrastructure. Examples are Amazon S3, Google Drive, and Microsoft SkyDrive. Besides storage, clouds also offer computation resources, such as Amazon Elastic Compute Cloud (EC2), which can significantly reduce the cost of maintaining resources locally. Besides, online collaboration tools, such as Google Apps or versioning repositories for source code make it easy to develop applications online without purchasing licenses for different softwares. Along with the enterprises, home users can also take advantage of cloud computing, if the services are available at reasonable prices. The use of new sophisticated handheld devices is drastically increasing day by day. But still these devices are lacking far behind the traditional computers in computational power. Nevertheless, notebook computers are now transforming to tablets or a light netbook, which can take advantage of cloud services for intensive computations. In the near future, cloud services will be widely used by the enterprises and individuals, using hybrid computing and communication devices. Thus it is required to provide cloud service to the individuals, at a very low cost which will boost up competition among cloud vendors and will result in reducing infrastructure costs for them [34, 35].

The core of the cloud services is comprised of three basic delivery models in the form of layers. The top layer is known as Software as a Service (SaaS). This layer delivers applications to consumers (either individual or enterprise) in a multitenant fashion. Usually the consumers use thin clients to access those services through internet. The principle benefit to consumer is that, he/she does not have to pay the upfront cost for hardware or software licensing. The by far best example of this service suit is the Google Docs which is equivalent to Microsoft Office. Google provides the aforementioned service to its consumers for free.

Platform as a Service (PaaS) is the second type of service in the layered stack which refers to delivering the development environment as a service to the consumers instead of installing development tools/softwares on host computers. This makes the consumers capable of doing their development remotely by using only the services provided by the service provider. Normally this kind of service works well at enterprise level and the best example is Google App Engine.

At the bottom of the layered stack, cloud computing provides Infrastructure as a Service (IaaS). Instead of application or environment, in this paradigm, physical resources are delivered to consumers as a service. These resources include servers, connections, and related tools necessary to build an application environment from the scratch. Consumers have virtually unlimited resources according to their budget. They can rent processing, storage, networks, and other fundamental computing resources on which the consumer then deploy and run arbitrary cloud application softwares and system softwares. Amazon is providing such services on rent through its elastic computing called EC2.

In the next section, we briefly discuss our proposed VANET clouds architectural framework.

4 Proposed VANET Clouds Architecture

Thanks to advancements in vehicular technologies by virtue of which today's high-end vehicles are capable of hosting substantial on-board computation, storage, sensing, and communication capabilities. These vehicles in combined fashion can serve as a huge farm of computers on the move. These aforementioned attributes make vehicles on the road not just moving machines as a mean of transportation, but also ideal candidates for the next paradigm shift from traditional VANET to VANET clouds so that their resources can be utilized in better way. Olariu et al. [14] for the first time, coined the term Autonomous Vehicular Clouds (AVC) as, "A group of largely autonomous vehicles whose corporate computing, sensing, communication, and physical resources can be coordinated and dynamically allocated to authorized users".

We take a step forward to broaden the idea of VANET clouds by first defining a communication paradigm for VANET clouds and then put forth the potential cloud services from VANET standpoint.

4.1 Communication Paradigm in VANET Clouds

Figure 1 shows the communication paradigm for VANET clouds. There are three layers of communications in VANET clouds at three different levels incorporating different entities.

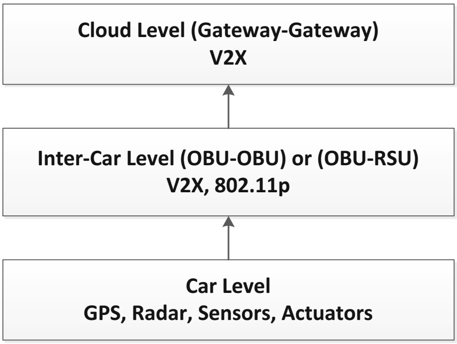
Cloud Level (Gateway-Gateway)
V2X
Inter-Car Level (OBU-OBU) or (OBU-RSU)
V2X, 802.11p
Car Level
GPS, Radar, Sensors, Actuators

Fig. 1 Communication paradigm of VANET clouds

The bottom level is communication at car level. Vehicles in standalone VANET have Global Positioning System (GSP) to obtain accurate location information, radar, sensors, and actuators. Communication among these aforementioned entities will take place at car level to form a networked environment in order to feed the data from aforementioned entities to the processing modules. For instance the data from these modules would be used to construct cooperative awareness messages or alarm messages otherwise. The second level of communication is inter-car level where vehicles communicate with each other at On-Board Unit (OBU) level. This communication can be either V2 or V2I by using IEEE 802.11p (WAVE) standard. Note that communication in the lower 2 levels of Fig. 1 is inherited from conventional VANET. The top most level enables vehicles to communicate at cloud level where vehicles or RSUs may serve as gateways. The nomination of vehicle or RSU as gateway will depend upon the underlying framework of VANET cloud.

4.2 Service Architecture in VANET-Based Clouds

As illustrated in Fig. 2, VANET clouds are suitable for IaaS and SaaS only, whereas PaaS does not seem to be logically appropriate for VANET environment. At IaaS level, the potential services provided by VANET clouds can be Network as a Service (NaaS) where a vehicular node moving on the road can be leveraged as a WiFi access point gateway to the internet. Logically while moving on the road, on highways in particular, the vehicles tend to move at relatively same speed and in normal cases, the neighborhood does not change abruptly. Nevertheless, connection time is an important factor for using NaaS service. The vehicles can rent their resources provided that the users intending to use the services, are willing to pay. At SaaS level, real-time VANET information can be shared with the subscribed users. Additionally, infotainment services and P2P applications are also suitable to be used as SaaS. An extra-ordinary benefit of VANET application as SaaS is that, the vehicles that do not have VANET capabilities, can still subscribe to VANET information in a virtualized fashion and they will be charged for what they subscribed for. The fact that drivers may not need VANET functionalities all the times will save them the resources.

4.3 Comparison Between Conventional and VANET Clouds

Figure 3 depicts the comparison between conventional clouds and VANET clouds. It is worth noting that each level in conventional cloud has its counterpart in the VANET scenario. For instance, the infrastructure, platform, and applications are obvious in both

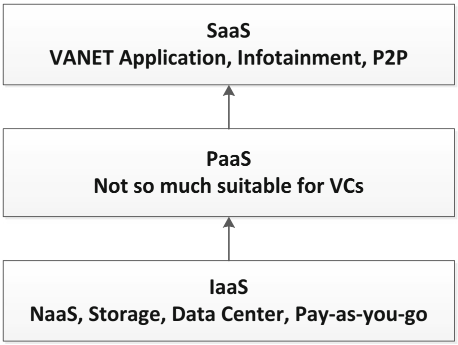
SaaS
VANET Application, Infotainment, P2P
PaaS
Not so much suitable for VCs
IaaS
NaaS, Storage, Data Center, Pay-as-you-go

Fig. 2 Service architecture in VANET clouds [32]

environments but at client's level in conventional clouds, the VANET counterparts may be vehicles themselves or general users, depending upon the service structure.

4.4 VANET Clouds Taxonomy

Figure 4 illustrates the brief taxonomy of VANET clouds. We divide VANET clouds into three major architectures namely vehicular clouds (VC), vehicles using clouds (VuC), and hybrid vehicular clouds (HVC). VC is further divided into two scenarios from movement standpoint. Static clouds refer to the stationary vehicles providing cloud services (renting out storage or processing resources). For instance a virtual super computer formed by the collaboration of vehicles parked in a big organization or enterprise's parking lot [12, 36]. In case of static VANET clouds, the infrastructure (communication, storage, and process) can be rented out to make revenue as well. IaaS and data storages services are feasible for such arrangements. On the other hand, dynamic clouds are formed on demand in ad hoc manner. VuC connects the VANET to traditional clouds where VANET users can use cloud services on the move such as infotainment, traffic information, and CAA to name a few. In HVC, vehicular clouds interact with traditional cloud for services exchange. The vehicles and RSUs serve as gateways on the VANET part thereby communicating with the gateways of the traditional clouds. Each section is further elaborated in the following sub-sections.

4.4.1 Vehicular Clouds (VC)

The main players in VC include VANET infrastructure itself, gateways, and brokers as shown in Fig. 5.

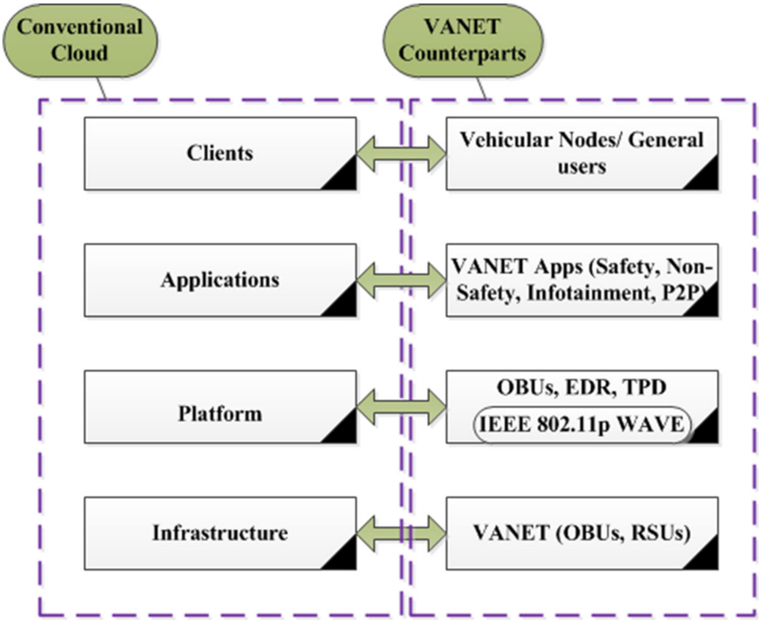

Fig. 3 Conventional clouds versus VANET clouds

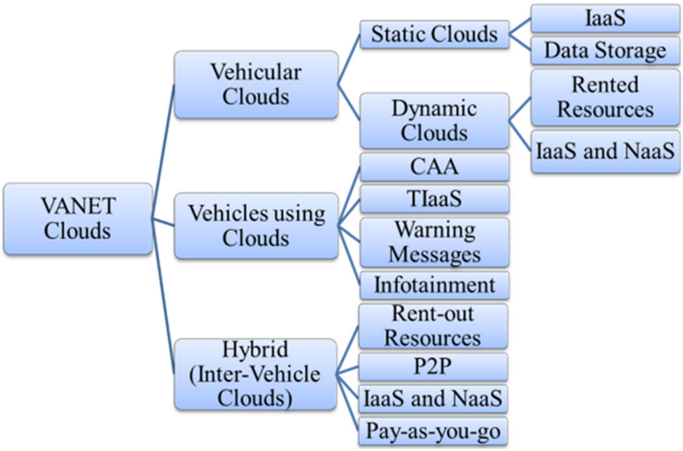

Fig. 4 Taxonomy of VANET clouds

Note that the vehicular nodes serve as service providers in this paradigm. As depicted in Fig. 4, VC can be divided into two classes namely static VC and dynamic VC. The lifetime of static VCs is longer than dynamic VC. However, both of them serve different classes of applications, for instance static VCs are more suitable for long-term services such as Storage as a Service (STaaS), IaaS, and Datacenter in the parking lot [36], whereas dynamic VCs are suitable for disposable clouds. Generic VC is formed in the following manner.

First, the vehicles in the vicinity initiate a protocol to select broker(s) among them and identify the boundaries of the cloud following by electing an Authorized Entity (AE) among the brokers to ask for authorization for cloud formation. After brokers and AE are elected, then AE invites the vehicular nodes in the premises of the cloud boundary to take part in cloud. Interested vehicles will reply with an acknowledgement. If the number of

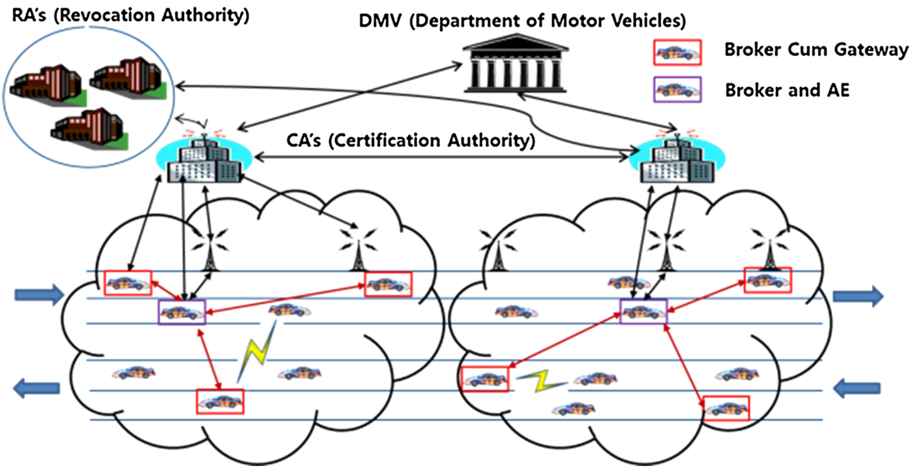
RA's (Revocation Authority)
DMV (Department of Motor Vehicles)
Broker Cum Gateway
Broker and AE
CA's (Certification Authority)

Fig. 5 Vehicular clouds (VC) [15]

interested vehicles is above certain threshold, then AE asks higher authorities about permission to form a cloud and provide the potential resources. Upon getting permission, the participants of the cloud pool their resources to form a resource rich virtual environment. AE sends the schedule plan to higher authorities and gets implementation authorization. Note that the job in hand can be handed over to the cloud by higher authorities in exchange of some incentives for the participants. AE dissolves the cloud after the job is done. It is worth noting that this strategy is different, at least in part, from that of Olariu et al.'s [14] scheme. It is better practice to first look for the volunteers before asking authorities for permission. It will save the bandwidth and communication if the number of volunteers for dynamic cloud formation is not enough and also when it is not possible to form a cloud.

One of the most appropriate examples of dynamic clouds is dynamic traffic lights scheduling [12, 14]. Consider a national sports event in a huge stadium watched by thousands of viewers. When the event is over, everybody wants to go out first and it will create catastrophic traffic jams in the vicinity of the stadium. The usual traffic lights would not be a suitable option to fade away the traffic jam. The better solution would be to re-schedule the scheduled traffic lights in a real-time. In worst case, it would include not only traffic lights in the stadium vicinity, but also the effect of changing one traffic light would affect many others thereby demanding re-scheduling the traffic lights on a large scale. In the aforementioned scenario, AE sends the traffic signals re-scheduling plan to the municipality and hence the traffic jams issues can be resolved in a timely manner.

Another promising application of dynamic VCs is Video on Demand (VoD) service on the road provided through the public transport buses in the vicinity. Resources rich public transport buses pool their shared storage resources to offer MoD service to the vehicles in the urban vicinity. Public transport buses are assumed to be equipped with both DSRC and 3/4G communication capabilities and the possible gateways to VANET and cloud infrastructure [37]. Besides, real-time navigation service can be provided with the help of cloud formed by the buses and other vehicles, to the subscribers. These cloud players will examine the current traffic conditions and make the navigation decisions accordingly.

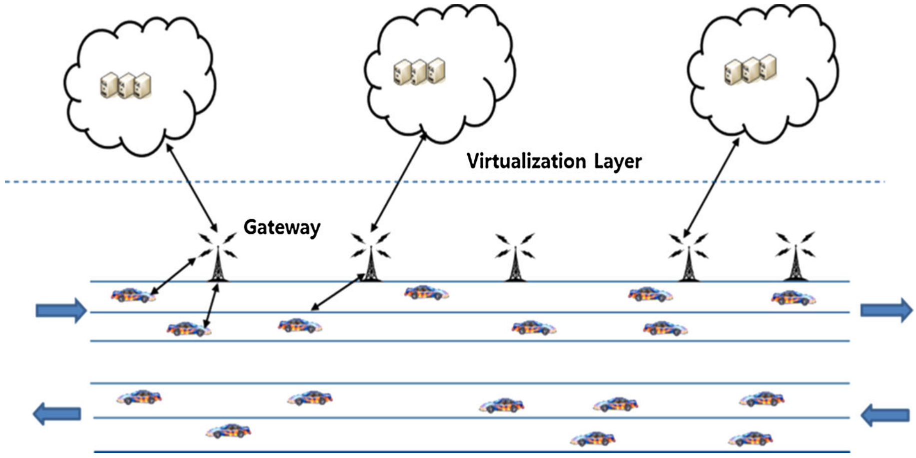

Fig. 6 Vehicles using clouds (VuC) [15]

4.4.2 Vehicles Using Clouds (VuC)

Figure 6 depicts the architecture of VuC where VANET uses cloud services on the move. VANET collaborates with cloud infrastructure and provides cloud with meaningful data that could be used in decision making. The virtualization layer is provided by the gateways. RSUs serve as gateway to the clouds. Moreover, vehicular nodes with 3/4G internet connection might also serve as gateway to cloud infrastructure in remote areas where vehicles have no direct connection with RSUs. High speed wired backbone channel is assumed to be present between static gateways and the cloud servers. Without loss of generality, VuC could be leveraged to provide VANET with CAA, real-time traffic information, and infotainment. However in this paper we emphasize only on traffic information. We consider fine-grained traffic information dissemination through clouds as a use-case in this paper [38]. Vehicles cooperate with cloud and provide cloud with coarse-grained whereabouts information that includes vehicle's current position, speed, and heading information. Whereas cloud after processing the coarse-grained information, constructs the fine-grained traffic information and disseminates it to the vehicles on the road based on their current and near-future locations.

Many applications of this category have already been outlined in [14] and [30]. Other promising applications of VuC include remote configuration and car performance checking, big traffic data analysis, smart location-based advertisements, and vehicles witnesses.

A. Remote Configuration and Car Performance Checking

By using cloud technology, a car can be monitored and debugged remotely. This technology has already been implemented by a well-known automobile company Hyundai [39], where they monitor their cars right from assembly line. The performance of the car is remotely checked by constantly receiving data from the car and is used to provide quality of services to the customers. Nevertheless user and location privacy are serious concerns for such approach.

B. Big traffic data analysis

Vehicles produce large amount of traffic data, for instance beacon messages produce data on the scale of milliseconds, that is valuable for the services provided by VANET. Data storage and processing would require large amount of storage and computation resources respectively. This data could be used for a variety of purposes ranging from traffic information to entertainment.

C. Smart location-based advertisements

With the advent of smart vehicles, billboards on the road-sides are likely to be replaced by in-car advertisement system, where drivers can get the ads of their interest based on their choice. As aforesaid, the whereabouts data, the driving pattern, and the location queries from the drivers would enable the decision making servers in the cloud to advertise the events and/or locations to the people in a smart way based on their interests.

D. Vehicle Witnesses

Recently, Hussain et al. [40] proposed Vehicles Witnesses as a Service (VWaaS) that leverages cloud infrastructure to save the original forensics in case of any incident on the road. Vehicles upon sensing an event, or getting instruction from authorities, take pictures of the site of interest, and send it to the cloud. Cloud infrastructure saves these pictures as forensic evidence and later on provides the forensics to law enforcement agencies, judiciary, and/or insurance agencies.

4.4.3 Hybrid Vehicular Clouds (Inter-vehicle Clouds)

HVC is the combination of VC and VuC where VC serves as both service provider and consumer at the same time. HVC architecture is shown in Fig. 7. The motivation behind HVC is that the vehicles moving on the road might want to rent out their resources and might want to use cloud services at the same time. NaaS and P2P are the most suitable examples for such scenarios. Nevertheless due to the ephemeral nature of VANET, connection among vehicular nodes is very intermittent. However, it can be argued that usually for P2P applications, the size of the files is fairly small making it suitable for short time connection. Other potential applications for this architecture include IaaS in case of VC.

Another potential application of HVC is the MoD service provided by public transport buses in a multi-cloud environment, where buses provide MoD to the subscriber vehicles. The buses use their local storage and if the requested file is not available locally, then they can use the multi-cloud architecture and use third-party service providers to access the requested file. In-car cloud for diagnostics and heterogeneous environment while using other third-party cloud is another promising application of HVC. In such scenario, the in-car cloud gathers data from different sensors in the car for instance tire pressure, brake oil, engine oil and so forth, and processes it for car diagnostics. There are two options, either this data could be dealt with locally or can be uploaded to the manufacturer cloud. Meanwhile the car's OBU also cooperates with the VANET cloud in the form of coarse-grained whereabouts information and receives fine-grained traffic information and warning from the cloud.

5 Use-Case (Traffic Information Dissemination Through Clouds)

5.1 Baseline

In this section we outline a novel use-case for our proposed VANET-based clouds framework which is based on Traffic Information as a Service (TIaaS) [38]. We chose the

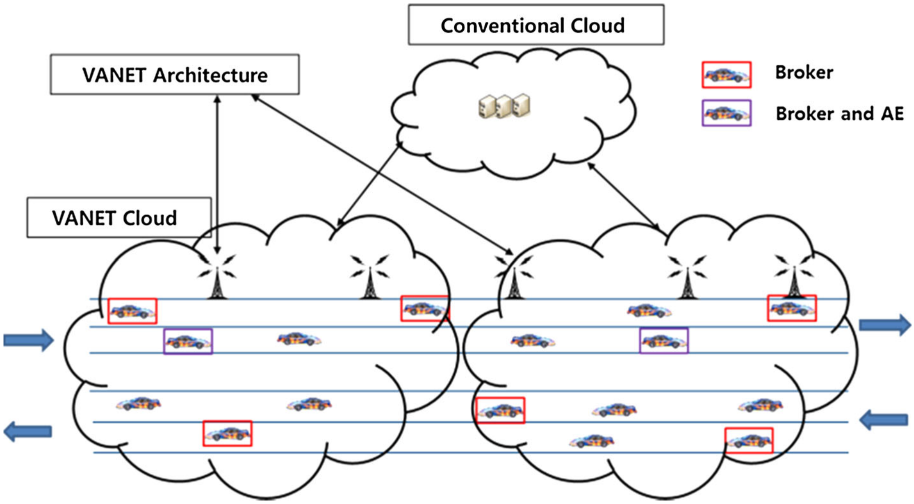

Fig. 7 Hybrid vehicular clouds (inter-vehicle clouds) [15]

widely used traffic information dissemination system (TIDS) among vehicles in VANET. Traditionally traffic views (short-range local and long-range extended) are constructed from the beacon information in hand by vehicles which consume a considerable amount of vehicle's processing power. Therefore, we propose cloud-based TIDS where vehicles share their coarse-grained traffic information with cloud in the form of beacons and cloud after processing, provides the subscriber vehicles with fine-grained traffic information based on their locations.

5.2 Network Model

Figure 8 illustrates our proposed network model. We divide our proposed architecture into two networks connected through Gateway Terminals (GTs). VANET architecture consists of traditional vehicular nodes, RSUs, and management/revocation authorities. Vehicles moving on the road serve both as producers (they share coarse-grained information with the cloud) and consumers (they subscribe to fine-grained traffic information from the cloud). RSUs serve as GT between vehicles and the cloud infrastructure. We assume that a fraction of vehicles on the road have 3/4G internet access which can be leveraged to serve as a secondary GT to the cloud.

It is worth noting that in case if there is no access to RSU directly, then vehicles with 3/4G connections could be used as mobile GT.

Cloud architecture consists of authenticator, Cloud Processing Module (CPM), Cloud Knowledge Base (CKB), and Cloud Decision Module (CDM). Authenticator is responsible for handling subscriptions from the vehicles and authenticating them. Data-contained coarse-grained *MVs* from vehicles are collected by cloud, stored at CKB and forwarded to CPM for processing. After processing coarse-grained *MV*, CPM constructs fine-grained traffic information and forwards it to CDM. CDM then categorizes the fine-grained data

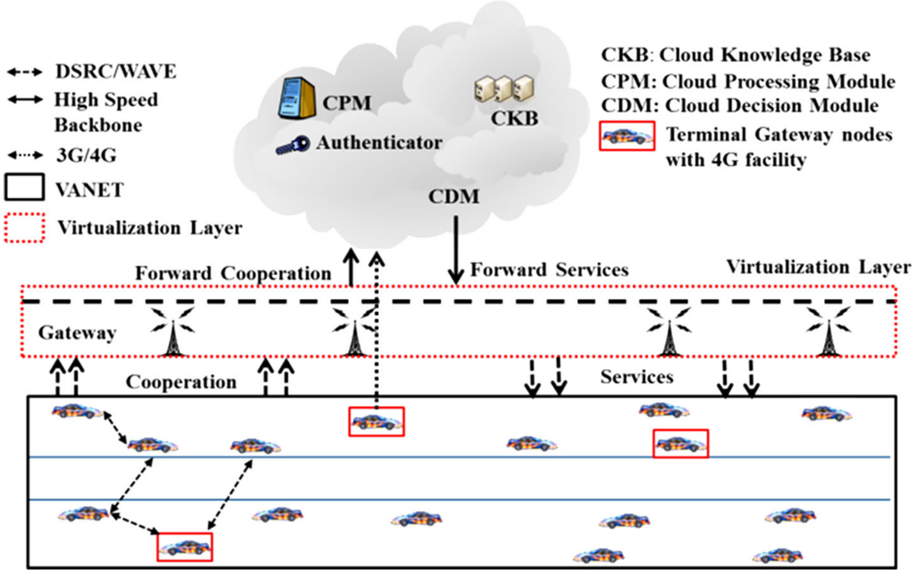

Fig. 8 Network model of traffic information as a service

based on physical locations. Without loss of generality, physical roads are divided into small manageable zones and zones are further divided into segments beforehand. The data is delivered to vehicles on the segment basis.

5.3 Mobility Vector (MV)

As a cornerstone of VANET, vehicles rely on situational awareness information from neighbors in order to have smooth, safe, and reliable driving experience. Such awareness is realized through beacons shared among the vehicles. The information contained in beacon (timestamp, location, speed, acceleration, and heading etc.) helps the neighbors to update their awareness about the network topology. We define a variation of beacon message namely *Movement Vector* (*MV*)[3] which is shared with the cloud, with slightly lesser frequency than the original beacon. The format of MV is given below:

$$MV_i = \{MD, (\delta_1, \delta_2, \ldots, \delta_n)\}$$

MV_i is i-th movement vector by vehicle V_i containing Movement Data (*MD*). The contents of *MD* are: $MD = (\delta, t_{cur}, loc_{cur}, vel_{cur}, dir)$. ($\delta_1$, δ_2,…, δ_n, δ) are the security parameters that guarantee different security aspects. It is worth noting that we do not consider the security aspects of the proposed TIDS. t_{cur} is the current time, and loc_{cur} is current position of the vehicle moving with velocity vel_{cur} in the direction *dir*.

Vehicles broadcast these movement vectors to the nearby neighbors in the transmission range and also to the gateways (RSUs). To realize a more practical scenario, we consider Hussain et al.'s mobile gateways/RSU mechanism [37].

5.4 Fine-Grained Traffic Information Dissemination

VANET is divided into manageable physical domains and each domain has its own potential cloud infrastructure for traffic information dissemination. It is also worth noting that the cloud must be established privately by the government authorities such as department of transportation, to minimize the transmission and/or access delays during the information retrieval. In order to guarantee the relevant and right information delivery to subscribers, domains are further divided into reasonable zones and without loss of generality, going down to another level of hierarchy, each zone consists of segments that correspond to small road segments (for instance in urban areas, a road segment between two traffic lights or a block). The number of road segments is the tradeoff between the granularity of traffic information and the performance. CPM constructs traffic information based on physical locations (segments). Similarly when CPM constructs fine-grained traffic information corresponding to segments, it forwards the information to CDM in order to provide the subscribers with the right and relevant information according to their current and near-future locations. The reason for segment level delivery is that the subscribers might only be interested in certain area. The desired information may vary depending on the direction of the vehicle. This fine-grained traffic information exhibits the extended traffic view of the vehicles ahead of them. The length of the extended traffic view is again a tradeoff between the granularity of the information and the length of the individual segments. The fine-grained traffic information message M_{TI} is given below:

[3] The terms 'movement vector' and 'mobility vector' are used in this paper interchangeably and both are represented by *MV*.

$$M_{TI} = (t_{cur}, ZID, Seg_{ID}, TD_{Seg_{ID}}, AV_{Seg_{ID}}, others)$$

TD_{SegID} is the traffic density at *SegID*, and AV_{SegID} is the average velocity at *SegID*. ‘*others*’ corresponds to any warning or alarming alert (for instance a black ice on the road or fog). It is worth noting that the pair *ZID* and *SegID* corresponds to a physical location and this information is used by CDM to forward the traffic information to concerned GT. The actual implementation of the graphical user interface can vary from vender to vender and we do not give implementation details here. The information displayed to the drivers on their on-board screen can be represented in different ways such as different colors of the road segments, exact physical representation of the vehicles and so forth. The complete protocol for traffic information dissemination through cloud infrastructure is shown in Fig. 9.

5.5 Performance Evaluation

5.5.1 Complexity

We do not consider the security and privacy factors of our proposed cloud-based TIDS in details and consider them to be out of the scope of this paper and leave it for future work. The complexity of our proposed cloud-based TIDS is $O(1)$ by searching the relationship of different security parameters, depending upon the hash function and its implementation. This complexity is incurred by the revocation authorities in worst case scenario, in order to find the relationship between different messages from the same user (contributor). Whereas in the previous efforts, Qin et al. [41] and Bernstein et al. [26] did not address worst case scenarios in case where liable situations are essential. Qin et al. leveraged Time Space Link Graph (TSLG) for defining vertices and edges in VANET where every vehicle can be source as well as destination at the same time. However in worst case, the number of links

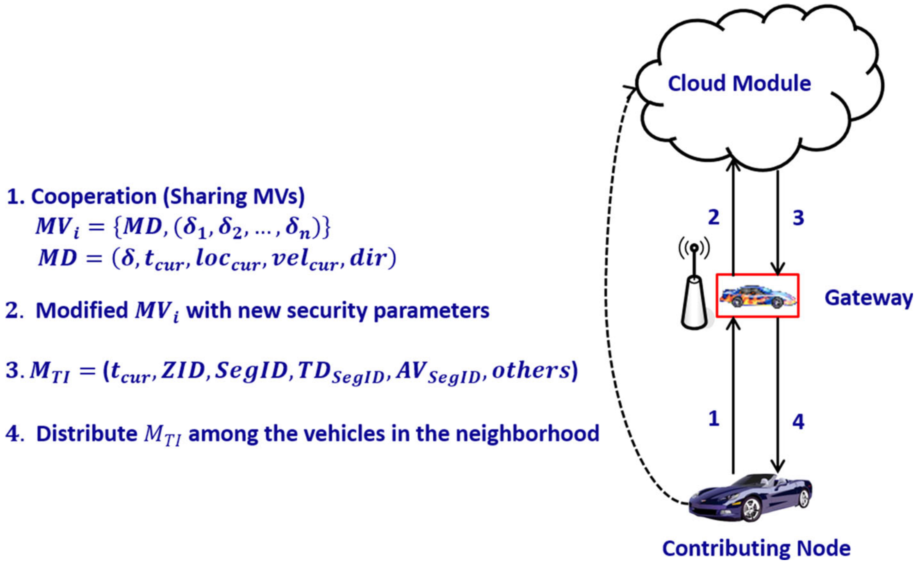
Cloud Module
1. Cooperation (Sharing MVs)
$MV_i = \{MD, (\delta_1, \delta_2, \ldots, \delta_n)\}$
$MD = (\delta, t_{cur}, loc_{cur}, vel_{cur}, dir)$
2. Modified MV_i with new security parameters
3. $M_{TI} = (t_{cur}, ZID, SegID, TD_{SegID}, AV_{SegID}, others)$
4. Distribute M_{TI} among the vehicles in the neighborhood
2
3
Gateway
1
4
Contributing Node

Fig. 9 Traffic information dissemination protocol

can be $(\frac{n(n-1)}{4})$ on average and the order of routing optimization is $O(n^2)$ where n is the number of vehicles in the network. In the next subsection, we explain our simulations results to argue on the feasibility of the proposed cloud-based TIDS. However, we argue that there are enough resources set by the authorities in a private cloud that meet the delay requirements of the VANET application. In our case, since we consider TIDS, the delay requirements are not that much stringent as compared to the safety applications. That is why, the arguments on the delay can be relaxed according to the VANET non-safety applications.

5.5.2 Simulation Setup

In this subsection, we present the simulation setup, simulation tools used, and simulation environment. Moreover we also discuss the traffic scenarios. We evaluate our proposed cloud-based TIDS using ns2[4] (version 2.34 with vanetrbc amendment and the FreeSpace propagation model). In order to generate the real traffic scenarios, we considered a 5 × 9 km^2 section of the Seoul city, South Korea and used TraNS[5] and SUMO[6] to generate the mobility traces for vehicles and RSUs. RSUs are randomly deployed in the simulation and observed section in the simulation exhibits both urban and semi-highway scenarios. The wireless bandwidth and the transmission ranges were set according to DSRC standard.

To investigate different traffic scenarios, we took into account, three traffic regimes, i.e. extensively dense traffic regime, average traffic regime, and sparse traffic regime. We set the simulation matrices as information retrieval rate (IRR), data loss rate (DLR) with varying movement vector frequency (ψ_{MV}), varying traffic density (Γ_{TD}), and varying traffic information frequency (Φ_{TI}). In order to realize the traffic information through clouds, we added another message type, traffic information message to the vanetrbc amendment of the ns2. The new message type represents the fine-grained traffic information from cloud to the vehicles through RSUs and currently our version supports long-range traffic views of the length up to 1, 1.5, 2 and 2.5 km. The simulation parameters used are listed in Table 1.

5.5.3 Simulation Results

In this subsection we demonstrate our simulation results. The main aim of these results is to show the feasibility of the traffic information through VuC architecture and a decent acceptable amount of traffic information retrieval from the cloud infrastructure through gateways. Without loss of generality, we assume a private dedicated cloud infrastructure owned by the authorities, for instance the transportation department of the government with unlimited computation resources. We also assume that the communication between the cloud and the gateways is fast enough and within acceptable delay range. Nonetheless the application we considered, i.e. traffic information dissemination, does not require tight-bound delay.

Information retrieval rate (*IRR*) Our simulation results show that almost every scenario exhibits the favorable percentage of retrieved fine-grained traffic information from the cloud infrastructure. Figure 10 shows the IRR with varying ψ_{MV}. It can be seen that the

[4] http://www.isi.edu/nsnam/ns/.

[5] http://lca.epfl.ch/projects/trans/.

[6] http://sumo-sim.org/.

Table 1 Simulation parameters

Category	Parameter	Value
PHY	Frequency	5.9 GHz
	Channel bandwidth	10 MHz
	IEEE 802.11p data rate	6 Mbps
	Vehicle vicinity	300 m
	RSU vicinity	300 m
MAC	Slot time	16 μs
	SIFS time	32 μs
	Header length	50 μs
	$CW_{\min}$	15
	$CW_{\max}$	1023
Scenario	Road length	5×9 km^2
	Observed length	5×9 km^2
	Vehicular density (Γ_{TD})	(1000,600,200)
	Simulation time	100 s
	Vehicle speed	~20 m/s
Application	ψ_{MV}	(300, 400, 500) Hz[a]
	Beacon size	200 bytes
	Traffic information frequency (Φ_{TI})	(2, 4, 6) s
	Extended view length	(1, 1.5, 2, 2.5) km
	M_{TI} (Traffic information message size)	(140, 210,280, 350) bytes

[a] The beacon frequency is measured in milliseconds

variance in ψ_{MV} slightly affects the rate of information retrieval. In Fig. 10a, the dense traffic regime with $\psi_{MV} = 300$ Hz obtains 83 % information which means that 83 % of the total time every vehicle retrieves fine-grained traffic information successfully. The IRR gets better when the traffic regime makes transition from dense to average and sparse. The natural drop in the IRR in case of dense traffic regime is understandable from the fact that when the number of vehicles increases in the area, the load on the channel also increases thereby causing packets drop. Figure 10b, c show the IRR in case of $\psi_{MV} =$ 400 and 500 Hz respectively. The results in case of dense and average traffic regimes, i.e. 1000 and 600 vehicles respectively, are naturally predictable and with the decrease in ψ_{MV} from 300 to 400 and 500 Hz, the IRR gets better. This behavior is expected because decreasing the movement vector frequency gives more room for the channel to receive more messages and the packets drop is subsequently decreased. However, the sparse traffic regime, i.e. 200 vehicles behaves unpredictably with the decrease in ψ_{MV} because the number of neighbors are decreased and the vehicles can easily go out of the range of the gateways easily. In our simulations, $\Phi_{TI} = 6$ s gives the best results, that is why in Fig. 11 we investigate the behavior of the vehicles against varying movement vector frequencies. It can be seen that $\Phi_{TI} = 6$ s gives above 94 % IRR which can result in the best performance of VANET application. It can be seen that there is minute variance in the IRR with different ψ_{MV}, however we argue that this small change will add up more to the

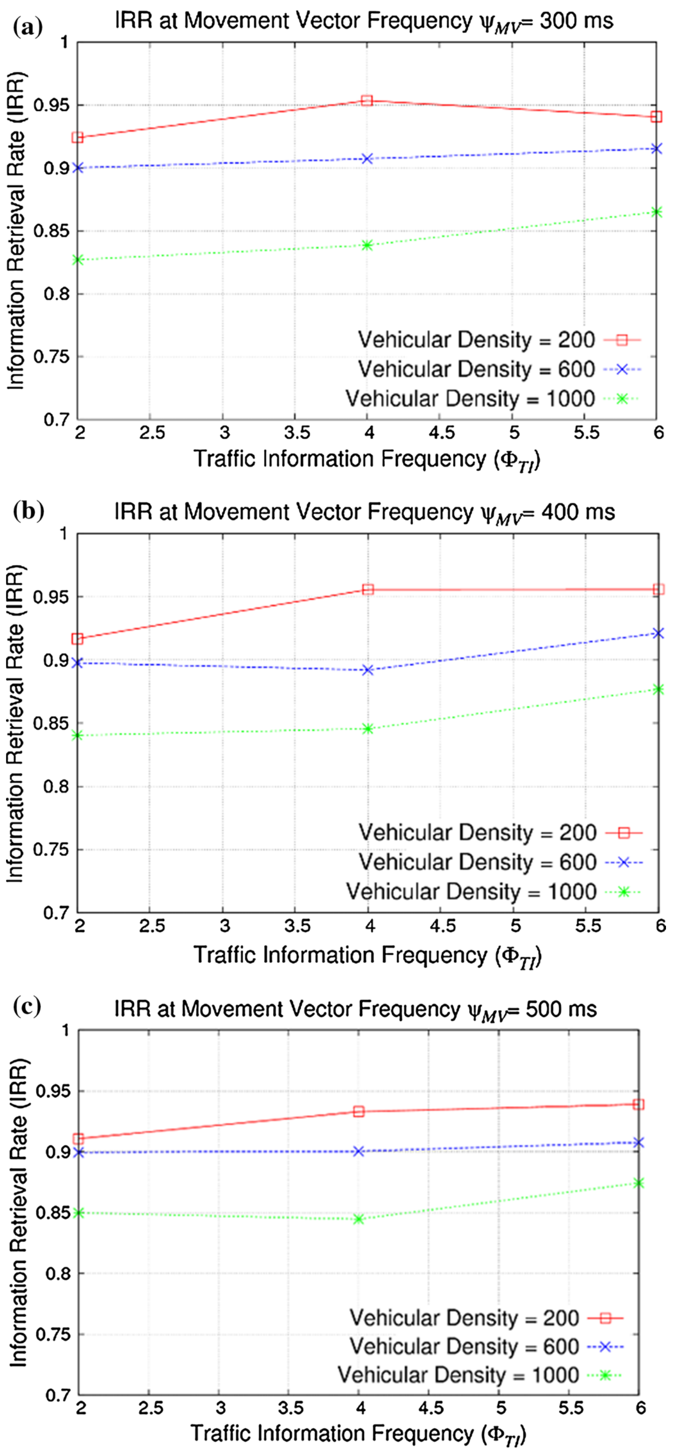

Fig. 10 Information retrieval rate (IRR)

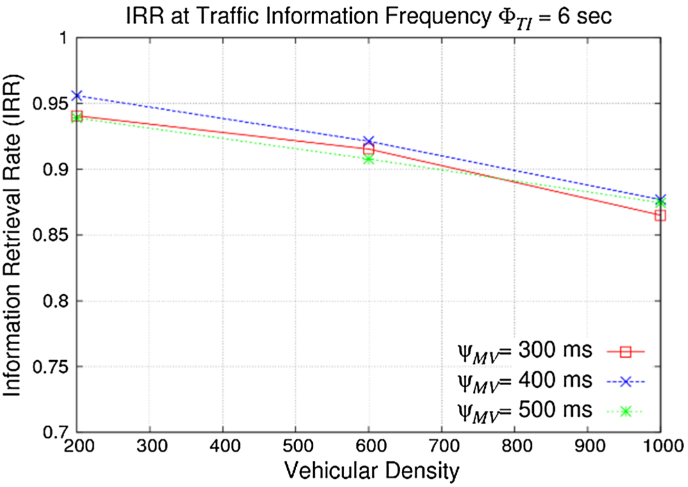

Fig. 11 Information retrieval rate at

optimization of the VANET application. To this end, $\Phi_{TI} = 6$ s performs best in all three traffic regimes.

Data loss rate (*DLR*) We investigate the percentage of data lost during communication while retrieving the fine-grained traffic information from the cloud. In our simulations, we vary both ψ_{MV} and Φ_{TI} with different traffic densities to see the behavior of the system. Figure 12 shows the effect of different Φ_{TI} and the information loss therein. In Fig. 12a we can see the unpredictable behavior in case of sparse traffic regime, where the data loss in case of $\Phi_{TI} = 2$ s is more than the data loss in case of $\Phi_{TI} = 4$ s. Such behavior is the result of the same argument that we made in case of IRR. In case of average and dense traffic regimes, the improvement in data loss with decreased Φ_{TI} is natural and expected. Figure 12b, c outlines the result obtains with $\psi_{MV} = 400$ ms and $\psi_{MV} = 500$ ms respectively. We can see the unpredictable behavior of the sparse traffic regime in both cases. However in case of average and dense traffic regime, the loss in data retrieval slightly increases with the increase traffic density, but the loss decreases with the decrease in Φ_{TI}, which means that fewer traffic information messages will be sent. In other words, $\Phi_{TI} = 2$ s causes more data loss than $\Phi_{TI} = 4$ s and $\Phi_{TI} = 6$ s which is the expected behavior.

5.5.4 Discussion

In the previous subsection, we investigated the different simulation scenarios to observe the feasibility of the traffic information dissemination through proposed VuC framework. Without loss of generality, we assume the established cloud framework and focus only on the gateways and the mobile vehicles on the road. Since we consider traffic information dissemination application as a use-case, the delay requirements are not stringent for such VANET applications. Therefore, above 70 % of the reception rate of the information will result in phenomenal quality of service (QoS) provided by the VANET application. In our case, as it can be seen from the graphs, in worst case each vehicle on the road received the traffic information 83 % of the total time. With more tuning and tweaking, these results can be further improved which will result in more QoS guarantees from the service provider

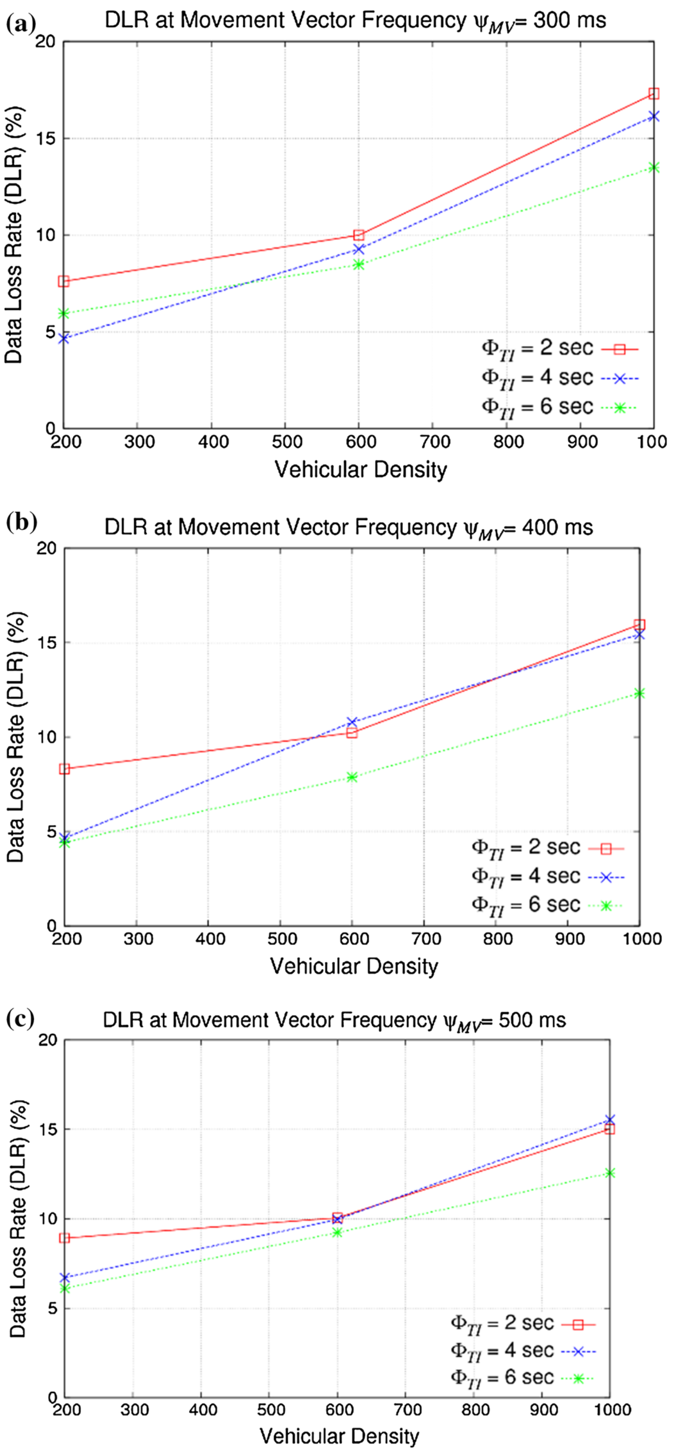

Fig. 12 Data loss rate (DLR)

standpoint. Moreover taking into account the urban scenario, the speed of the vehicles is relatively slow or moderate, that means a little less frequent information retrieval would be acceptable by the application. Overall our simulation results show that the traffic information through gateways from clouds is feasible and fulfills the VANET application requirements. To be more precise, it can be seen that on average, the most favorable parameter for generic semi-optimized VANET application (from traffic information dissemination standpoint) is $\Phi_{TI} = 6$ s and $\psi_{MV} = 400$ ms.

6 Security Challenges in VANET-Based Clouds

Security and privacy are indispensable in vehicular communications for successful acceptance and deployment of such technology. Similarly there are many risks involved with renting virtual resources in cloud environment or storing data in cloud thereby releasing control over data. One concern that many users are aware of, is loss of the privacy and data storage security. Nevertheless, the popularity of social networks and online data sharing repositories suggest that many users are willing to forfeit their privacy to some extent which enabled them to offshore their data and information [25, 34]. Logically VANET clouds inherit their parental long-chased security and privacy issues from both VANET and cloud computing. We take a different road towards security issues in VANET clouds. Unlike Yan et al.'s scheme [27], where the authors discussed spoofing of identities, repudiation issues, DoS and so forth, we believe that potential solutions to such issues have been put forth by VANET community already. These issues can be solved with the scheme designed for signature VANET and cloud computing. The same argument holds for traditional cloud architectural issues.

The security and privacy challenges faced by standalone VANET and cloud computing will remain unchanged even if the two technologies are merged to form VANET clouds. We scrutinize the security challenges faced by VANET clouds from both structural and operational standpoint. We believe that in addition to security threats faced by VANET and cloud computing, the following challenges must be addressed as well.

A. Gossip Interval

Vehicles while moving on the road, have very less time to be in the neighborhood of other vehicles thereby leaving very less room for inter-connection among them. Such topology dynamism is a nightmare for cloud service providers and vehicles themselves. This scenario is a challenge for dynamic VANET clouds. The connection time, at least probabilistically, must be taken into account before using and/or renting the services.

B. Mobile Authentication

High mobility is a distinguishing characteristic of VANET. This mobility may become a bottleneck in authentication process where gossip interval is too small. Efficient authentication schemes must be in place to take the mobility and high speed into account.

C. Conditional anonymity yet virtualization

Since cloud computing's core idea is virtualization of resources but conditional anonymity of users and service providers in case of VANET cloud must be made sure so that in case of a dispute, revocation of user, message, or service provider whichever is necessary, can be possible.

D. Insiders and Outsiders

Insiders and outsiders are two kinds of attackers in VANET. The former are legitimate VANET users and the latter are non-authorized users. In VANET clouds scenario, both insiders and outsiders are crucial threat for cloud services as well as VANET services. Strong security measures must be taken in both static and dynamic VANET clouds against them.

E. Renting out resources, Autonomy, and Control

The other huge challenge for VANET clouds is the tussle among 'renting out resources', autonomy, and control. These three terms have conflict of interest which makes the security of VANET clouds more challenging. Renting out only resources but not control, is an ideal solution for VANET clouds, but autonomy may need to be compromised to some extent. The middle way would be conditional autonomy where in case of a dispute, non-repudiation must be possible.

F. Cooperation Middlewares

Cooperation middleware solutions must be developed in order to connect VANET clouds to each other and/or to external clouds. This situation may arise in case of VuC and HVC scenarios. These middleware solutions will provide trust relationship, data flow control, security, and privacy for the connecting infrastructures.

G. Trust

Trust will be a major concern in VANET-based clouds. Since a considerable number of VANET applications would need to either store the data at the cloud or retrieve data from the cloud, in such case the privacy-critical data storage at cloud would need effective countermeasures. If the government authorities are not the cloud service providers, then the third party cloud service provider might be a vulnerability point as well.

H. Location Security and Privacy

Location security is a challenge in VANET-based clouds and its parental VANET as well, but it gets worse in VANET-based clouds because of the nature of services provided by this technology. Most of the VANET-based clouds applications demand accurate location information from users. The users' location information is used for service provisioning. However adversaries, with enough resources, can manipulate location information to construct users' movement profiles. That is why in order to stimulate active participation from the users, their location security and privacy must be preserved.

7 Conclusions and Future Directions

In this paper, we put forth the vision of combining two emergent fields, VANET and cloud computing. In the recent past, the core idea of vehicular clouds was suggested for the first time in the literature but to date, architectural framework for VANET-based clouds has not been proposed. To this end, only application is emphasized in vehicular clouds environment. To the best of our knowledge, ours is the first effort to suggest a concrete VANET clouds architecture from services standpoint. A brief taxonomy of VANET clouds is outlined. We divide VANET clouds into three architectural frameworks namely Vehicular Clouds (VC), Vehicles using Clouds (VuC), and Hybrid Vehicular Clouds (HVC). In order to better understand our framework, we take cloud-based traffic information dissemination as a use-case. Our simulation results show that the traffic information dissemination through clouds is feasible and offer acceptable throughput with phenomenal information reception rate thereby improving VANET application functionality. It is also to be noted, that by leveraging cloud computing infrastructure for information dissemination, complex and computation and communication-expensive multi-hop communication can be avoided. Moreover we also put light on the security challenges unique to VANET clouds. In the future, we want to derive the optimized values for different frequencies of movement vectors and the traffic information messages of the VANET traffic view application. Additionally we intend to cover more services offered by the VANET-based clouds.

Acknowledgments This work was supported in part by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2014-H0301-14-1015) supervised by the NIPA (National IT Industry Promotion Agency). This work was also supported in part by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2014-H0301-14-1044) supervised by the NIPA(National IT Industry Promotion Agency). This work was also supported in part by the NRF (National Research Foundation of Korea) grant funded by the Korea government MEST (Ministry of Education, Science and Technology) (No. NRF-2012R1A1A2009152). This work was also supported in part by the NRF (National Research Foundation of Korea) grant funded by the Korea government MEST (Ministry of Education, Science and Technology) (No. NRF-2012R1A2A2A01046986).

References

1. Hartenstein, H., & Laberteaux, K. P. (2009). *VANET: Vehicular applications and inter-networking*. Chichester: Wiley. ISBN 978-0-470-74056-9.
2. Raya, M., & Hubaux, J.-P. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security, 15*(1), 39–68.
3. Leinmuller, T., Schoch, E., & Maihofer, C. (2007). Security requirements and solution concepts in vehicular ad hoc networks. In *Proceedings of the wireless on demand network systems and services (WONS '07), fourth annual conference on* (pp. 84–91).
4. Dötzer, F. (2006). Privacy issues in vehicular ad hoc networks. In G. Danezis & D. Martin (Eds.) *Privacy enhancing technologies*, Lecture notes in computer science 3856 (pp. 197–209). Berlin: Springer.
5. Antolino Rivas, D., Barceló-Ordinas, J. M., Guerrero Zapata, M., & Morillo-Pozo, J. D. (2011). Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation. *Journal of Network and Computer Applications, 34*(6), 1942–1955.
6. Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., et al. (2008). Secure vehicular communication systems: Design and architecture. *IEEE Communications Magazine, 46*(11), 100–109.
7. Kargl, F., Papadimitratos, P., Buttyan, L., Muter, M., Schoch, E., Wiedersheim, B., et al. (2008). Secure vehicular communication systems: Implementation, performance, and research challenges. *IEEE Communications Magazine, 46*(11), 110–118.
8. National Transportation Statistics Book (2008). U.S. Department of Transportation, Research and Innovative Technology Administration. http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/2008/index.html [Online]
9. Traffic Safety Facts. (2006). [Online], http://www.nhtsa.gov/
10. Lee, U., Cheung, R., & Gerla, M. (2009). Emerging vehicular applications. In S. Olariu & M. C. Weigle (Eds.) *Vehicular networks: From theory to practice* (pp. 1–30). BocaRaton, FL: Taylor and Francis.
11. Xu, Q., Mak, T., Ko, J., & Sengupta, R. (2004). Vehicle-to-vehicle safety messaging in DSRC. In *Proceedings of the 1st ACM international workshop on vehicular ad hoc networks*, ACM, Philadelphia, PA, USA (pp. 19–28).
12. Abuelela, M., & Olariu, S. (2010). Taking VANET to the clouds. In *Proceedings of the 8th international conference on advances in mobile computing and multimedia (MoMM'10)* (pp. 6–13).
13. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., et al. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50–58.

14. Olariu, S., Eltoweissy, M., & Younis, M. (2011). Towards autonomous vehicular clouds. *ICST Transactions on Mobile Communications and Applications, 11*(7–9), 1–11.
15. Hussain, R., Son, J., Eun, H., Kim, S., & Oh, H. (2012). Rethinking vehicular communications: Merging VANET with cloud computing. In *Proceedings of the IEEE 4th international conference on cloud computing technology and science (CloudCom)* (pp. 606–609).
16. Hartenstein, H., & Laberteaux, K. P. (2008). A tutorial survey on vehicular ad hoc networks. *Communications Magazine, IEEE, 46*(6), 164–171.
17. Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., et al. (2008). Secure vehicular communication systems: Design and architecture. *Communications Magazine, IEEE, 46*(11), 100–109.
18. Hussain, R., Kim, S., & Oh, H. (2009). Towards privacy aware pseudonymless strategy for avoiding profile generation. In H. Youm & M. Yung (Eds.), *VANET. Information security applications*, Lecture notes in computer science 5932 (pp. 268–280). Berlin: Springer.
19. Jinyuan, S., Chi, Z., Yanchao, Z., & Yuguang, F. (2010). An identity-based security system for user privacy in vehicular ad hoc networks. *Parallel and Distributed Systems, IEEE Transactions on, 21*(9), 1227–1239.
20. Li, C.-T., Hwang, M.-S., & Chu, Y.-P. (2007). A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. *Computer Communications, 31*(12), 2803–2814.
21. Wlodarczyk, T. W., & Chunming, R. (2011). An initial survey on integration and application of cloud computing to high performance computing. In *Proceedings of the cloud computing technology and science (CloudCom), IEEE third international conference on* (pp. 612–617).
22. Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and privacy in cloud computing: A survey. In *Proceedings of semantics knowledge and grid (SKG), sixth international conference on* (pp. 105–112).
23. Zeng, K., & Cavoukian, A. (2010). *Modeling cloud computing architecture without compromising privacy: A privacy by design approach*. Ontario: NEC Company Ltd, and Information and Privacy Commissioner.
24. Bessani, A., Correia, M., Quaresma, B., Andr, F., & Sousa, P. (2011). DepSky: Dependable and secure storage in a cloud-of-clouds. In *Proceedings of the sixth conference on computer systems (EuroSys'11)*, ACM (pp. 31–46).
25. Cachin, C., Keidar, I., & Shraer, A. (2009). Trusting the cloud. *SIGACT News, 40*(2), 81–86.
26. Bernstein, D., Vidovic, N., & Modi, S. (2010). A cloud PAAS for high scale, function, and velocity mobile applications—With reference application as the fully connected car. In *Proceedings of the systems and networks communications (ICSNC), fifth international conference on* (pp. 117–123).
27. Yan, G., Rawat, D. B., & Bista, B. B. (2012). Towards secure vehicular clouds. In *Proceedings of the complex, intelligent and software intensive systems (CISIS), sixth international conference on* (pp. 370–375).
28. Yan, G., Wen, D., Olariu, S., & Weigle, M. C. (2013). Security challenges in vehicular cloud computing. *Intelligent Transportation Systems, IEEE Transactions on, 14*(1), 284–294.
29. Yu, R., Zhang, Y., Gjessing, S., Xia, W., & Yang, K. (2013). Toward cloud-based vehicular networks with efficient resource management. *IEEE Network, 27*(5), 48–55.
30. Whaiduzzaman, M., Sookhak, M., Gani, A., & Buyya, R. (2014). A survey on vehicular cloud computing. *Jouranl of Network and Computer Applications, 40*, 325–344.
31. Wolterink, W. K., Heijenk, G., & Karagiannis, G. (2011). Dissemination protocols to support cooperative adaptive cruise control (CACC) merging. In *Proceedings of the ITS telecommunications (ITST), 11th international conference on* (pp. 15–20).
32. Watson, J. D., Pellerito, M., Gladden, C., & Huirong, F. Simulation and analysis of extended brake lights for inter-vehicle communication networks. In *Proceedings of the distributed computing systems workshops, ICDCSW '07, 27th international conference on* (p. 87).
33. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling data in the cloud: Outsourcing computation without outsourcing control. In *Proceedings of the 2009 ACM workshop on cloud computing security, CCSW'09* (pp. 85–90).
34. Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. In *Proceedings of the cloud computing technology and science (CloudCom), IEEE second international conference on* (pp. 693–702).
35. Ngo, C., Membrey, P., Demchenko, Y., & de Laat, C. (2011). Security framework for virtualised infrastructure services provisioned on-demand. In *Proceedings of the cloud computing technology and science (CloudCom), IEEE third international conference on* (pp. 698–704).

36. Arif, S., Olariu, S., Wang, J., Yan, G., Yang, W., & Khalil, I. (2012). Datacenter at the airport: Reasoning about time-dependent parking lot occupancy. *IEEE Transactions on Parallel and Distributed Systems, 23*(11), 2067–2080.
37. Hussain, R., Abbas, F., Son, J., Kim, S., & Oh, H. (2014). Using public buses as mobile gateways in vehicular clouds. In *Proceedings of the IEEE international conference on consumer electronics (ICCE)* (pp. 175–176).
38. Hussain, R., Abbas, F., Son, J., & Oh, H. (2013). TIaaS: Secure cloud-assisted traffic information dissemination in vehicular ad hoc networks. In *Proceedings of the 13th IEEE/ACM international symposium on cluster, cloud, and grid computing (CCGrid)* (pp. 178–179).
39. http://articles.sae.org/11340/. Accessed on February 5, 2014.
40. Hussain, R., Abbas, F., Son, J., Kim, D., Kim, S., & Oh, H. (2013). Vehicle witnesses as a service: Leveraging vehicles as witnesses on the road in VANET clouds. In *Proceedings of the cloud computing technology and science, IEEE international conference on, (CloudCom'13)* (pp. 439–444).
41. Qin, Y., Huang, D., & Zhang, X. (2012). VehiCloud: Cloud computing facilitating routing in vehicular networks. In *Proceedings of the security and privacy in computing and communications (TrustCom), IEEE 11th international conference on* (pp. 1438–1445).

Rasheed Hussain received his B.S. in Computer Software Engineering from N-W.F.P University of Engineering and Technology, Peshawar, Pakistan in 2007 and M.S. degree in Computer Engineering from Hanyang University, South Korea in 2010. Recently, he completed his Ph.D. degree in Computer Engineering from Hanyang University, South Korea. His main research interests include information security and privacy issues in vehicular ad hoc network (VANET), information dissemination in VANET, VANET applications, cloud computing, and VANET-based clouds. He is currently working on framework, security challenges in VANET-based clouds, and new services in VANET-based clouds.

Zeinab Rezaeifar received her B.S. in Communication Engineering, from Shahid Bahonar University of Kerman, Iran in 2008 and M.S. degree in Network Communication Engineering, from Isfahan University of Technology, Iran in 2012. Currently she is working toward the Ph.D. degree in Computer Engineering from Hanyang University, South Korea. Her main research interests include routing in VANET (vehicular ad hoc networks), information security and privacy issues in VANET and DTN (delay tolerant network) in VANET.

Heekuck Oh received his B.S. degree in Electronics Engineering from Hanyang University in 1983. He received his M.S. and Ph.D. degrees in Computer Science from Iowa State University in 1989 and 1992, respectively. In 1994, he joined the faculty of the Department of Computer Science and Engineering, Hanyang University, ERICA campus, where he is currently a professor. His current research interests include network security and cryptography. Prof. Oh is the president of Korea Institute of Information Security and Cryptology, and is a member of Advisory Committee for Digital Investigation in Supreme Prosecutors' Office of the Republic of Korea. He is also a member of Advisory Committee for Internet Security under Korea Communications Commission.