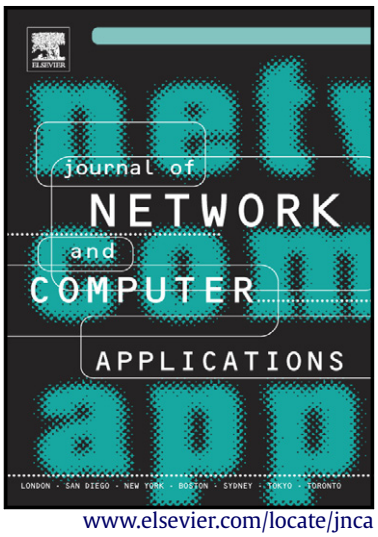

www.elsevier.com/locate/jnca

A Survey on Vehicular Cloud Computing

Md Whaiduzzaman, Mehdi Sookhak, Abdullah Gani, Rajkumar Buyya

PII: S1084-8045(13)00179-3
DOI: http://dx.doi.org/10.1016/j.jnca.2013.08.004
Reference: YJNCA1107

To appear in: *Journal of Network and Computer Applications*

Received date: 27 February 2013
Revised date: 6 June 2013
Accepted date: 20 August 2013

Cite this article as: Md Whaiduzzaman, Mehdi Sookhak, Abdullah Gani, Rajkumar Buyya, A Survey on Vehicular Cloud Computing, *Journal of Network and Computer Applications,* http://dx.doi.org/10.1016/j.jnca.2013.08.004

A Survey on Vehicular Cloud Computing

Md Whaiduzzaman [a], Mehdi Sookhak[a], Abdullah Gani[a], Rajkumar Buyya[b]

[a] Mobile Cloud Computing Research Lab, Faculty of Computer Science & Information Technology, University of Malaya, 50603, Kuala Lumpur, Malaysia; E-Mails: wzaman110054@siswa.um.edu.my; mehdi.sookhak@siswa.um.edu.my; abdullahgani@ieee.org

[b] Department of Computing and Information Systems, The University of Melbourne, Doug McDonell Building, Parkville Campus, Melbourne, VIC 3010, Australia; E-Mail: raj@csse.unimelb.edu.au

Abstract: Vehicular networking has become a significant research area due to its specific features and applications such as standardization, efficient traffic management, road safety and infotainment. Vehicles are expected to carry relatively more communication systems, on board computing facilities, storage and increased sensing power. Hence, several technologies have been deployed to maintain and promote Intelligent Transportation Systems (ITS). Recently, a number of solutions were proposed to address the challenges and issues of vehicular networks. Vehicular Cloud Computing (VCC) is one of the solutions. VCC is a new hybrid technology that has a remarkable impact on traffic management and road safety by instantly using vehicular resources, such as computing, storage and internet for decision making. This paper presents the state-of-the-art survey of vehicular cloud computing. Moreover, we present a taxonomy for vehicular cloud in which special attention has been devoted to the extensive applications, cloud formations, key management, inter cloud communication systems, and broad aspects of privacy and security issues. Through an extensive review of the literature, we design an architecture for VCC, itemize the properties required in vehicular cloud that support this model. We compare this mechanism with normal Cloud Computing (CC) and discuss open research issues and future directions. By reviewing and analyzing literature, we found that VCC is a technologically feasible and economically viable technological shifting paradigm for converging intelligent vehicular networks towards autonomous traffic, vehicle control and perception systems.

Keywords: vehicular networks, road vehicle control, intelligent transportation systems, cloud computing, vehicular cloud computing

1. Introduction

Recent improvements in software, hardware and communication technologies are empowering the design and implementation of several types of networks deployed in different environments. For the last few years, one such network that has received much attention is the Vehicular Ad-Hoc Network (VANET) (Olariu et al. , 2011, Zeadally et al. , 2010). A VANET is a set of moving vehicles in a wireless network that apply the Information Communication Technology (ICT) to provide state-of-the-art services of traffic management and transport. Presently, VANET has received significant consideration because of the prospect of enabling novel and attractive solutions in areas such as vehicle and road safety, traffic efficiency and Intelligent Transportation Systems (ITS) (Al-Sultan et al. , 2013, Hartenstein and Laberteaux, 2008). The promise of vehicular networking has led to a fast convergence with ITS and to the advent of Intelligent Vehicular Networks (Hossain et al. , 2010), which are anticipated to transform driving styles by creating a secure, safe and healthy environment that will ultimately encompass our busy city streets and highways. Thus, the intelligent vehicular networks will provide infotainment and will enable a new versatile system that enhances transportation efficiency and safety (Olariu et al. , 2013). Although many efforts have been made to reach these objectives, VANET has several drawbacks, such as the high cost of the service constrained communications due to the high mobility of the vehicle (Akbari Torkestani, 2012, Qin et al. , 2012).

Advances in vehicular technology have provided resources such as fixed storage devices, better computing power, cognitive radios, and different types of programmable sensor nodes. By using Wireless Sensor Networks (WSNs), intelligent applications enhance ITS and can improve both driving safety and traffic efficiency (Fonseca and Vazão, 2012). The arrival of mobile internet in vehicles brings together the innovative and, widely divergent benefits of the internet, and such developments have a tremendous social impact(Goggin, 2012). Therefore, in the futures, cars and vehicles will be ubiquitously furnished with communication, computing and sensing devices, and universal networks will make the internet available on the move. Thus, the driving experience will be more enjoyable, comfortable, safe and environmental friendly. Eventually, the billboards of our highways will be exchanged for in-vehicle advertising, where the driver can choose advertisement based on their needs. However, the remarkable array of on board computing abilities present in our vehicles is most likely not utilized by the applications mentioned above(Karagiannis et al. , 2011).

Mobile Cloud Computing (MCC) is a new paradigm that can be used by vehicle drivers to leverage services as a utility by a pay as you go model, and can process a large amount of data on demand anytime from anywhere. The drivers can use their mobile devices to connect to the cloud via the internet. MCC provides the essential environment and foundation to integrate platforms and technology that will monitor road safety by processing sensor network data using different mobile cloud architectures, such as Platform as a Service (PaaS). However, the mobile devices suffer from computing resources limitations (resource and battery restriction, processing time (Shiraz et al. , 2012). In addition, uploading real-time information on the cloud such as traffic jam or accident situation, by using the internet is costly and time consuming (Fernando et al. , 2012).

Vehicular Cloud Computing is a new technological shifting, which takes advantage of cloud computing to serve the drivers of VANETs with a pay as you go model. Thus, the objectives of VCC are to provide several computational services at low cost to the vehicle drivers; to minimize traffic congestion, accidents, travel time and environmental pollution; and to ensure uses of low energy and real time services of software, platforms, and infrastructure with QOS to drivers (Gerla, 2012). VCC can address the convergence of ITS and the tremendous computing and storage capabilities of MCC. Furthermore, VCC provides a technically feasible incorporation of the ubiquitous sensing of WSN, ITS and MCC for better road safety and secured intelligent urban traffic systems(Tekbiyik and Uysal-Biyikoglu, 2011, Wang et al. , 2011).

We are motivated because the communication, storage and computing resources available in the vehicles are generally underutilized. Combining these resources meaningfully will have a momentous influence on society. As such the underutilized vehicular resources including computing power, net connections and storage facilities can be pooled with those of other drivers on the road or rented to customers, similar to the way in which the resources of the present conventional cloud are provided. With current technology, Vehicular Clouds are technologically feasible and economically viable and will be the next paradigm shift. They will provide many benefits, including societal and technological impacts. The idea of a Vehicular Cloud is recent(Olariu and Weigle, 2009) and our emphasis is on the prospective applications and significant aspects of research challenges.

In this paper, we highlight Vehicular Clouds (Olariu, Hristov, 2013, Olariu, Khalil, 2011), an extension of conventional Cloud Computing with several new dimensions. Our aim in this paper is to help readers better understand the fundamental vehicular cloud computing mechanisms and point out the potential applications for improving vehicular network and road safety. We present a comprehensive taxonomy of vehicular networking and a comparative study between CC and VCC. In addition, we explain the VCC architecture, autonomous cloud formation and the extensive application scenario. Each vehicle in VCC can communicate to the other vehicles or the network infrastructures by using the vehicle to vehicle or the vehicle to infrastructure network communication. We describe a key management method to provide a secure communication channel in the vehicular network. Furthermore, we categorize the vehicular networks based on the security issues and solutions. The security and privacy of VCC, the research challenges and open issues are also discussed.

The rest of this paper is organized as follows: Section 2 discusses the vehicular network, which is the key component in vehicular clouds. Section 3 offers an overview of cloud computing, and section 4 provides an overview of VCC and services that motivated the vision of vehicular clouds. Section 5 focuses on the applications and possible uses of VCC and some distinguishing features. Security, privacy and key management issues are discussed in section 6, and section 7 discusses open issues and challenges in research. Finally, section 8 concludes with future remarks and new research directions.

2. The Vehicular Network

For the last few years, smarter vehicles, safer, and less stressful driving experiences have been realized. Currently, ordinary vehicles have devices such as GPS, radio transceiver, small-scale collision radars, cameras, on board computers and different types of sensing devices to alert the driver to all types of road safety conditions and mechanical malfunctions. Vehicles are becoming more sophisticated with on-board storage, powerful on-board computing capabilities, significant communication capabilities and less power limitations, which are supported by hosts of sensors, actuators, on board radar and GPS(Fleming, 2012, James, 2012).

Most types of vehicles can be equipped with Event Data Recorder (EDR) and on board GPS devices in the near future (Gabauer and Gabler, 2008, Mousannif et al. , 2011). The EDR is accountable to record necessary mobility attributes such as acceleration, deceleration, sensor and radar readings, lane changes and similar data. The logged data are properly documented and associated with a GPS reading. Along with the time interval, the EDR collects information such as the lowest and highest speed, the time and the position of the best acceleration/deceleration, and the location and target lanes for different lane changes. Additionally, all of the vehicles will have a number of sensors such as fuel tank level, tire pressure, engine, and external temperature sensors which provide readings for the EDR. Thus, these collections of computing and sensing capabilities, available internet and power supplies will require smart applications for vehicles to accommodate powerful on board computers with huge storage devices, which can collectively be known as networked computing centers on wheels(Olariu and Weigle, 2009), for example in-vehicle computing devices such as VBOX (SINTRONES, 2009) and NEXCOM (NEXCOM, 2011).

Table 1. List of acronyms

Amazon EC2	Amazon Elastic Computing Cloud
AVS	Autonomous Vehicular Cloud
CA	Certificate Authority
CaaS	Cooperation as a Service
CC	Cloud Computing
CRL	Certificate Revocation List
CRM	Customer Relationship Management
DoS	Denial of Services
DRP	Distributed Revocation Protocol
EBS	Elastic Book Store
EDR	Event Data Recorder
ENaaS	Entertainment as a Service
GPS	Global Positioning System
HOV	High Occupancy Vehicle
IaaS	Infrastructure as a Service
INaaS	Information as a Service
ITS	Intelligent Transportation Systems
MANET	Mobile Adhoc Network
MCC	Mobile Cloud Computing
NaaS	Network as a Service
OBU	On Board Unit
PaaS	Platform as a Service
PKI	Public Key Infrastructure
RSU	Road Side Unit
RTPD	Revocation Protocol of the Tamper Proof Devices
S3	Simple Storage Service
SaaS	Software as a Service
STaaS	Storage as a Service
V2I	Vehicle to Interface
V2V	Vehicle to Vehicle
VANET	Vehicular Adhoc Network
VC	Vehicular Cloud
VCC	Vehicular Cloud Computing
V-Cloud	Vehicular Cloud
VM	Virtual Machine
VPKI	Vehicular Public Key Infrastructure
WSN	Wireless Sensor Network

In 2009 in the US, there were 33,000 causalities and 2.2 million different injuries due to motor vehicle crashes. These crashes impact the society economically and incur an annual estimate cost of $230 billion dollars. For every single person in the USA, $750 dollars is spent. Moreover, the highway congestion costs $78 billion annually(Abid et al. , 2011).

Currently, congestion on highways is a daily event, and most of the time, we are not alerted by advance notification of congestion. For several years, the ITS forum has planned different solutions to reduce congestion. Among the proposed solutions is increasing the number of traffic lanes on highways and streets. A recent study

showed that this solution is ineffective in the long run and may even increase congestion and pollution levels. By conveying advance adequate notification(Olariu and Weigle, 2009), drivers could make educated decisions that would reduce the congestion, improve traffic safety, and save fuel and time.

Using cutting edge technological advancements are inevitable for an innovative and effective traffic hazard detection and monitoring systems. Thus, the idea of involving Mobile Ad-hoc Networks (MANET) for street and highways communications was inspired. A new sort of network, which engages an amalgamation of Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications, is known as a Vehicular Ad Hoc Network (VANET), which provides early notification of hazards and incidents to the drivers. Each vehicle, in the V2V system is normally accountable for gathering information on the incidents based on the feedback from closing vehicles. Regrettably, this system can lead to well-organized security attacks by marking incorrect inferences, which produce more congestion and a greater possibility of severe hazards. Thus far, much attention has been drawn by a noteworthy number of publications to solve this security problem in VANETs(Aijaz et al. , 2006, Lochert et al. , 2007, Lochert et al. , 2008, Yan, Olariu, 2009, Yan et al. , 2008).

VANET solicitations emphasize emergency alerts, cooperative driving, traffic status reports, collision avoidance and other apprehensions (Bilal et al. , 2013, Zarifneshat and Khadivi, 2013). The recent rapid convergence of ITS and VANET leading to the advent of Intelligent Vehicular Networks can ultimately transform our driving by building a secure, safe, healthy, and ubiquitous computing environment. Vehicle-based emerging communication and computing expertise will have a vast societal impact (Anda et al. , 2005, Czajkowski et al. , 2001, Festag et al. , 2008, Nakanishi et al. , 2006). To handle this envisioned societal impact, government, agencies and vehicle manufacturers have produced international associations devoted exclusively to VANETs, for examples, Car 2 Car Communication, Networks on Wheels, Honda's Advanced Safety Program, and the Vehicle Safety Communications Consortium among many others(Festag, Baldessari, 2008, Nakanishi, Yendo, 2006). The applications and the requirements for vehicular networks are illustrated(Karagiannis, Altintas, 2011) in Figure 1, in which several requirements of vehicular networks and applications are mentioned.

3. Cloud Computing and Mobile Cloud Computing

Mobile Cloud Computing is a recent emerging paradigm in the information technology arena. To better understand and leverage its technological advances, it is necessary to define both Cloud Computing and Mobile Cloud Computing.

The National Institute of Standards and Technology (NIST), gives a formal definition of CC: "Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"(Mell and Grance, 2011).

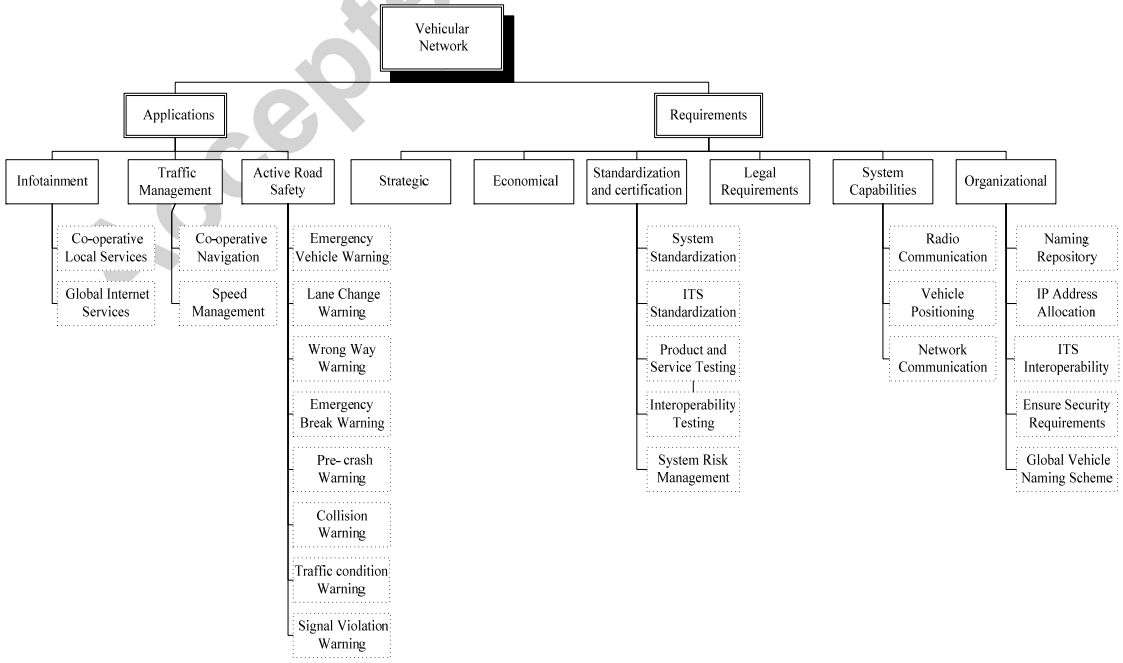

Fig. 1. Vehicular Networking: Applications and Requirements

The Mobile Cloud Computing Forum defines MCC as follows (MCC-forum, 2011):

"Mobile Cloud Computing at its simplest refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just smartphone users but a much broader range of mobile subscribers".

Mobile cloud computing is based on the fact that, without financing in infrastructure, businesses can function by renting the infrastructure and the necessary software for their organization.

Several features are unique in mobile cloud computing in terms of hardware and service provisioning(Dinh, Lee, 2011, Mell and Grance, 2011):

- Provides the users the facility of unlimited computing power accessible on demand
- Does not require early planning of resource provisioning.
- Upfront costs can be avoided by cloud users, which permit companies to start new small businesses and extend their hardware resources when they are only needed for popular applications.
- Ability to pay for computing resources up to the required time on a short-term basis and release them when they are no longer necessary.
- Services can be accessed from anywhere in the world.
- Capable of accessing the resources at any time.
- By virtualization techniques, one machine can serve several users and act as separate machines.
- By resource pooling, many customers can be served with a large networked data center.

3.1. Mobile Cloud Computing Architecture

Considering the definitions and services described in section 3, the architecture for MCC is illustrated in Figure 2. This architecture contains three layers, the Application layer (SaaS), the Platform layer (PaaS) and the Infrastructure layer (IaaS).

Each of these layers provides a specific service for users, which are explained as follows(Dinh, Lee, 2011) :

1. Infrastructure as a Service (IaaS): Several types of virtualization occur in this layer. Among the other resources, computing, network, hardware and storage are also included. In the bottom layer of the framework, infrastructure devices and hardware are virtualized and provided as a service to users to install the operating system (OS) and operate software applications. Therefore, this layer is named Infrastructure as a Service (IaaS).
2. Platform as a Service (PaaS): In PaaS, mobile operating systems such as Android, iPhone, Symbian and other OS, as well as database management and IMS are included in this section. This layer contains the environment for distributing storage, parallel programming design, the management system for organizing distributed file systems and other system management tools for cloud computing. Program developers are the primary clients of this platform layer.
3. Software as a Service (SaaS): Analytical, interactive, transaction and browsing facilities are included in the Application layer. SaaS delivers several simple software programs and applications as well as customer interfaces for the end users. Thus, in the application layer, this type of services is called Software as a Service (SaaS). By using the client software or browser, the user can connect services from providers via the internet and pay fees according to their consumed services, such as in a pay as you go model.

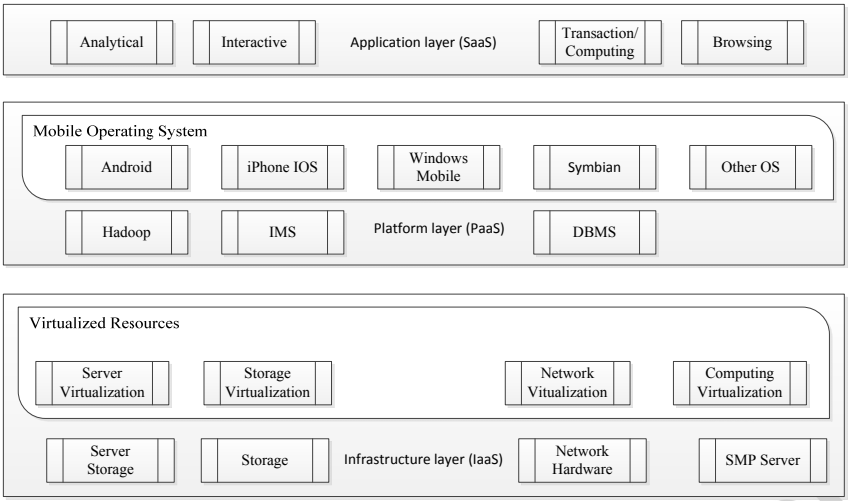

Fig. 2. Mobile Cloud Computing Architecture(Dinh et al. , 2011)

In the CC, MCC and Sensor-cloud architecture, a physical datacentre unit is in charge of performing the data computation and storage (Hossain, 2013), (Dinh, Lee, 2011). In VCC, however, the virtual aggregated of vehicles' resources generates the datacentre cloud (Gerla, 2012), actually they are the combinations of participating vehicles and RSU combined resources.

4. Vehicular Cloud Computing

The cloud computing paradigm has enabled the exploitation of excess computing power. The vast number of vehicles on streets, roadways and parking lots will be treated as plentiful and underutilized computational resources, which can be used for providing public services. Every day, many vehicles, spend hours in a parking garage, driveway or parking lot. The parked vehicles are a vast unexploited resource, which is currently simply wasted. These features make vehicles the perfect candidates for nodes in a cloud computing network. Some vehicle owners may agree to rent out excess on board resources, similar to the holders of huge computing and storage facilities who rent out their excess capacity and benefit economically. The travelers normally park their cars in airport parking spaces while they are travelling. The airport authority will power the vehicles' computing resources and allow for on demand access to this parking garage data center. Similarly, the drivers stuck in traffic congestion will agree donate their on board computing resources to help city traffic authorities run complex simulations designed to remove congestion by rescheduling the traffic lights of the city.

Recently, Olariu et al.(Eltoweissy et al. , 2010a, Olariu, Khalil, 2011) introduced the concept of a Vehicular Cloud (VC) that leverages the on board resources in participating cars. Some vehicles are parked for long times while others are stuck in congested traffic and move slowly, altering their position in some wireless network. Finally, our cars spend significant time on the road and may face dynamically fluctuating locations. In this case, the vehicles will help local consultants resolve traffic incidents in a timely fashion which is not possible with the municipal traffic management centers alone due to the lack of adequate computational resources. We expect that, the vehicles are capable of solving problems in many situations that may require an indefinite time for a centralized system.

Ultimately, by using self-organized autonomous resources, vehicles will serve on demand in real time to resolve large, serious problems of unexpected occurrences. The new vehicular clouds will help resolve technical challenges and contribute to complex transportation systems with their evolving behavior.

The Vehicular Cloud Computing can be defined as follows(Eltoweissy, Olariu, 2010a, Olariu, Hristov, 2013):

"A group of largely autonomous vehicles whose corporate computing, sensing, communication and physical resources can be coordinated and dynamically allocated to authorized users."

The VC concept is a further step to assemble the computational and situational consciousness of drivers in public and the greater portion of the population. The ultimate focus of the VC is to offer on demand solutions for unpredictable events in a proactive fashion (Olariu, Hristov, 2013). We must outline the structural, functional and behavioral characteristics of VCs and recognize the independent cooperation of vehicular resources as a unique feature of VCs. VCs are able to offer a unified incorporation and reorganized management of on board facilities. VC can adapt dynamically according to the changing application requirements and system environments.

In the near future a huge federation of VCs will be established ad hoc with the provision of alleviating massive emergencies because emergency evacuation in the face of a potential natural disaster that will abolish the standing infrastructure and lead to chaos with mobile networks. Therefore, a federation of VCs will offer a decision support system for a while and become the temporary infrastructure replacement.

In the USA, the Federal Communications Commissions allocated Dedicated Short Range Communications (DSRC) with a range of 75 MHz of the spectrum (5.850 to 5.925 GHz) in support of vehicular networking (Hussain et al. , 2012, Liu et al. , 2009). Moreover, roadside infrastructures such as inductive loop detectors, video cameras, acoustic tracking systems, microwave radar sensors, and access points are also helpful for VCC. As part of a project, Ford motor company combines social networks, GPS location awareness, and real-time vehicle data in ways that help drivers go where they want efficiently by using the cloud . Ford is equipped with cloud features called Ford SYNC, which connects customers to real time traffic updates, information, turn-by-turn driving directions, business, sports, weather, and news through voice commands. Ford's research into cloud-based technology includes adaptive vehicle dynamics, driver health well-being, and smart electrification. The car could monitor driver health condition and the smart phone apps can interact with the car. The software system provides access to vehicle performance data, networking services, voice recognition, social networking tools and other data (Ford-Comp., 2010). Recently, Toyota and Microsoft announced a new, $12 million partnership to bring cloud computing to Toyota vehicles(Squatriglia, 2011). The partnership will equip Toyota vehicles with the latest technology to access telecommunications information, streaming music, energy management, and GPS services, while on the road. Within 2015, by using Microsoft windows Azure cloud platform, Toyota will be possible to turn on heating and air condition while drive towards home. In addition, for hybrid car could select the best time for charging when energy cost is less expensive, check and monitor battery level for calculation how far it can go (Gayomali, 2011).We also consider another motor company named General Motors. The General Motor perception and vehicular control groups are engaged in developing a vehicle to vehicle communication system(Quick, 2011). GM provides the benefits of the connectivity include in-vehicle Wi-Fi hot spots for mobile devices, entertainment options like streaming video for passengers, real-time updates, and faster application downloads. By OnStar track maintenance and provide more accurate traffic data and Internet radio options and connect to personal mobile devices enabling embedded vehicle capabilities (Harris, 2013). The technology will provide viable solutions for essential safety information for drivers. Figure 3 presents a taxonomy of vehicular cloud computing which will be discussed in the following sections.

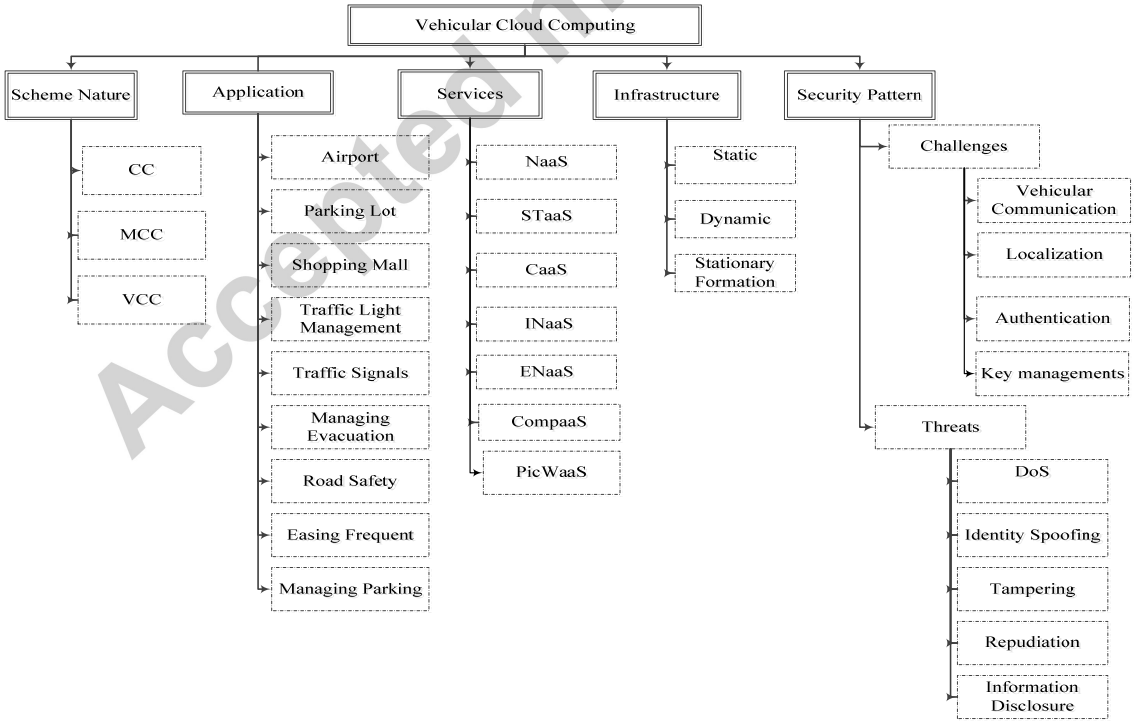

Fig. 3. Taxonomy of Vehicular Cloud Computing

4.1. Vehicular Cloud Computing Architecture

The Vehicular cloud computing architecture relies on three layers: inside-vehicle, communication and cloud. As illustrated in Figure 4, the first layer is the inside-vehicle layer, which is responsible for monitoring the health and mood of the driver and collecting information inside the car such as pressure and temperature by using body sensors, environmental sensors, smartphone sensors, the vehicle's internal sensors, inertial navigation sensors (INS), and driver behavior recognition (Chung et al. , 2009, Oliver and Pentland, 2000) to predict the driver's reflexes and intentions. Then, the information collated via sensors should be sent to the cloud for storage or for use as input for various software programs in the application layer, for example, delivers health and environmental recognition applications. We assume that each vehicle is equipped with an OBU that including a built-in navigation system, with a map and the location of a RSUs. The OBUs have a broadband wireless communication to transfer data through 3G or 4G cellular communication devices, Wi-Fi, WiMAx, Wireless Access in Vehicular Environment (WAVE)(Jiang and Delgrossi, 2008), or Dedicated Short Range Communication (DSRC) (Xu et al. , 2003).

The next layer of this architecture is called communication, which includes two parts: the vehicular-to-vehicular (V2V) systems via DSRC (Yang et al. , 2004). If a driver indicates the abnormal behavior on the road such as: changing direction dramatically, driving over the speed limit or the occurrence of a major mechanical failure in the vehicle, an Emergency Warning Messages (EWMs) will be generated and sent to the cloud storage and surrounding vehicles, which contains the geographical location, speed, acceleration and moving direction of the offender. The second component of the communication layer is vehicle-to-infrastructure (V2I), which is responsible for exchanging the operational data among vehicles, infrastructures and the cloud over wireless networks such as 3G, satellite or internet. The V2I component is used to augment the safety level of vehicles on highways by reducing the percentage of crashes, delays and congestion improve mobility, and provide Wireless Roadside Inspection (WRI) to automatically inspect commercial vehicles(Bordley et al. , 2012).

One of the most important advantages of VCC is data aggregation by using cloud storage, where various governmental and private agencies, particularly the police or the meteorology department can use the stored data in the cloud to perform various studies. However, the cloud which is the last layer of the VCC architecture, can compute the massive and complex computations in minimal time. The cloud layer consists of three internal layers: application, cloud infrastructure, and cloud platform. In the application layer, various applications and services are considered as real-time services or cloud primary services, which are accessible remotely by drivers, such as fuel feedback, human activity recognition, health recognition and environmental recognition.

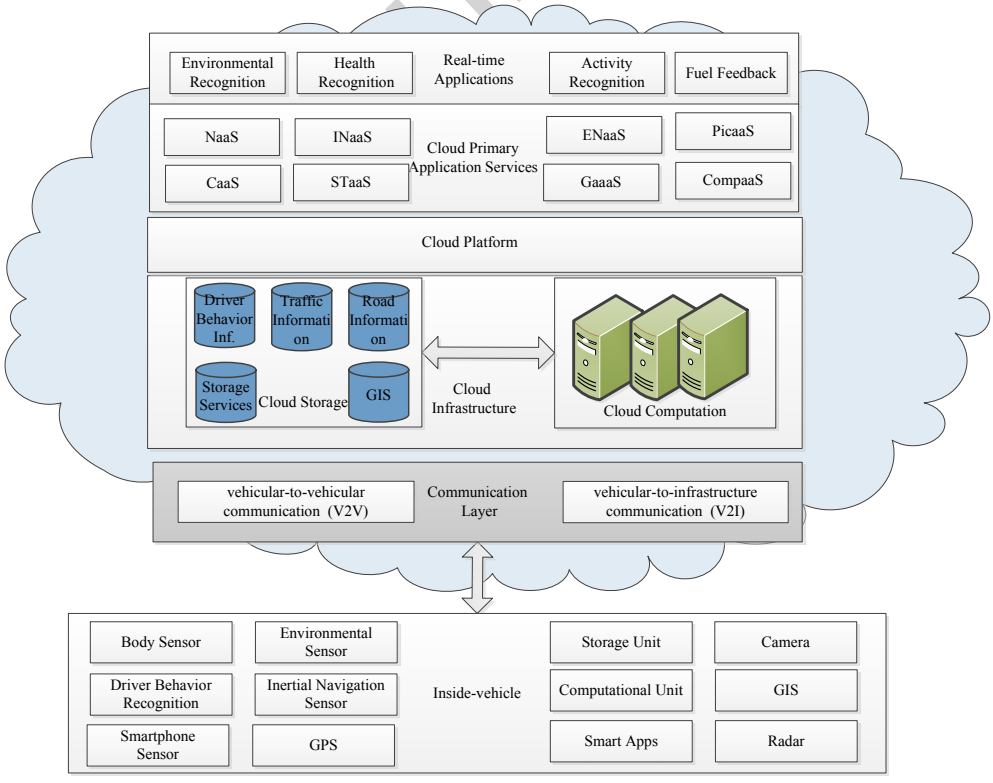

Fig. 4. VCC Architecture

Human activity recognition is used for an automated analysis (or interpretation) of ongoing events and their context of video data. In the primary services, several services are deployed, such as Network as a Service (NaaS), Storage as a Service (STaaS), Cooperation as a Service (CaaS), Information as a Service (INaaS), and Entertainment as a Service (ENaaS), which are discussed in the rest of this section. The cloud infrastructure consists of two parties: cloud storage and cloud computation. The data gathered by the inside-vehicle layer will be stored in the geographic information system (GIS), a road traffic control device or a storage system based on the type of applications. The computation part is used to calculate the computational tasks which provides faster performance, for example, the health recognition sensors send data to driver behaviour database in cloud storage

There are various components in the cloud primary application services layer which are called vehicular cloud computing services and are described as follows:

4.1.1 Network as a Service (NaaS):

Although some cars on the road have net connections, most cars do not have Network as a Service. The cars with internet access can offer this facility for other cars, if they need the internet, while on the move. On the road while driving, many drivers will have internet connections through mobile phone networks or other fixed access points. Today, PCs and laptops are connecting to the net but are underutilized, and in the same way, this road network resource may remain unutilized. These essential resources can be shared on the road by giving net access to those who are interested in renting it from the drivers. The driver who is agreeing to share this resource has to advertise such information among all other vehicles around them on the highway. Information can pass among the existing vehicles in the local proximity who can act as an access point hop to the internet. Given the relatively small speed difference between cars travelling in the same direction, we then compare the system to normal mobile ad hoc networks, MANETs, which consists of fixed access points and a number of mobile computing devices. These current protocols can be used by the vehicles in a certain local area by available access points or cars that have an internet connection (Mousannif, Khalil, 2011).

4.1.2 Storage as a Service (STaaS)

While some vehicles have plenty of on-board storage capability, and other cars it is predicted that some other vehicles may require additional storage to run their applications. Because of the small size and the inexpensive price of storage, it is anticipated that the on-board computer of vehicles will have multiple Terabytes of storage. Hence, the vehicles with additional capability will provide storage as a service (Arif et al. , 2012).

It is clear that the storage as a service in vehicular networks is different from offering network access or computing resources. Although the probable customers benefit instantly from computing and network access, they are able to use the storage for backup purposes or for p2p applications over an extended period of time. This limitation may be a real obstacle for renting car storage as a backup or p2p applications (Olariu, Hristov, 2013).

One of the important techniques to overcome this issue is using Replication-based storage in which multiple copies of the original file will be stored in multiple storage to increase the availability and reliability of data on untrusted storage or the vehicles that leave the place (Chen et al. , 2010). Whenever a vehicle leaves the place, the intact copy of the file can be used. Figure 5 shows when at the server 3 becomes unavailable, the non-corrupted server (server 1) is used to generate a new copy based on replication method.

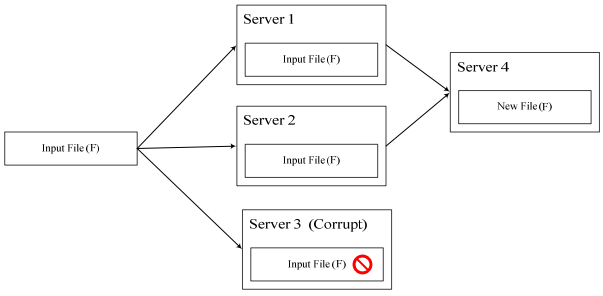

Fig. 5. Replication-based Storage as a Service

4.1.3 Cooperation as a Service (CaaS)

Vehicular Networks provide a variety of new services, such as driver safety, traffic information, warnings of traffic jams and accidents, weather or road conditions, parking availability and advertisements. Recently, 3G

networks and sophisticated ITS have been used to offer such services, but these services come with a cost at the hardware and network levels. We can consider a new form of community service that is called CaaS. It allows drivers to obtain services using very minimal infrastructure, if the infrastructure exists and by V2V communications if no infrastructure exists. CaaS uses the appliance where the subscriber states their preferences for a service, and cars subscribed to the same service will help to give the subscriber important information about the service or by announcing information to the network. CaaS can divide the network into clusters, as in Content-Based Routing for intra cluster communications and delay and Disruption Tolerant Network routing for inter cluster communications(Arif, Olariu, 2012).

Mousannif, Khalil (2011) introduced Cooperation as a service(CaaS) which provides several free services without any additional infrastructure, by exploiting the advantages of vehicular cloud computing. CaaS uses a mechanism by which the drivers express their interest for a service or a set of services network where the cars having the same service subscribed to cooperate the subscriber by necessary information regarding the service he subscribed to by publishing the information to the network. CaaS formulates the network as a cluster by using Content Based routing (CBR) for intra cluster communications and geographical routing for inter cluster communications.

In VANETs, Content based data dissemination, where information is routed based on the content rather than the destination address. However, it requires a one-tree structure network topology, almost impossible to maintain when the size of the network increases. The high mobility of nodes in the network may make this tree maintenance issue difficult because a tree may become partitioned into a number of trees leading to other issues finding a connectable path to merge those trees. By taking advantage of the benefits of CBR and reduce its disadvantages, more than one tree structure in the network is allowed. Each tree will represent a cluster whose size and depth are appropriately chosen to allow a proper maintenance of the trees. CBR is used for intra-cluster communications; subscriptions of all members of the cluster are forwarded to a clusterhead and updated regularly to deal with the continuous movement of the nodes. The intra-cluster structure considers the following roles to set up a routing infrastructure: Clusterhead node is responsible for summarizing subscriptions of the cluster members and forwarding them to other clusters. It is also responsible for delivering publications to interested nodes inside the cluster. Broker node acts mainly as a relay. Each broker holds a subscription table used to determine how to disseminate subscriptions/publications along the tree. Subscriber node expresses its interest in a service and the Publisher node publishes information about services in which vehicles might be interested.

4.1.4 Computing as a service

Recent US-DOT statistics disclose that the registered vehicular fleet on American streets and roadways is almost 256 million vehicles strong and growing progressively. They also reveal that most of these vehicles spend several hours per day parked in a parking garage, parking lot, or driveway (ITS_Committee, 2008). While some vehicles are parked in the parking for a period of time, the computing and storage resources of these vehicles are unused and the opportunity for their use is unexploited. VCs can aggregate the computing and storage capabilities of parked cars and presents it as a new service to customers.

4.1.5 Pictures on a Wheel as a Service

Mario Garla et al. described VCC services as a picture on a wheel where the images can be delivered on demand to the citizen by using on board car cameras. This could be used as survey applications exploiting the mobility of the vehicles extend the coverage beyond the reach of static sensors.

Mobile phones can be used as a source of this service. However, battery and resource constrained and there is chance of security issues and the risk of exposure. On the other hand, for VCC there is no concern about power and resources and that much security concern or exposer problem. The Pics-on-Wheels service selects a group of vehicles to take photo shots or videos of a given urban landscape for limited timeframe as requested by a customer. To participate in this Service, vehicles should register to the centralized cloud manager. They also upload their own GPS location periodically to the cloud manager. The on board navigation system in each vehicle maintains the trace of the vehicle for a predefined time period. Then the main concern is to select the vehicle for shooting images. After suitable and careful consideration vehicle will be selected. In case of no vehicle in the target area or deny to service request, then this service will be unavailable. They propose an algorithm for best vehicle selection for taking the shot. At the time of the accident, this service can help for forensic and insurance claim purpose.

4.1.6 Information as a Service (INaaS) and Entertainment as a Service (ENaaS)

On the move, drivers often need some sort of information for safe driving, such as road conditions, advance warnings, news of large events, or any type of sudden road crash or emergency situations. All of these factors can influence our driving and those services together can be recognized as Information as a Service (IaaS).

For a comfortable journey on the road, people now need entertainment to make their journey as enjoyable as possible. Therefore, many commercials that are found beside the road today will come to the car screen of the driver soon. These advertisements, movies, and commercials will open a new era of entertainment for the road users and make life more comfortable and enjoyable. Thus, these types of facilities are identified as entertainment as a service on the highway.

4.2. Cloud Computing (CC) Versus Vehicular Cloud Computing (VCC)

VC in a static mood has the same behavior as conventional cloud computing (CC). Our cars remain on the road busy with various dynamically changing situations or events every day. The occurrence of vehicles in close vicinity to an incident is very often an unplanned process which can be called mobility. Again, the resources of those vehicles that form a VC to alleviate the event must occur naturally, which can be called autonomy. Conventional clouds do not have these features which are considered a significant major characteristic of VCs. By analyzing these characteristics, we have outlined an extensive comparative study of CC and VCC, as shown in Table 2.

4.3 Formation of VC Infrastructure Perspective

In this subsection, several VC formation scenarios are outlined.

4.3.1 Stationary VC Formation

In several cases a VC may act as a normal conventional cloud especially in static environments. Let us, consider a small company that is hiring people and concentrating on providing IT services and support. By allowing carpooling, we will have many cars parked in the company's parking lot. All day long, those cars are standing idle with computing resources. By providing the necessary rewards, the company may actively request the formation of a stationary VC for its staff, who will rent the resources. The combined static VC will accumulate the storage resources and computational power of the participating vehicles and form a computer cluster and a gigantic distributed data storage center, which with proper security safeguards, can become an important asset for any corporate company (Eltoweissy et al. , 2010b), (Olariu, Khalil, 2011).

4.3.2 Linked with a Fixed Infrastructure

The creation of a VC can evolve in an area instrumented and be deployed by some form of a static infrastructure that supports the management of various events. In urban areas, such infrastructure contains cameras, traffic lights, and utility or street-light poles. In roadways, the static infrastructure contains the road side units, Inductive Loop Detectors (ILDs) and other ITS hardware deployed in the monitoring and management of traffic. Figure 6 shows how RSUs are used and deployed in the VC.

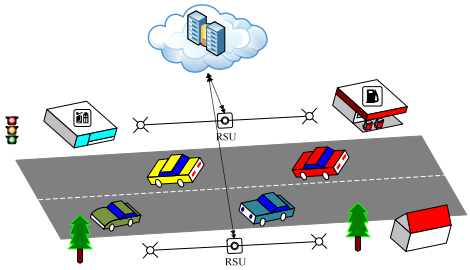

Fig. 6. Cloud Formation with Fixed Infrastructure

Table 2. Comparative study of CC and VCC

Characteristics	Description	CC	VCC	Ref.
On demand elastic application	Get the required service when necessary and applications can run and uses resources dynamically.	Yes	Possible	(Buyya et al. , 2009), (Olariu, Hristov, 2013)
Virtualization	Several requests can be served by one machine but pretend to be separate machines.	Yes	Yes	(Pelzl et al. , 2009)
Pay as you go	The business model of paying and using the services.	Yes	Possible	(Buyya, Yeo, 2009), (Olariu, Hristov, 2013)
Any time any where	Services are available and online every moment from anywhere.	Yes	No	(Buyya, Yeo, 2009)
Network as a Service	Providing communication and network-related services.	Yes	Yes	(Arif, Olariu, 2012)
Storage as a Service	Provide pooling storage and serve this to the user as a storage service provider.	Yes	Yes	(Arif, Olariu, 2012)
Corporation as a Service	By carpooling, information and entertainment services are provided.	Possible	Yes	(Mousannif, Khalil, 2011)
Commercials and Infotainment	Commercials, information and entertainment for the drivers.	Yes	Yes	(Dinh, Lee, 2011),
Planned and unplanned disaster management	Disaster management using roads and vehicles.	Possible	Yes	(Eltoweissy, Olariu, 2010b)
Large traffic event management	Managing large-scale traffic management.	Possible	Yes	(Eltoweissy, Olariu, 2010b)
Moving Network Pool	Moving vehicles are dynamically pooled and make a huge network.	No	Yes	(Gerla, 2012)
Autonomous Cloud formation	Running or idle vehicle can make a cloud autonomously.	No	Yes	(Eltoweissy, Olariu, 2010b)
Automatic Cloud Federation	On the move, several clouds can be formed as a large single cloud.	No	Yes	(Gerla, 2012)
Trust and authentication management	Provide trust management and authentication to build confidence.	Yes	Yes	(Yan et al. , 2013)
Mobility of clouds	Clouds or Cloud provider serves while moving.	No	Yes	(Dinh, Lee, 2011),

VC benefits from interaction with the existing static infrastructure. An example is a city block where a minor traffic incident has occurred. The congested vehicles will accumulate all of their computing resources as a pool, and indicate the higher authority to reschedule traffic lights to de-congest that area as soon as possible. In this particular case, rescheduling traffic lights does not require several VC federations (Olariu, Hristov, 2013).

4.3.3 Dynamic Formation

The architectural support of the formation of this type of VC will involve the following elements. A broker elected among the vehicles will try to form a VC. Then, the broker will obtain initial authorization from the authority to form a VC. Among the vehicles, one will secure authorization and succeed, and the others will formulate the coordination and help to form the VC. A unique broker will invite the vehicles for VC formation in the area after receiving authorization. However, the responses from the cars will truly have an autonomous basis. When a sufficient number of cars are in place, then the broker will decide to announce the VC formation. Finally, the VC will accumulate computing resources to form a large computing entity similar to a supercomputer. By using a digital map of the area, the VC will instruct the authority for approval of the proposed plan and then implement it. After accepting and implementing the proposal, the VC is dissolved. In this scenario, it is necessary to rearrange the traffic lights in a large area and hence motivate the formation of

several VCs. The dynamic formation of Autonomous Vehicular Cloud (AVC) is shown in Figure 7(Olariu, Khalil, 2011).

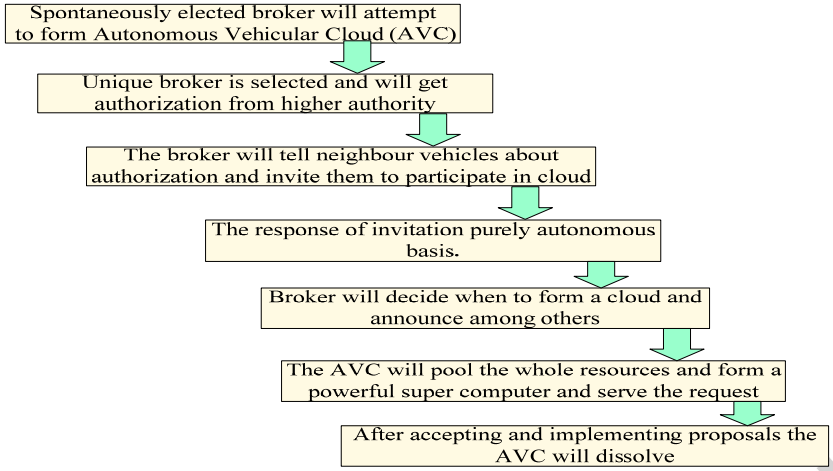

Fig. 7. Dynamic AVC Formation

5. Applications of Vehicular Cloud Computing

In this section several possible implementation scenarios and the application outcome of VCC are discussed:

5.1. An Airport as a DataCenter

While some cars are parked in the long-term parking lot of a central airport for several days, this pool of cars can be used as a basis for a datacentre at the airport. The cars that are participating in the vehicular cloud need to be plugged into a standard power outlet and be connected to the Internet by cable. However, the main issue to schedule resources and to assign computational tasks to the various cars in the vehicular cloud considering with the time-varying nature of the arrival and departure rates. Arif, Olariu (2012) were the first to address this issue by proposing a time-dependent parking lot occupancy model based on the Eucalyptus open-source cloud-computing system (Nurmi et al. , 2009). The Eucalyptus model involves a client-side API on one side of the network communicates with a cloud controller that is in charge of managing multiple cluster controllers.
Arif, Olariu (2012) considered a datacentre manager as a cloud controller to create a relationship with the outside world, which includes four components (Figure 8): (1) broker daemon: negotiates with various potential clients that require the cloud service and has authority to accept possible requests, (2) virtualization agent: is responsible for configuring the available cloud resources to meet the commitments underwritten by the broker in the best way, (3) resource manager: that discovers and manages the dynamically changing cloud resources based on the arrival and departure rates of vehicles, and (4) task scheduler: is in charge of allocating computational tasks to each cluster - that interfaces with the vehicles - or even to individual vehicles of a cluster based on the amount of available resources.

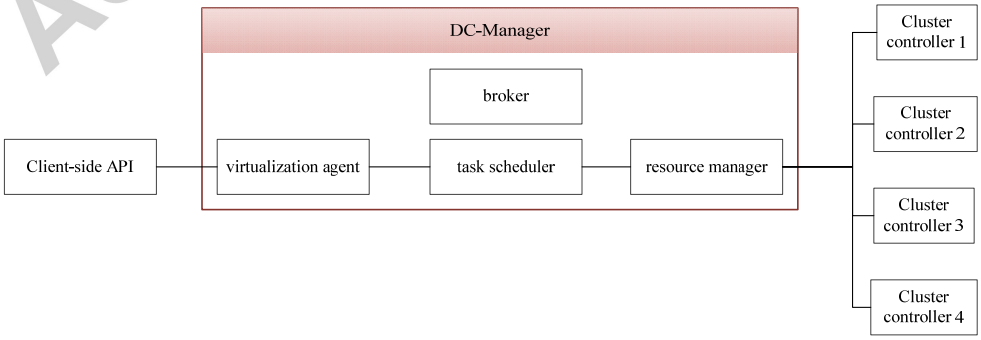

Fig. 8. The architecture of datacentre in the airport

5.2. Parking Lot Data Cloud

Recent US-DOT statistics disclose that the registered vehicular fleet on American streets and roadways is almost 256 million vehicles strong and growing progressively. Also, statistics reveal that most of these vehicles spend several hours per day parked in a parking garage, parking lot, or driveway. Still, the computing and storage resources of these vehicles are unused and the opportunity for their use is unexploited (Arif, Olariu, 2012). Let us consider a small company employing a few hundred people providing IT services. We allow for carpooling and vehicles remain parked in the car park. In those vehicles, the computational resources have no use and remain idle for hours. The company can give incentives for employees who will rent the resources for the VC formation. Hence, the participating vehicles in the car park create a computer cluster and provide ample facilities for secured data storage.

5.3. Shopping Mall Data Center

In the future, we will move on to more dynamic scenarios. US statistics show that mall customers spend hours shopping everyday with some peaks over the weekends or during the holiday season. A recent study performed on teens shopping at malls showed that 95% of shoppers spent more than one hour at the mall while 68% of them spent more than two hours (Scarborough-Research, 2009). Thus, thousands of customers visit different malls every day, parking their cars in the mall garage or parking lot and spending a couple of hours doing their shopping while leaving their computing resources in their vehicles idle. The Mall management can use this unutilized hardware by allowing as a pay as you go service for computing resources through the internet. The shop management can make lucrative offers for the customers to share the parked vehicle resources, for example, discounted at the mall, free parking or similar parking facilities elsewhere. However, one of the big challenges of short-term parking as a data center is its dynamic nature considering with the high rate of arrival and departure and time limitation per car.

5.4. Dynamic Traffic Light Management

Todays, due to increasing a number of vehicles on the roads, the traffic is becoming a daily phenomenon which wastes the valuable time and energy of human, threatens the health of citizens, and needs the huge computational effort to be solved. One of the best solutions to overcome this issue is to allocate the right amount of resources rather than pre-allocating of huge resources as a basis for the worst situation. Let us consider an event such as a football match that is attended by thousands of people, where a traffic jam may occur at the end of the game. Although a number of studies are performed to address this issue by leveraging VANETs and ITS, they are not able to report traffic problems quickly and usually cannot provide a traffic mitigation plan. VCC is able to present a more efficient and economical way to solve the congestion by providing the required resources from the available vehicles participating in the traffic and involving them in finding a solution autonomously without waiting for officials react (Eltoweissy, Olariu, 2010b).

5.5. Optimizing Traffic Signals

Traffic signals set the signal cycle length and the green phase lengths. Signal system optimization is currently occurring off line at either the isolated intersection or the corridor level. The time periods are defined by the timing plans for certain time periods, such as the weekday morning or afternoon peak hours. One of the disadvantages of this method is that it requires data on traffic turning movements that are regularly collected to ensure that the signal timing plans are suitable for the current traffic volume conditions. Another disadvantage is that this scheme does not cope well with uncertain changes in traffic situations. Thus, VCs can maximize the signal system performance by making dynamic use of a vehicular network.

Wooseong and Gerla (Wooseong and Gerla, 2011) proposed a Navigator Assisted Vehicular route Optimizer (NAVOPT) based on the Vehicular Cloud and the Internet cloud in which the vehicular cloud is sensing the segment traffic congestion by transferring the time, GPS coordinates and final destination to a Navigation Server through on board vehicle navigators. The navigator server– that is implemented in the Internet Cloud– is in charge of computing the optimal routes by constructing traffic load map and the traffic pattern matrix and estimating road segment loads and delays. Finally, the server returns the optimized routes to the vehicles.

5.6. Self-Organized High Occupancy Vehicle (HOV) Lanes

For precise and predefined travel time, HOV lanes carry a vast number of cars, which carry many passengers especially during periods of high traffic congestion. However, the authorities know about the congestion and

have the official power to set up HOV lanes, but they do not have sufficient resources to compute and assess the situation to establish the time frame to use the HOV lane to ease the effects of traffic jam. VCs could set up HOV lanes dynamically by stimulating the flow of traffic and reducing the travel times for HOV lanes. VCs can dynamically provide the solution by gathering data from on board vehicle sensors, and this type of solution is not possible with the current technology (Eltoweissy, Olariu, 2010b).

5.7. Managing Evacuation

Computationally intensive traffic modelling enables evacuations from a metropolitan area to be measured. Transportation agencies often develop simulations to identify potential traffic control strategies for possible evacuation events. Thus, evacuation events can be subdivided into cases where prior notice of an imminent event is provided.

The natural ways a VC can work with the disaster response authority for evacuation to afford travel time calculations and judge the availability of resources, such as food, water, shelter, gasoline. The self-organized vehicles participating in the evacuation procedure will form one or a combination of vehicular clouds, which will work closely with the emergency rescue response office. The emergency management team uploads the latest information regarding open shelters, food, and water to the main server computer.

In contrast, for the unplanned evacuations, no advance notice is possible because evacuations are in response to a totally capricious event. Therefore, planning for no notice events is much more difficult for the location and type of events. The modelling large scale unnoticed events are based on a number of assumptions, so we are not sure whether this modelling really demonstrates a real event response.

Alazawi et al. (2011) proposed an intelligent disaster management system by exploiting the Intelligent Transportation System, Vehicular adhoc network, and mobile and cloud computing technology Hybrid vehicular communications based on V2I and V2V protocols are opportunistically exploited. Traditionally, information about traffic on a road is only available through inductive loops, cameras, roadside sensors and surveys. VANETs provide new arenas for collecting real-time information from onboard sensors on vehicles and for quick dissemination of information. The information collected through individual vehicles participating in VANETs can be integrated together to form a real time picture of the road situation. The various ITS stakeholders working together to make VANETs based ITS a reality. Hundreds of projects are underway in the different countries worldwide for helping with research, innovation, and standardization (Mehmood and Nekovee, 2007, Schweiger et al. , 2011).They propose a system architecture consists of three main layers such as the cloud infrastructure as service, the intelligent layer, and the system interface. The system should acquire real time data and establish communication through V2X hybrid protocol, process the data and devise the optimum strategy by data analysis, control and coordinate the road traffic through disseminations information and management of the available infrastructure. They evaluated the model with simulations and modeling and found the effectiveness in terms of effective improved disaster evacuation management characteristics.

5.8. Road Safety Message

New cars have embedded sensing devices for proficient and safe operation. The cameras help the driver by tracking the lines on the road and assist them in staying in the lane. Thus, cars have a sensor node, and a VC can form dynamically with a large wireless sensor network. Vehicles query the sensors of other cars in close proximity to increase the fidelity and obtain a valuation of the potential road hazard ahead, the road conditions, speed breakers, holes, and black ice. However, the present VANET design will not give us the coordination of safety measures and a faster solution (Eltoweissy, Olariu, 2010b).

5.9. Easing Frequent Congestion

Few drivers seek diversion and alternate routes using local roads. Making decisions while driving is challenging, especially when many cars try to go towards the same road and the local road capacity is exceeded thus causing deadlocks. The traffic advisory and contemporary ITS system are both slow to solve traffic congestion and have no alleviation plan. An AVC centered solution can be suitably solved. Thus, vehicles in the vicinity will be able to calculate the impact of the local road and the cause of the congestion in the traffic flow and can determine the bottleneck (Eltoweissy, Olariu, 2010b).

5.10. Managing Parking Facilities

Finding a suitable parking space in the area close to university or in big cities would benefit from the help of an automated parking management utility. Recently, the known solutions based on a unified style from single parking garages and parking meters have been combined and then spread to the community. Todays, the drivers

are able to find a parking space by using their smartphone applications (e.g., Smartpark, ParkMe and ParkMate). However, these applications have some drawbacks that have not been addressed, such as: covering the limited point of the world and the need for accessing Internet. In addition, many studies on VANET-based parking schemes have been proposed in recent years (Panayappan et al. , 2007, Rongxing et al. , 2009, Szczurek et al. , 2010, Zhu et al. , 2013) which can be improved by using VC services. We visualize the real time pooling of parking locations using the statistics in the city from various locations. The vehicles that form the VC in a specific neighbourhood will manage real time data of available parking spaces and instruct drivers to the most suitable position.

5.11. VC in Developing Countries Perspective

Due to lack of sophisticated centralized decision support systems and infrastructure, the concept of VC will be very important in developing countries as well. Moreover, VCs will play a vital role in making a vast number of computing resources accessible through a vehicular network by using many computing applications dynamically, which are not possible to use with the current infrastructure.

Figure 9 shows the various types of VCC application scenario. The VCC Application Scenarios are divided into three types: dynamic VCC, static VCC and static/dynamic VCC.

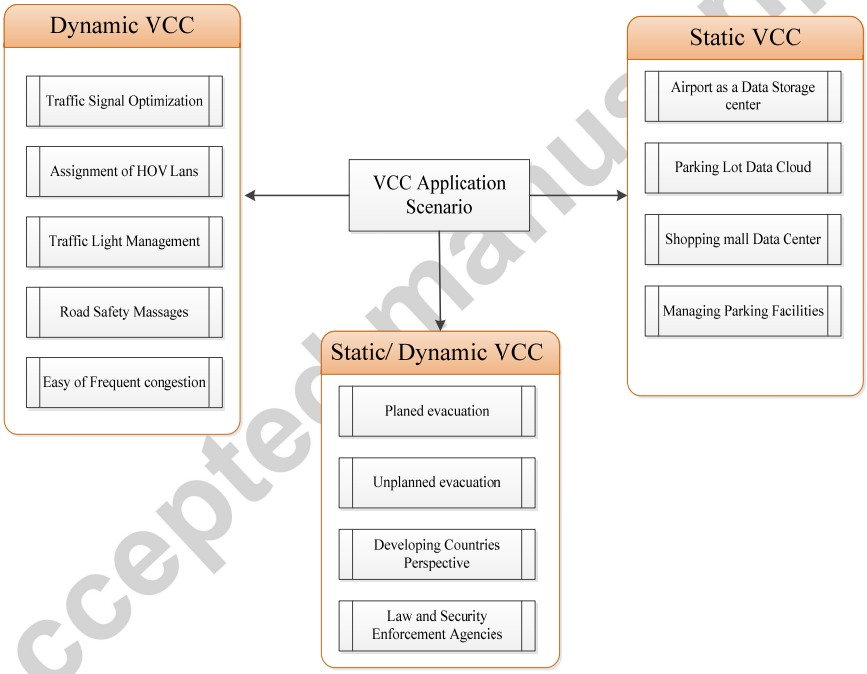

Fig. 9. Various types of VCC application scenarios

6. Security and Privacy in Vehicular Cloud Computing

Olariu et al.(Olariu, Khalil, 2011) claim that, there are several resources to compute or store data that are sometimes not used completely in vehicles. By using Cloud Computing capabilities, these resources can be shared among surrounded vehicles that need them to perform their tasks better. To provide a more comprehensive control system with better performance for vehicles, the use of wireless sensors is unavoidable(Park et al. , 2009).

Vehicle Cloud Computing is a new hybrid technology consists of the combination of various networks such as mobile ad hoc networks, wireless sensor networks, vehicular ad hoc networks, and cloud computing to provide better services for automatic cars such as control car movements and handling navigation system to provide reliable and shorter routes, which also ensures safety (Olariu, Hristov, 2013).

Security and privacy are the two major challenges for all wireless or wired networks that allow users to share the same set of resources. As shown in Figure 10, the architecture of VCC can be classified into three layers: networks, the wireless communication channel and cloud computing. The first part is responsible for collecting

the information and events from the environment. Then, this information is transferred to the cloud by using the wireless communication channel as a wireless access point. Therefore, the security of vehicular networks depends on providing the security of these three layers.

1. Security of the network layer (VANET, WSN)
2. Security of the transmission layer (wireless communication channel)
3. Security of the cloud computing

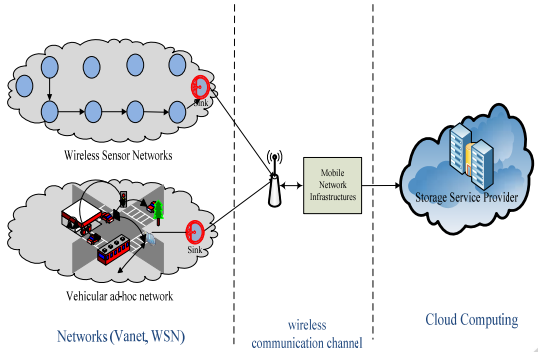

Fig. 10. Data Transmission in vehicular cloud computing

In this paper, the security and privacy of VC are classified in three subsets such as security threats, security requirements, and security challenges (Figure 11). The security threats include various security issues that threaten the security of VC. There are some requirements that should be met to provide a secure environment in the VC. In the last group, some security challenges of VC and the applicable solutions to overcome these challenges are surveyed. Although, some security solutions of vehicular network are applicable in VC, due to a few numbers of specific security solutions for the VC, this area needs more consideration.

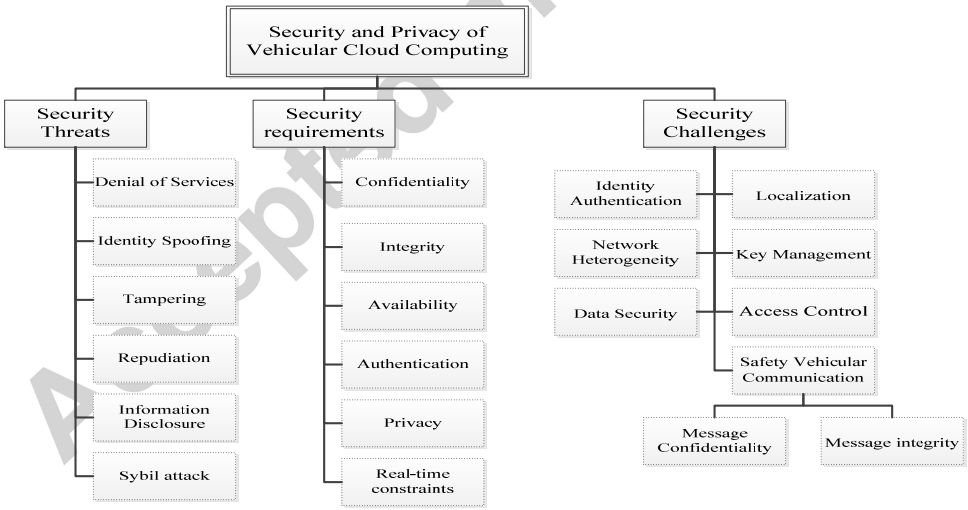

Fig. 11. Taxonomy of security and privacy of vehicular cloud

6.1. Security of Vehicular Networks

A vehicular network is one of the most important technologies to implement different applications related to vehicles, traffic, and safety. There are several challenges that threaten the security of vehicular networks. Providing security in a vehicular network is more difficult than in other networks such as WSN due to the high mobility and wide range of vehicles (Karagiannis, Altintas, 2011). As it is shown in Table 3, the security challenges of vehicular networks can be classified into five parts, namely, confidentiality, authentication, non-repudiation, localization and verification of data. For example, non-repudiation is the assurance that entities cannot deny receiving or sending a message that originated from them. In addition, data-centric trust and

Table 3. Vehicular Networking: Security Issues and Solutions

Security Issue	Solution	Authors	Description
Secure Localization	Plausibility Checks	(Song et al. , 2004), (Harsch et al. , 2007)	1. Secure Location Verification (SLV): it uses a distance bounding, plausibility checks and ellipse-based location estimation to verify the position claimed by a vehicle. 2. Position Based Routing (PRB): is constructed based on beaconing, location service and forwarding.
	Logic Reception Beacons	(Vora and Nesterenko, 2006)	Synchronized acceptor and rejector nodes
Authentication and Privacy	Tamper Proof GPS	(Hubaux et al. , 2004)	Each vehicle has a GPS receiver to register its location and send this information to others
	Identity Based Cryptography	(Kamat et al. , 2006)	Using Identity-Based method to verify trail between the pseudonyms and the real identities of the vehicle
	Pseudonymous-	(Calandriello et al. , 2007)	Ensures that cryptographically protected message should not allow for their sender to be identified.
	Attribute-Based Encryption	(Verma and Huang, 2009)	Each vehicle has a set of attribute and each attribute is associated with a single public key. The private key of the vehicle, however, includes several shared keys. Each shared key is installed in a different vehicle to communicate each other.
Confidentiality	RSUs to control a region	(Raya et al. , 2006a)	Vehicles that entering a region should register within that RSU to receive a symmetric public key for encrypting the communications between vehicles for a period of time.
	self-organizing geographical regions	(Huang et al. , 2010)	Group communication is established based on the geographical location of vehicles and a node is automatically selected as a group leader to generate and distribute a symmetric public key.
	Group-based solution	(Sampigethaya et al. , 2005)	The group leader acts as a proxy between RSUs and the group members.
Non-Repudiation	Digital Signature	(ITS-Committee, 2006), (Boneh and Shacham, 2004)	The following methods can be used to achieve the goal: 1. Elliptic Curves Cryptography 2. Group signatures
Verification of Data-centric	Proactive security concepts	(Raya and Hubaux, 2007), (Papadimitratos et al. , 2008), (Calandriello, Papadimitratos, 2007),	It can be used for traffic safety applications in vehicular networks, which includes the following solutions: 1. Signature based 2. Proprietary System design 3. Tamper Resistant Hardware
	Reactive security concepts	(Zhang et al. , 2003), (Golle et al. , 2004),	Compare the received information with the observing information through: 1. Signature-based: attack detection by comparing the network traffic to known signatures of attacks 2. Anomaly-based: comparing the received information to the normal operation behavior. 3. Context verification: comparing the received information with the collected information from any information source by each vehicle

verification is used to protect the vehicular network from various attacks on the communicated information such as modification of in-transit traffic or impersonation (Fuentes et al. , 2010, Karagiannis, Altintas, 2011).

To provide for these requirements and protect vehicular networks against these challenges, several solutions have been suggested. For instance, Plausibility Checks(Schneier, 1999), Logic Reception Beacons(Vora and Nesterenko, 2006) and Tamper Proof GPS(Hubaux, Capkun, 2004) are three methods to protect vehicular networks against deliberate retrieval of the location of vehicles by attackers. In addition, there are two types of methods to provide data-centric trust and verification in the vehicular networks: reactive and proactive security concepts.

6.2. Vehicular Cloud Computing Threats

With increasing vehicular cloud computing usage, the significance of security in this area is also increasing (Gerla, 2012). There are various security issues that threaten the security of vehicular cloud computing. These threats can be classified into six groups: denial of services, identity spoofing, modification repudiation, repudiation, Sybil attack, and information disclosure. (1) Denial of services: is a common attack on vehicular clouds and networks which attempts to make the resources unavailable (Blum et al. , 2008), (2) Identity spoofing: is the second threats and allows an unauthorized user or application to abuse someone else's identity and security credentials (Chen et al. , 2007), (3) Data modification (Tampering): is another security threat in VCC which can be performed by several attackers before the data are received by the destination, for example, the Man-in-the-Middle attack is the most popular attack on this group, (4) Repudiation: the repudiation attacker is able to manipulate or forge the identification of new actions, data and operations due to the lack of adopting controls to track and log users properly. In other words, the repudiation means the ability to deny a fact, or to deny that an action took place. (5) Sybil attack: is to create a large number of pseudonymous identities in order to redundantly carry out a remote operation which cause the system to select a single remote entity multiple times and defeat the redundancy, (6) Information disclosure: to acquire the specific information of a system due to the lack of data privacy. This attack includes Information Leakage (reveal sensitive data), Path Traversal (force access to outsourced data), and Predictable Resource Location (finding hidden content and functions).

It is impossible to provide a secure environment for vehicular cloud computing without considering some security requirements such as confidentiality, integrity and authentication. (1) Confidentiality: Sensitive data should not be disclosed by unauthorized users, (2) Integrity: Data should not be tampered with or modified. The messages must be reliable and valid, (3) Availability: Data should be available whenever they are needed. (4) Authentication: Determining whether someone or something is, who or what it is claimed to be, (5) Privacy: The user's privacy should be preserved, and (6) Real-time constraints: Some applications, such as accident alerts, require real-time or near real-time communication. Table 4. illustrates the effects of the security threats of VCC on these requirements.

Table 4. The side effect of threats on VCC

Threats	Description	Conf.	Int.	Ava.	Auth.
Denial of Services	Overloading the communication channels or consuming the resources to make them unavailable	No	No	Yes	N/A
Identity Spoofing	Unauthorized person pretends to be a legitimate user to access data	Yes	Yes	N/A	Yes
Tampering	Altering and modifying data by an attacker	N/A	Yes	No	No
Repudiation	Deny a fact, or to deny that an action took place	Yes	Yes	N/A	No
Information Disclosure	Hiding the identity of users by an attacker to acquire specific information	Yes	Yes	No	Yes
Sybil attack	Forging of multiple identities	Yes	Yes	Yes	Yes

6.3. Vehicular Cloud Computing Security Challenges

One of the main characteristics of vehicular cloud is the high mobility of nodes, that causes several security challenges in the VCC, such as authentication, secure location information, message confidentiality, the safety of messages and securing vehicular communication. In this section, we introduce these security challenges.

6.3.1. Authentication

The authentication in VC contains verifying the authentication of users and the integrity of messages. There are some studies to overcome this challenge in vehicular network such as "Probabilistic Adaptive Anonymous Authentication in Vehicular Networks" is an authentication method for a vehicular network proposed by (Xi et

al. , 2008) and "Auditable and Privacy-Preserving Authentication in Vehicular" was proposed by (Kim et al. , 2008) based on the MAC-chain method for privacy-preserving authentication and using a one-time pseudonym to manage a revoke list. However the VC environment is more challenging than vehicular network and cloud computing, due to the high mobility of nodes. In addition, verifying the authentication of transmitting messages by using location based authentication methods in VC is difficult because of high mobility of nodes. For example, the authentication of accident alert messages associated with the location of vehicles and time of the accident cannot be verified easily because the location of vehicles is changing (Yan et al. , 2012).

6.3.2. Secure Location and Localization

Location information plays a vital role in VC to transmit data and create connections because most applications in vehicular systems rely on location information such as traffic status reports, collision avoidance, emergency alerts, and cooperative driving. Therefore, the security of location information and localization should be provided among vehicles.

There are three models to validate and integrate the location information in a VC. An active location integrity model is the first approach and validates vehicle locations by using devices such as radar. The second model is passive location integrity which is based on filtering the impossible locations and building previous location of neighbouring vehicles without using radar. The last location integrity method is a general location integrity model that calculates the high accuracy location from the low resolution location by filtering the malicious location in VC (Gongjun et al. , 2010, Yan, Olariu, 2009).

"Secure Relative Location Determination in Vehicular Network" (SRLD) is one of the localization methods proposed by Tang et al. (Tang et al. , 2006) to determine the correct locations of a set of connected vehicles by using the locations of surrounding vehicles. Yan et al.(Yan, Olariu, 2009) proposed another localization method based on filtering malicious data, addressing the inter-cell position information integrity of vehicles or using GPS and radar. The third method to provide secure localization is called "Cross-layer Location Verification Enhancement in Vehicular Networks" (CLVE), which was designed by Gongjun et al. (Gongjun, Olariu, 2010) by addressing a location of the validation mechanism to validate the locations vehicles. This method is implemented in three layers: the physical layer, the network layer and the application layer. The last localization method is "A Geographic Location-based Security Mechanism for Intelligent Vehicular Network" (GLM) which was proposed by Yan et al.(Yan et al. , 2011) in which a cryptographic algorithm is designed to convert a location into a key (geolock) to improve the location error tolerance in vehicular networks. Table 5 consists of several methods to validate the location information.

Table 5. Comparison of several location verification methods

Scheme	Requirements	Active	Passive	General
(SRLD) [53]	Using cryptographic algorithm	No	Yes	No
Providing Location Security in Vehicular Ad-hoc Networks [16]	1. Using GPS and radar 2. Filtering 3. Inter-cell position	Yes	Yes	Yes
CLVE [51]	Using GPS and radar	Yes	No	No
(GLM) [52]	Using cryptographic algorithm	Yes	No	No

6.3.3. Securing Vehicular Communication

As mentioned in section 4.1, all nodes, such as vehicles and road-side infrastructures are able to communicate with each other based on the V2V or V2I communication models in vehicular cloud computing. Furthermore, the vehicles and road-side infrastructures are required to communicate with the cloud to store or process their data. These communications are illustrated in Figure 12.

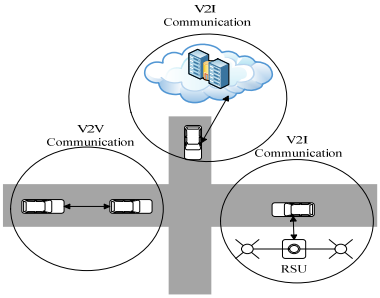

Fig. 12. Illustration of communication in vehicular cloud computing

The details of this communication are shown in Figure 13, in which an OBU is responsible for establishing communication between vehicles or between vehicles and infrastructures. A RSU is an access point that is connected to a location server that records or processes all location data forwarded by RSUs. The location server sends the data to the cloud for processing or storage. Furthermore, a trusted certificate authority (CA) is in charge of providing authentication services for vehicles and location-based service providers(Sampigethaya, Huang, 2005).

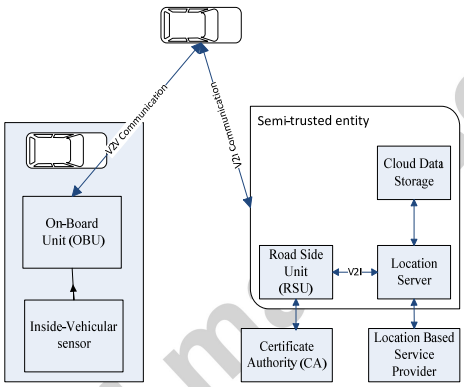

Fig. 13. Block diagram of a vehicular cloud communication system (Yan et al. , 2009)

The VC's message is constructed from some fields such as : vehicle id or pseudonym to identify the driver, time stamp, message type, length of message, data, geographic position, direction, and error checking field. The type of message can be: (1) short message: to send an alert message or warning messages, (2) Media message: to get an environment services from other vehicles or a cloud, (3) Priority message: to end the alert messages or urgent messages, and (4) Acknowledge message: to confirm the delivery of messages (Baby et al. , 2013).

Providing secure communication in a vehicular cloud plays a central role in creating safer and more efficient driving. There are several security holes in vehicular communication, which make it vulnerable against attackers, for example, preventing communication (jamming), forging messages and transmitting false hazard warnings by the attacker (forgery), dropping or modifying a message by intermediate nodes (traffic tampering), and privacy violations. Figure 14 shows the jamming of communication in a VC.

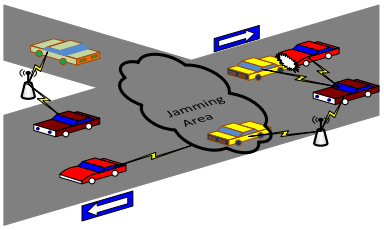

Fig. 14. Jamming communication

To protect vehicular communication against wide ranges of attacks, the use of a cryptographic algorithm is inevitable. ElGamal signature scheme (ElGamal, 1985) is a way to create a secure communication in VC environment. Each vehicle has a specific public and private key $\left(k_{pu}, k_{pr}\right)$ where $k_{pu} = g^{k_{pr}} \bmod p$, g is a

multiplicative group generator and p is a large prime number. Before sending a message, a specific private and public key $\left(k_{mpr}, k_{mpu} = g^{k_{mpr}} \bmod p\right)$, is computed for it and then the message digest d_m is generated by hashing the concatenation of message and message public key ($d_m = H(m \mid T_m)$). The message, its public key and signature that is generated by using the following formula is sent to the destination.

$$S_m = k_{mpr} + d_m k_{pr} \bmod (p-1)$$

Upon receiving the message, the message signature should be verified by checking:

$$g^x \stackrel{?}{=} k_{mpu} k_{pu}^{d_m}$$

The most challenging part of each cryptographic algorithm in vehicular cloud is key management. The Vehicular Public Key Infrastructure (VPKI) is a common key management method to ensure the integrity and confidentiality of the message in vehicular clouds.

6.3.4.Vehicular Public Key Infrastructure (VPKI)

The wide ranges of vehicles that are registered in various countries are able to travel beyond their registration regions and require a robust key management scheme. The Vehicular Public Key Infrastructure is one of the most important schemes to provide key management among vehicles, and it consists of three steps as follows:

- Key assignment by Certificate Authorities (CAs): In this step, public and private keys are issued for each vehicle. Key assignment is generated based on a unique ID with an expiration period.
- Key Verification (Authentication): In this step, the vehicle public key validation can be checked by CAs. When a vehicle i requests a public key from CA_j, Pu_i will be issued by CA_j as a public key for this vehicle. Then, CA_j computes a certification ($Cer_i[Pu_i]$) for this vehicle based on the vehicle public key and the ID of CA_j as follows:

$$Cer_i[Pu_i] = Pu_i \mid Sign_{\Pr_{CA_j}}(Pu_i \mid ID_{CA_j}) \qquad (1)$$

Here, $Cer_i[Pu_i]$ is public key vehicle i issued by CA_j, $\Pr_{CA_j}$ is the private key of CA_j, the identity of CA_j is shown by ID_{CA_j} and $(Pu_i \mid ID_{CA_j})$ is signed by the private key of CA_j.

Certificate Revocation: One of the most significant ways to protect data against an attacker is certificate revocation. Generally, when the attacker certification is detected or the certification of one node is exposed by attackers, the certificate should be revoked(Papadimitratos, Buttyan, 2008, Raya et al. , 2006b). The Certificate Revocation List (CLR)(Housley et al. , 2002) that is proposed by Housley et al. is the most important revocation methods in a vehicular network. The CRL contains a list of the most recently revoked certificates which is broadcast among vehicles immediately. However, CLRs has several drawbacks: the length of list can be very long and the lifetime of certificates can be very short. To protect the security of vehicles, three certificate revocation protocols are proposed, such as (1) "Revocation Protocol of the Tamper-Proof Devices" (RTPD)(Raya, Papadimitratos, 2006b), (2) RC^2RL ("Revocation Protocol uses Compressed Certificate Revocation Lists"), and (3) "Distributed Revocation Protocol" (DRP)(Raya and Hubaux, 2007). In the RTPD method, when the CA decides to delete the pair key of each vehicle, a revocation message is encrypted with the vehicle public key and then it is sent to the vehicle (Pu_{V_i}). This message will be verified by the tamper-proof device (TPD) and then all key pairs will be revoked. Finally, an acknowledgment message will be transferred to the CA. In this method, the CA must know the current location of V_i; otherwise, the revocation message should be broadcast among all vehicles. Figure 15 shows the procedure of the RTPD model in which the CA must revoke all private and public keys of car M.

If the CA wants to revoke a subset of the vehicles' keys or if the TPD of V_i is unavailable, the RC^2RL method is used. Finally, the DRP method is used when vehicles collect accusations against the misbehavior of vehicles in which the neighbors of the misbehaving vehicle (V_i) are able to revoke the key of V_i. Consequently, by using these approaches, the communication links in vehicular cloud computing can be trusted.

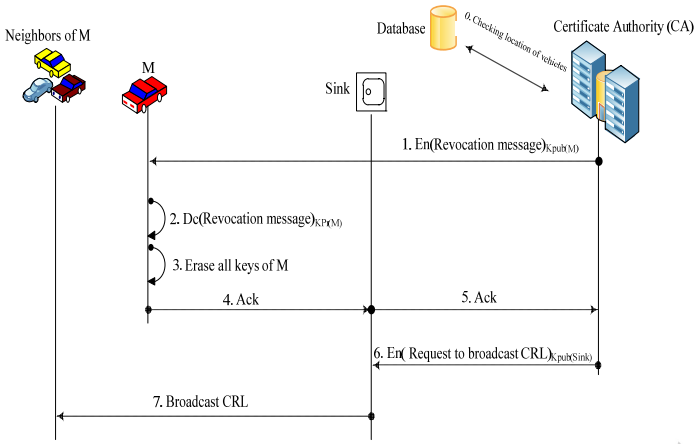

Fig. 15. Revocation Protocol of the tamper-proof device (RTPD)

6.3.5. Data Security

As mentioned in the previous section, VC provides an efficient way to exploit the utilized computation and storage resources of vehicles. Without considering the security restriction, the vehicles are able to access or alter the stored data on other vehicles. Therefore, the sensitive data that are stored in each vehicle should be encrypted (e.g., by the vehicle's private key) to protect it against the unauthorized access.
On the other hand, when the parked vehicles in the shopping mall are used as a data center, it is possible to store the sensitive data of the customers in a vehicle temporarily. Before the vehicle leaves the parking, this data needs to be removed from the devices. Therefore, the VC requires a virtual machine to manage the assignment of physical devices which have been used to compute or store sensitive data. The Virtual machine is able to provide a following advantages: (1) the host vehicle or other VMs cannot interfere with the applications and services that run within a VM for providing isolation ensures, (2) to be copied, moved or reassigned between host servers for optimizing hardware resource utilization, (3) simplifying data backup and recovery (Armbrust et al. , 2010).

6.3.6. Network Heterogeneity

The vehicles usually have a large number of different on-board devices, including GPS, wireless transceivers, and on-board radar devices. The different vehicles are able to have a different combination of these on-board devices with different capabilities such as speed of processor, volume of memory, storage, and CPU capacity. Therefore, providing a security for these heterogeneous vehicles in VC environment is difficult because most of cryptographic algorithms are not lightweight and the vehicles need to have certain hardware conditions.

6.3.7. Access Control

Access control is a challenging aspect of the VC in which an identification of the user is checked before gaining access to the resources. In the VC, various access control levels are pre-defined and each user belongs to a specific cluster based on its role in the network (Gongjun et al. , 2012).

7. Open issues and Research Challenges

This section presents several important open issues and research challenges as well as research directions for successful VCC deployment and implementation. Due to the dynamic environment of computing, sensing, communicating, and organizing structures enable autonomy and authority to cope with the local surroundings that have an extensive influence. Vehicular clouds are complex entities that must be engineered and designed to work with the operating environment and the inherent stresses. A VC's physical resource, synchronization, control and aggregation are research challenges, which are described below.

7.1. Architectural formation of VC

Challenges include issues regarding the formation of the logical structure of the VC and interactions with physical resources. Hence the acute necessity of managing the mobility of the host and heterogeneity should be

considered for computing, communication and storage facilities, and vehicle associations such as changes in interest or location, resource failure, and denial. Thus, we have to consider the following aspects:

- Flexible mobile architecture: One of the main characteristics of VC is the mobility of the nodes which directly affects on the available computational capabilities and storage resources, for example, the number of parked vehicles in the parking is not constant. Therefore, To provide fluctuating application requirements and resource accessibility on the move, the necessary related protocol architecture and VC networking must be developed.
- Robust architecture: The fundamental building blocks and structures that compose VC should be engineered and designed to face the structural stress of the unstable working situation. Olariu, Hristov (2013) was the first to propose a robust dynamic architecture for VC based on Eucalyptus cloud system (Nurmi, Wolski, 2009) and virtualization approach to aggregate the computational and storage resources. Greater emphasis and more researches are necessary for the migration of virtual machines among cars and efficient vehicle visualization.
- Service-based network architecture: The existing layered network architecture, for example TCP-IP stack, is not adequate to support ongoing evolving technologies and applications. Hence, It needs to use the service-oriented and component-based network architecture (Brown et al. , 2002) with sufficient learning opportunities and monitoring facilities in order to cope with reusable and extensible applications and resources, which require to be largely deployed as common services available in VC environments (Exposito, 2013).
- Scopes of Services: New emerging services can be possible of wise and technically controlled uses of VCC. Photo as a service can collect evidence and context awareness services which will be benefited by the forensic examinations and the car insurance company to mitigate the insurance claim. Gateway as a service (Yen-Wen et al. , 2011) will integrate with the net more profoundly. We are expecting more applications of VCC in different real world scenario and applied applications from new researchers.

7.2. Privacy and security of VC

Security and privacy are very important aspects for the establishing and maintaining the trust of users in VC. Privacy measures are required to ensure the VC communication and information in the isolated and trustworthy environment, while security procedures are needed to protect against network threats. Establishing trust relationships between several participants is a vital part of trustworthy communication and computation. As some of the vehicles related to VC may have met previously, the proactive task of launching a fundamental trust relationship among vehicles is desirable and possible. Olariu, Khalil (2011) described VC as a set of vehicles which share the capability of computing power, Internet access and storage to form conventional cloud computing. Therefore, it is anticipated that VC suffers the same security problem as CC (Yan, Rawat, 2012). As mentioned in section 6, the main security challenges of VC include: (i) verifying the authentication of users and the integrity of messages due to the high mobility of nodes, (ii) ensuring the confidentiality of sensitive message by using the cryptographic algorithm, (iii) ensuring the secure location and localization because most applications in vehicular systems rely on location information, (iv) providing data isolation to ensure the security of stored data on the cloud, (v) secure data access to protect stored data on the cloud against unauthorized access. The security and privacy issue of VC has not yet been addressed in the literature and need more consideration (Yan, Wen, 2013).

7.3. Policy and Operational Management

We must address the establishment of the incentives, the availability metrics, the rules and the regulations of the VC to operate seamlessly in a decision support system, a control structure and a management system. Facing these issues requires a wider community, which must engage local and global decision makers. The metrics are needed to determine the economic models for realistic pricing and billing of different VC services and features. Thus, we should give emphasis to the following factors:

- Assurance of trust management: In some situations, the VC may require to have authority to to take local action instead of a central authority. For example, when the vehicles involves a traffic jam, for rescheduling the traffic lights, a cooperation between the cloud formation and municipal or county authority needs to promote the rapid dissipation of congestion. Hence, the existence of a trust management in VC can be useful for automated verification of actions.
- Essential functioning policies: Effective operational policies are needed for seamless inters-operation, decision support, establishing accountability metrics, standardization, regulations, and even local and national policy making.
- Federation of different clouds: We are expecting in the near future, several types of clouds will emerge such as the VCC-car cloud, sensor cloud, Smartphones cloud, all clouds will interact with each other and can

connect on demand real time scenario to real cloud computing cloud. Hence the interoperability of different types of clouds , connection, synchronization , and reliability and efficiency should be addressed.

8. Conclusion and Future Remarks

We have reviewed and highlighted a recent new concept, Vehicular Cloud Computing, whose time has arrived. VCC emerges from the convergence of powerful implanted vehicle resources, advances in network mobility, ubiquitous sensing and cloud computing. The combination of a massive amount of unutilized resources on board vehicles, such as internet connectivity, storage and computing power, can be rented or shared with various customers over the internet, similar to the usual cloud resources. Several of these resources can dynamically provide us support for alleviating traffic incidents. We also advocate that, when fully realized and deployed, VCCs can lead to a significant enhancement in terms of safety, security and economic viability of our society. Thus, VCs could establish a large ad hoc federation to help mitigate many types of emergencies. In a planned or unplanned evacuation, there is possible damage to the mobile communication infrastructure, and federated VCs could help a decision support system and offer a temporary replacement for the infrastructure.

In this survey, the architecture, several interesting application scenarios, security and privacy issues, key management strategies and the formation of VCCs have been identified and discussed. We present a comprehensive taxonomy of vehicular networking, VCC and a comparative study between CC and VCC. We also recognized efficient traffic management, cloud communication systems and interoperability between the vehicular cloud. However, a number of areas still remain unexplored for researchers including: context based routing, security and privacy aware data sharing, data indexing, high mobility, unstable communication links, physical location of attackers inside the same cloud server, and the synchronization of VC federation.

A new research and expansion programs are required to create VCC reference models, protocols, and architectures for addressing evolving trust and privacy issues. Hence, we need a concerted effort among industry and academia and the close cooperation of the auto industry and the government. Thus, the VCC can be the next technological shifting paradigm that provides technologically feasible and economically viable solutions by converging intelligent vehicular networks towards autonomous traffic, vehicle control and perception systems.

9. Acknowledgments

This work is fully funded by the Malaysian Ministry of Higher Education under the University of Malaya High Impact Research Grant UM.C/HIR/MOHE/FCSIT/03.

References

Abid H, Phuong LTT, Wang J, Lee S, Qaisar S. V-Cloud: vehicular cyber-physical systems and cloud computing. Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies. Barcelona, Spain: ACM; 2011. p. 1-5.

Aijaz A, Bochow B, Dötzer F, Festag A, Gerlach M, Kroh R, et al. Attacks on inter vehicle communication systems-an analysis. 2006.

Akbari Torkestani J. Mobility prediction in mobile wireless networks. Journal of Network and Computer Applications. 2012;35:1633-45.

Al-Sultan S, Al-Doori MM, Al-Bayatti AH, Zedan H. A comprehensive survey on vehicular Ad Hoc network. Journal of Network and Computer Applications. 2013.

Alazawi Z, Altowaijri S, Mehmood R, Abdljabar MB. Intelligent disaster management system based on cloud-enabled vehicular networks. 11th International Conference on ITS Telecommunications (ITST). St. Petersburg 2011. p. 361-8.

Anda J, LeBrun J, Ghosal D, Chuah CN, Zhang M. VGrid: vehicular adhoc networking and computing grid for intelligent traffic control. IEEE; 2005. p. 2905-9.

Arif S, Olariu S, Wang J, Yan G, Yang W, Khalil I. Datacenter at the airport: Reasoning about time-dependent parking lot occupancy. IEEE Transactions on Parallel and Distributed Systems. 2012.

Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, et al. A view of cloud computing. Commun ACM. 2010;53:50-8.

Baby D, Sabareesh RD, Saravanaguru RAK, Thangavelu A. VCR: Vehicular Cloud for Road Side Scenarios. In: Meghanathan N, Nagamalai D, Chaki N, editors. Advances in Computing and Information Technology: Springer Berlin Heidelberg; 2013. p. 541-52.

Bilal SM, Bernardos CJ, Guerrero C. Position-based routing in vehicular networks: A survey. Journal of Network and Computer Applications. 2013;36:685-97.

Blum JJ, Neiswender A, Eskandarian A. Denial of service attacks on inter-vehicle communication networks. Intelligent Transportation Systems, 2008 ITSC 2008 11th International IEEE Conference on: IEEE; 2008. p. 797-802.
Boneh D, Shacham H. Group signatures with verifier-local revocation. ACM; 2004. p. 168-77.
Bordley L, Cherry CR, Stephens D, Zimmer R, Petrolino J. Commercial Motor Vehicle Wireless Roadside Inspection Pilot Test, Part B: Stakeholder Perceptions. Transportation Research Board 91st Annual Meeting2012.
Brown A, Johnston S, Kelly K. Using service-oriented architecture and component-based development to build web service applications. Rational Software Corporation. 2002.
Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems. 2009;25:599-616.
Calandriello G, Papadimitratos P, Hubaux JP, Lioy A. Efficient and robust pseudonymous authentication in VANET. ACM; 2007. p. 19-28.
Chen B, Curtmola R, Ateniese G, Burns R. Remote data checking for network coding-based distributed storage systems. Proceedings of the 2010 ACM workshop on Cloud computing security workshop. Chicago, Illinois, USA: ACM; 2010. p. 31-42.
Chen Y, Trappe W, Martin RP. Detecting and localizing wireless spoofing attacks. Sensor, Mesh and Ad Hoc Communications and Networks, 2007 SECON'07 4th Annual IEEE Communications Society Conference on: IEEE; 2007. p. 193-202.
Chung TY, Chen YM, Hsu CH. Adaptive momentum-based motion detection approach and its application on handoff in wireless networks. Sensors. 2009;9:5715-39.
Czajkowski K, Fitzgerald S, Foster I, Kesselman C. Grid information services for distributed resource sharing. IEEE; 2001. p. 181-94.
Dinh HT, Lee C, Niyato D, Wang P. A survey of mobile cloud computing: architecture, applications, and approaches. Wireless Communications and Mobile Computing. 2011.
ElGamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In: Blakley G, Chaum D, editors. Advances in Cryptology: Springer Berlin Heidelberg; 1985. p. 10-8.
Eltoweissy M, Olariu S, Younis M. Towards autonomous vehicular clouds. Ad Hoc Networks. 2010a:1-16.
Eltoweissy M, Olariu S, Younis M. Towards Autonomous Vehicular Clouds. In: Zheng J, Simplot-Ryl D, Leung VM, editors. Ad Hoc Networks: Springer Berlin Heidelberg; 2010b. p. 1-16.
Exposito E. Service-Oriented and Component-Based Transport Protocol. Advanced Transport Protocols. 2013:187-200.
Fernando N, Loke SW, Rahayu W. Mobile cloud computing: A survey. Future Generation computer systems. 2012.
Festag A, Baldessari R, Zhang W, Le L, Sarma A, Fukukawa M. Car-2-x communication for safety and infotainment in europe. NEC Technical Journal. 2008;3:21-6.
Fleming B. Smarter and Safer Vehicles. Vehicular Technology Magazine, IEEE 2012;7:4-9.
Fonseca A, Vazão T. Applicability of position-based routing for VANET in highways and urban environment. Journal of Network and Computer Applications. 2012.
Ford-Comp. Ford, University of Michigan Reveal Students' Vision for Future of In-Car Cloud Computing Apps. Ford Online; 2010.
Fuentes JM, González-Tablas AI, Ribagorda A. Overview of security issues in Vehicular Ad-hoc Networks. 2010.
Gabauer DJ, Gabler HC. Comparison of roadside crash injury metrics using event data recorders. Accident Analysis & Prevention. 2008;40:548-58.
Gayomali C. Toyota and Microsoft Team Up to Bring Cloud Computing On the Road. Time Tech; 2011.
Gerla M. Vehicular Cloud Computing. The 11th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)2012. p. 152-5.
Goggin G. Driving the Internet: Mobile Internets, Cars, and the Social. Future Internet. 2012;4:306-21.
Golle P, Greene D, Staddon J. Detecting and correcting malicious data in VANETs. ACM; 2004. p. 29-37.
Gongjun Y, Olariu S, Weigle MC. Cross-layer location verification enhancement in vehicular networks. Intelligent Vehicles Symposium (IV), 2010 IEEE2010. p. 95-100.
Gongjun Y, Rawat DB, Bista BB. Towards Secure Vehicular Clouds. Complex, Intelligent and Software Intensive Systems (CISIS), 2012 Sixth International Conference on2012. p. 370-5.
Harris C. General Motors Connects Cars to 4G LTE Tech Page One 2013.
Harsch C, Festag A, Papadimitratos P. Secure Position-Based Routing for VANETs. 66th IEEE Conference on Vehicular Technology. Baltimore, MD2007. p. 26-30.
Hartenstein H, Laberteaux KP. A tutorial survey on vehicular ad hoc networks. Communications Magazine, IEEE. 2008;46:164-71.

Hossain E, Chow G, Leung V, McLeod RD, Mišić J, Wong VWS, et al. Vehicular telematics over heterogeneous wireless networks: A survey. Computer Communications. 2010;33:775-93.
Hossain MA. A Survey on Sensor-Cloud: Architecture, Applications, and Approaches. International Journal of Distributed Sensor Networks. 2013;2013.
Housley R, Polk W, Ford W, Solo D. Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile. RFC 3280, April; 2002.
Huang D, Hong X, Gerla M. Situation-aware trust architecture for vehicular networks. Communications Magazine, IEEE. 2010;48:128-35.
Hubaux JP, Capkun S, Luo J. The security and privacy of smart vehicles. Security & Privacy, IEEE. 2004;2:49-55.
Hussain R, Son J, Eun H, Kim S, Oh H. Rethinking Vehicular Communications: Merging VANET with cloud computing. 4th International Conference on Cloud Computing Technology and Science (CloudCom), 2012: IEEE; 2012. p. 606-9.
ITS-Committee. IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. IEEE Vehicular Technology Society Standard 16092. 2006:0_1-105.
ITS_Committee. Intelligent Transportation Systems for Planned Special Events: A Cross-Cutting Study. Technical Report FHWA-JPO-08-056: U.S. Department of Transportation Intelligent Transportation Systems, Highway Administration; 2008. p. 1-60.
James T. Smart cars. Engineering & Technology. 2012;7:50-1.
Jiang D, Delgrossi L. IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. Vehicular Technology Conference, 2008 VTC Spring 2008 IEEE: IEEE; 2008. p. 2036-40.
Kamat P, Baliga A, Trappe W. An identity-based security framework For VANETs. Proceedings of the 3rd international workshop on Vehicular ad hoc networks. Los Angeles, CA, USA: ACM; 2006. p. 94-5.
Karagiannis G, Altintas O, Ekici E, Heijenk G, Jarupan B, Lin K, et al. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. Communications Surveys & Tutorials, IEEE. 2011;13:584-616.
Kim SH, Kim BH, Kim YK, Lee DH. Auditable and privacy-preserving authentication in vehicular networks. IEEE; 2008. p. 19-24.
Liu Y, Bi J, Yang J. Research on vehicular ad hoc networks. Control and Decision Conference, 2009 CCDC'09 Chinese: IEEE; 2009. p. 4430-5.
Lochert C, Scheuermann B, Caliskan M, Mauve M. The feasibility of information dissemination in vehicular ad-hoc networks. IEEE; 2007. p. 92-9.
Lochert C, Scheuermann B, Wewetzer C, Luebke A, Mauve M. Data aggregation and roadside unit placement for a vanet traffic information system. ACM; 2008. p. 58-65.
MCC-forum. Discover the world of Mobile Cloud Computing London: mobile cloud computing forum; 2011.
Mehmood R, Nekovee M. Vehicular ad hoc and grid networks: discussion, design and evaluation. PROCEEDINGS OF THE 14TH WORLD CONGRESS ON INTELLIGENT TRANSPORT SYSTEMS (ITS). HELD BEIJING: ITS America; 2007.
Mell P, Grance T. The NIST Definition of Cloud Computing. Maryland, US: The National Institute of Standards and Technology; 2011.
Mousannif H, Khalil I, Al Moatassime H. Cooperation as a Service in VANETs. Journal of Universal Computer Science. 2011;17:1202-18.
Nakanishi T, Yendo T, Fujii T, Tanimoto M. Right Turn Assistance System at Intersections by Vehicle-Infrastructure Cooperation. IEEE; 2006. p. 100-5.
NEXCOM. In-Vehicle PC NEXCOM International Co.; 2011.
Nurmi D, Wolski R, Grzegorczyk C, Obertelli G, Soman S, Youseff L, et al. The Eucalyptus Open-Source Cloud-Computing System. 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, 2009 Shanghai2009. p. 124-31.
Olariu S, Hristov T, Yan G. The next paradigm shift: From vehicular networks to vehicular clouds. In: S. Basagni MC, S. Giordano and I. Stojmenovic, editor. Mobile Ad Hoc Networking: Cutting Edge Directions, Second Edition NJ, USA.: John Wiley & Sons, Inc., Hoboken; 2013.
Olariu S, Khalil I, Abuelela M. Taking VANET to the clouds. International Journal of Pervasive Computing and Communications. 2011;7:7-21.
Olariu S, Weigle MAC. Vehicular networks: from theory to practice: Chapman & Hall/CRC; 2009.
Oliver N, Pentland AP. Driver behavior recognition and prediction in a SmartCar. PROC SPIE INT SOC OPT ENG: Citeseer; 2000. p. 280-90.
Panayappan R, Trivedi JM, Studer A, Perrig A. VANET-based approach for parking space availability. Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks. Montreal, Quebec, Canada: ACM; 2007. p. 75-6.

Papadimitratos P, Buttyan L, Holczer T, Schoch E, Freudiger J, Raya M, et al. Secure vehicular communication systems: design and architecture. Communications Magazine, IEEE. 2008;46:100-9.
Park P, Yim H, Moon H, Jung J. An OSGi based in-vehicle gateway platform architecture for improved sensor extensibility and interoperability. IEEE; 2009. p. 140-7.
Pelzl J, Wolf M, Wollinger T. Virtualization technologies for cars: Solutions to increase safety and security of vehicular ECUs. Proceedings, embedded world Conference. Nuremberg, Germany2009.
Qin Y, Huang D, Zhang X. VehiCloud: Cloud Computing Facilitating Routing in Vehicular Networks. 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom): IEEE; 2012. p. 1438-45.
Quick D. GM developing vehicle-to-vehicle and vehicle-to-infrastructure communications systems. Gizmag; 2011.
Raya M, Aziz A, Hubaux JP. Efficient secure aggregation in VANETs. ACM; 2006a. p. 67-75.
Raya M, Hubaux JP. Securing vehicular ad hoc networks. Journal of Computer Security. 2007;15:39-68.
Raya M, Papadimitratos P, Hubaux JP. Securing vehicular communications. Wireless Communications, IEEE. 2006b;13:8-15.
Rongxing L, Xiaodong L, Haojin Z, Xuemin S. SPARK: A New VANET-Based Smart Parking Scheme for Large Parking Lots. The 28th Conference on Computer Communications (IEEE INFOCOM). Rio de Janeiro IEEE 2009. p. 1413-21.
Sampigethaya K, Huang L, Li M, Poovendran R, Matsuura K, Sezaki K. CARAVAN: Providing location privacy for VANET. WASHINGTON UNIV SEATTLE DEPT OF ELECTRICAL ENGINEERING; 2005.
Scarborough-Research. Teen Mall Shopping Attitudes and Usage Survey. NEW YORK: Scarborough Research and Arbitron; 2009.
Schneier B. Attack Trees: Modeling security threats. Dr Dobb's Journal. 1999.
Schweiger B, Ehnert P, Schlichter J. Simulative Evaluation of the Potential of Car2X-Communication in Terms of Efficiency. In: Strang T, Festag A, Vinel A, Mehmood R, Rico Garcia C, Röckl M, editors. Communication Technologies for Vehicles: Springer Berlin Heidelberg; 2011. p. 155-64.
Shiraz M, Gani A, Khokhar R, Buyya R. A Review on Distributed Application Processing Frameworks in Smart Mobile Devices for Mobile Cloud Computing. IEEE Communications Surveys & Tutorials. 2012;PP:1-20.
SINTRONES. In-Vehicle Computing. SINTRONES Technology Corp; 2009.
Song J-H, Wong VWS, Leung VCM. A framework of secure location service for position-based ad hoc routing. Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks. Venezia, Italy: ACM; 2004. p. 99-106.
Squatriglia C. Toyota, Microsoft to Bring the Cloud to Cars. Wired; 2011.
Szczurek P, Xu B, Wolfson O, Lin J, Rishe N. Learning the relevance of parking information in VANETs. Proceedings of the seventh ACM international workshop on VehiculAr InterNETworking. Chicago, Illinois, USA: ACM; 2010. p. 81-2.
Tang L, Hong X, Bradford P. Secure relative location determination in vehicular network. Mobile Ad-hoc and Sensor Networks. 2006:543-54.
Tekbiyik N, Uysal-Biyikoglu E. Energy efficient wireless unicast routing alternatives for machine-to-machine networks. Journal of Network and Computer Applications. 2011;34:1587-614.
Verma M, Huang D. SeGCom: secure group communication in VANETs. IEEE; 2009. p. 1-5.
Vora A, Nesterenko M. Secure location verification using radio broadcast. Dependable and Secure Computing, IEEE Transactions on. 2006;3:377-85.
Wang J, Liu Y, Jiao Y. Building a trusted route in a mobile ad hoc network considering communication reliability and path length. Journal of Network and Computer Applications. 2011;34:1138-49.
Wooseong K, Gerla M. NAVOPT: Navigator Assisted Vehicular Route OPTimizer. Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS). Seoul2011. p. 450-5.
Xi Y, Sha KW, Shi WS, Schwiebert L, Zhang T. Probabilistic adaptive anonymous authentication in vehicular networks. Journal of Computer Science and Technology. 2008;23:916-28.
Xu Q, Segupta R, Jiang D, Chrysler D. Design and analysis of highway safety communication protocol in 5.9 ghz dedicated short range communication spectrum. Vehicular Technology Conference, 2003 VTC 2003-Spring The 57th IEEE Semiannual: IEEE; 2003. p. 2451-5.
Yan G, Lin J, Rawat DB, Yang W. A geographic location-based security mechanism for intelligent vehicular networks. Intelligent Computing and Information Science. 2011:693-8.
Yan G, Olariu S, Weigle M. Providing location security in vehicular Ad Hoc networks. Wireless Communications, IEEE. 2009;16:48-55.
Yan G, Olariu S, Weigle MC. Providing VANET security through active position detection. Computer Communications. 2008;31:2883-97.
Yan G, Rawat DB, Bista BB. Towards Secure Vehicular Clouds. Sixth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS): IEEE; 2012. p. 370-5.

Yan G, Wen D, Olariu S, Weigle MC. Security Challenges in Vehicular Cloud Computing. IEEE Transactions on Intelligent Transportation Systems. 2013;14:284-94.
Yang X, Liu L, Vaidya NH, Zhao F. A vehicle-to-vehicle communication protocol for cooperative collision warning. Mobile and Ubiquitous Systems: Networking and Services, 2004 MOBIQUITOUS 2004 The First Annual International Conference on: IEEE; 2004. p. 114-23.
Yen-Wen L, Jie-Min S, Hao-Jun W. Cloud-assisted gateway discovery for vehicular ad hoc networks. 5th International Conference on New Trends in Information Science and Service Science (NISS)2011. p. 237-40.
Zarifneshat M, Khadivi P. Using mobile node speed changes for movement direction change prediction in a realistic category of mobilitymodels. Journal of Network and Computer Applications. 2013.
Zeadally S, Hunt R, Chen YS, Irwin A, Hassan A. Vehicular ad hoc networks (VANETs): status, results, and challenges. Telecommunication Systems. 2010:1-25.
Zhang Y, Lee W, Huang YA. Intrusion detection techniques for mobile wireless networks. Wireless Networks. 2003;9:545-56.
Zhu J, Feng Y, Liu B. PASS: Parking-Lot-Assisted Carpool over Vehicular Ad Hoc Networks. International Journal of Distributed Sensor Networks. 2013;2013:9.