# Vehicular Cloud Networks: Architecture, Applications and Security Issues

Farhan Ahmad, Muhammad Kazim, Asma Adnane
College of Engineering and Technology,
University of Derby,
Derby, United Kingdom
Email: {f.ahmad, m.kazim, a.adnane}@derby.ac.uk

Abir Awad
Software Research Institute,
Athlone Institute of Technology,
Athlone, Ireland
Email: aawad@research.ait.ie

***Abstract*— Vehicular Ad Hoc Networks (VANET) are the largest real life application of ad-hoc networks where nodes are represented via fast moving vehicles. This paper introduces the future emerging technology, i.e., Vehicular Cloud Networking (VCN) where vehicles and adjacent infrastructure merge with traditional internet clouds to offer different applications ranging from low sized applications to very complex applications. VCN is composed of three types of clouds: Vehicular cloud, Infrastructure cloud and traditional Back-End (IT) cloud. We introduced these clouds via a three tier architecture along with their operations and characteristics. We have proposed use cases of each cloud tier that explain how it is practically created and utilised while taking the vehicular mobility in consideration. Moreover, it is critical to ensure security, privacy and trust of VCN network and its assets. Therefore, to describe the security of VCN, we have provided an in-depth analysis of different threats related to each tier of VCN. The threats related to vehicular cloud and infrastructure cloud are categorized according to their assets, i.e., vehicles, adjacent infrastructure, wireless communication, vehicular messages, and vehicular cloud threats. Similarly, the Back-End cloud threats are categorized into data and network threats. The possible implications of these threats and their effects on various components of VCN are also explained in detail.**

***Keywords*—Vehicular Networks, Vehicular Cloud Networks, Security, Threats, Clouds, Assets**

## I. Introduction

With large number of vehicles distributed around the world, *Vehicular Networks (VANET)* [1] are considered as the basis of Intelligent Transport Systems (ITS). The next generation of vehicles will be equipped with different smart sensors, wireless communication modules, computational and storage capabilities [2]. The sensors will collect important information from surroundings and share it with neighbouring vehicles and adjacent road side units (RSU) via vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication. The fact that each vehicle has hardware constraints results in the limited applications offered by these computational and storage resources. For example, in order to provide in-vehicle entertainment to users high storage and computational capabilities are required which may not be supported by individual vehicle.

To support bandwidth hungry applications with complex computation, the vehicles and adjacent RSU must cooperate together to share their computational and storage resources, resulting in a temporary cloud with more resources. Similarly, merging traditional cloud [3] with these temporary clouds can further enhance the network efficiency. This introduces the concept of newly emerging technology called "Vehicular Cloud Networking (VCN)" [4] [5]. The temporary clouds can be used for low-sized applications such as traffic management, safety applications and sharing traffic conditions while the resources of traditional clouds can be used for complex applications like providing in-vehicle entertainment to the vehicular user.

In recent years, different research projects have been carried out which suggest how VANET can be used in conjunction with cloud computing. The concept of VCN was first introduced by Olariu et al. in the form of autonomous vehicular clouds (AVC) where autonomous vehicles dynamically allocate computing and communication resources to authorized users [6]. In [7], Bernstein et al. have taken a step further by introducing a platform as a service (PaaS) model to incorporate millions of users in a highly mobile environment. They introduced an architecture for their platform and discussed that a highly resourceful PaaS will be required for such complicated application scenarios. Hussain et al. introduced an architecture consisting of vehicular cloud (VC), vanet using clouds (VuCs), and hybrid clouds (HCs) in [8]. In their architecture, vehicles plays both roles, i.e., cloud service providers and clients. Yu et al. in [9] proposed a scheme to integrate cloud computing in different applications of vehicular networks. Their architecture enables the vehicles to share the storage, computation and bandwidth resources. However, this architecture lacks the implementation details in different context of VANET such as urban and rural areas.

Security is an important aspect of VCN and it should be addressed properly to gain users trust. Security of VCN is discussed by Yan et al. and Lee et al. in [10] [11]. These security schemes of VCN are quite generic and do not discuss the possible threats on different assets of VCN. The main contribution of this paper is twofold: 1) First, we describe a three-tier architecture for cloud based vehicular networks and propose detailed use cases of each cloud and 2) secondly, we provide an in-depth threat analysis of VCN by analysing threats to every asset of three-tier based architecture. The threats to tier-1 and tier-2 are identified for each asset of VCN, such as threats to vehicles, infrastructure, wireless communication, important messages and temporary clouds i.e., vehicular cloud and infrastructure cloud. While tier-3 threats are categorized into data threats and network threats.

The remainder of the paper is organised as follows: Section

978-0-7695-5697-0/15 $31.00 © 2015 IEEE
DOI 10.1109/UCC.2015.101

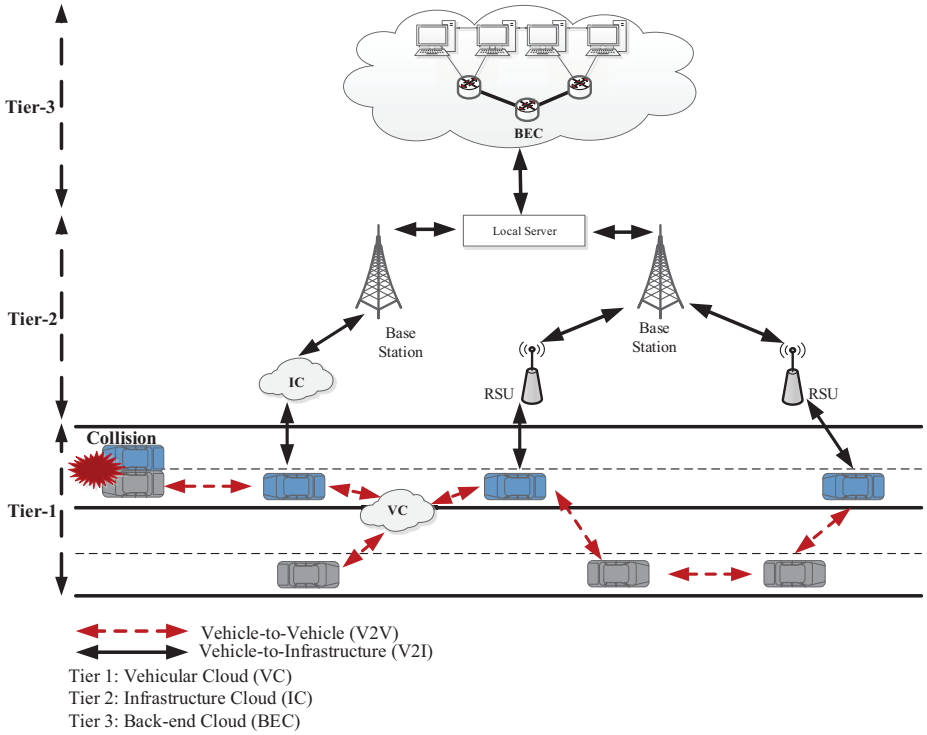


Fig. 1: Vehicular Cloud Networking Architecture

II introduces the proposed architecture of VCN while section III explains its operation. Potential applications of VCN are discussed in section IV. Section V explains the threats and security challenges to 3-tiers of VCN and section VI gives the conclusion of the paper.

## II. Vehicular Cloud Networking (VCN) Architecture

The proposed architecture of VCN is depicted in Fig. 1. The proposed architecture is a three tier architecture consisting of three levels:

(A) Tier-1 cloud: Vehicular Cloud (VC)
(B) Tier-2 cloud: Infrastructure Cloud (IC)
(C) Tier-3 cloud: Back-End Cloud (BEC)

### A. Vehicular Cloud (VC):

In VC, the physical resources (storage and computation) of vehicles are shared between group of vehicles only. This results in high overall efficiency of the network. The scope of VC is local in the context of VANET where the information is shared between the vehicles via V2V communication. Since the network usually experience vehicles with both high and low mobility, the technical difficulty of the formation of VC varies for different context of VANET. Following use cases of VC are possible:

- *Urban Areas:* Usually, mobility of the vehicles in urban areas (e.g., city center) is low as compared to highways, resulting in collaboration among vehicles for a longer period of time. This allows the possibility of formation and existence of VC in urban areas which can be used in different applications such as video surveillance of public transport.
- *Rural Areas:* Rural areas mostly experience high speed vehicles where different vehicles collaborate for a very short span of time resulting in a very short life cycle of VC. The other important factor in rural area is the low frequency of vehicles which makes it even harder for VC to be created and implemented.
- *Parking:* Parking is the best scenario to implement VC due to zero or negligible mobility of vehicles. The life cycle of VC in parking is long compared to rural and urban areas. The computation and storage resources of parked vehicles can be used to create a VC which can potentially be used to serve users in that particular geographical location, e.g., VC created in car park of the shopping mall can be used to serve users of that specific region.

### B. Infrastructure Cloud (IC)

IC is mostly initiated by adjacent RSU along the road where vehicles request to access the services provided by cloud. The scope of this cloud is local to small geographical area where RSU is located [12]. Communication between different ICs is carried out through dedicated local servers. Since both static (RSU) and mobile (vehicle) entities are

involved in IC, the technical difficulty of formation of IC varies for different scenarios of VANET.

- *Urban Areas:* As urban areas mostly involves vehicles with low mobility and excessive adjacent infrastructure, the formation and existence of IC is possible for urban scenarios due to the availability of enormous amount of RSU. IC in urban areas can be used in various applications such as remote navigation and traffic management.
- *Rural Areas:* The possibility of formation of IC is low in rural areas due to absence of adjacent infrastructure and high mobility of vehicles. In this scenario, the transient cloud is formed between RSU and vehicle for a very short span of time.
- *Parking:* If the vehicles have negligible mobility and adjacent infrastructure such as RSU is available, then the formation, existence and implementation of IC in the vicinity of respective RSU is highly possible. The combination of both VC and IC can serve higher number of users, resulting in very high efficiency of the network.

### C. Back-end Cloud (BEC)

BEC is the largest traditional cloud in vehicular environment which exists in the internet domain. BEC has more resources which can be used by vehicles for extensive data storage and high computation [9]. The scope of BEC is spread over the large geographical area to serve the vehicles. BEC can play a vital role during bandwidth management applications where it serves the users with high bandwidth requirements such as to provide in-vehicle multimedia.

## III. Vehicular Cloud Networking (VCN) Operation

To create and initiate a cloud in vehicular networks, it demands a cloud leader which can be either vehicle or adjacent RSU. If the leader is a vehicle to initiate the cloud and no adjacent RSU participates in cloud formation, then the resulting cloud is VC. However, if the request for cloud is initiated by RSU as a leader and neighbouring vehicles responds to its request results in the formation of IC.

The cloud leader invites cloud members i.e. vehicles and adjacnet RSUs in its vicinity by transmitting resource request messages (REQs) to form a cloud. Any vehicle wishes to join the cloud responds back to the cloud leader with resource reply messages (REPs) [13]. When cloud leader receives the confirmation via REP messages, it keeps its members' ID and assign different tasks and applications with them accordingly. The members communicate constantly with its cloud leader. Based on the permission from cloud leader, the members can publish and share the content received from leader with other vehicles.

Cloud leader is responsible for the maintenance of the cloud it created. However, if any cloud member, who wishes to leaves the cloud requests the resource leaving message to cloud leader. In that case, the cloud leader confirms the release of its member and recruits new members by broadcasting REQ messages. However, in case if the cloud leader itself no longer want to keep the cloud, it broadcasts the cloud release message and leaves the cloud.

## IV. Potential Applications of Vehicular Cloud Networking

Since different vehicles and RSU share their resources with each other along with traditional back-end clouds, VCN offers a wide range of applications such as,

### A. Video Surveillance in Urban Areas

VCN can be helpful for law enforcement agencies in urban areas to track a vehicle or people using high definition (HD) video to ensure security. Since, processing of HD video in real time requires large storage, VCN is one of the best available option for law enforcement agencies to take immediate decisions. For example, HD video of public transport from London to Scotland will produce a very large amount of content. This content will be passed on to concerned authorities using VC and IC which can then be processed to track people to ensure security.

### B. Bandwidth Management

With the increase in the interest of VCN day by day, various new applications are being designed with different sizes. Some applications are of large sizes e.g. vehicular user multimedia applications while others are of very small size such as vehicle safety and warning applications. These applications have different bandwidth requirements. VCN can be used to manage applications according to available resource to better use the available spectrum. For example, applications with small bandwidth requirements can be used directly through VC while vehicular user multimedia applications can be processed via IC and BEC.

### C. Real-time Navigation

In a traditional vehicular networks, static geographic maps are provided for vehicular navigation [9]. However, for accurate 3D maps, the resources within the vehicle may not be sufficient. VCN is a good application to provide real time vehicular navigation via IC.

### D. Remote Traffic Management

Remote traffic management is one of the important application of VCN. For a very long queue of vehicles on the motorway, information and suggestions can be provided via clouds. For example, if there is a congestion on motorway M1 and exit 1 due to accident, the information can be spread to other vehicles at exit 2 and further via IC and BEC. This way, the vehicles can take different routes to reduce congestion.

## V. Threats in Vehicular Cloud Networking

The main motivation of VANET is to provide safety on roads and infotainment to vehicular user while VCN provides more resources for these applications. Ensuring security, privacy and trust in these applications is a vital aspect in VCN. VCN involves different assets which need security from an attacker. The assets in VCN are: vehicles, vehicular user, wireless communication, messages, adjacent infrastructure,

and clouds i.e., VC, IC and BEC. To secure VCN environment, it is necessary to identify the possible threats in all assets. This section introduces threats for every asset of 3-tier structure of VCN.

### A. Threats to Tier-1 and Tier-2 Clouds

The threats in this category are specific to tier-1 and tier-2 clouds of VCN. The threats lies to the vehicles, adjacent infrastructure, messages, wireless communication and the resources which vehicles and RSU share among them. The threats can be exploited as:

- *Vehicle:* Usually, VCN involves highly mobile vehicles and the two vehicles communicate with each other for a very short span of time to form VC [14]. However, there are still some threats to vehicles and its different components. The attacker can plan to access the On-Board Unit (OBU) or Application Unit (AU) of vehicle and sensors. The threat also lies to the software running on AU and sensors where strong aim of attackers is to introduce malware. Firmware updates are also one of the targets where the attacker injects malicious code inside the in-vehicle network via high speed internal buses. This can lead to drastic results e.g., the attacker can misconfigure the sensor with its malicious code [15].
- *Adjacent Infrastructure:* Infrastructure includes the static entity called RSU. As these are not mobile, the major threats lie to its hardware. Usually, physical security to RSU hardware is provided via CCTV. Other threats to infrastructure includes illegal access of attacker to its software platform and DoS attack.
- *Wireless Communication:* Wireless communication is a medium, responsible for exchanging messages with neighbouring vehicles and adjacent RSU via V2V and V2I communication. As this wireless medium is exposed to different vulnerabilities, if offers several opportunities for an attacker to exploit it for its own benefits [16]. The threats to wireless communication includes Denial of Service (DoS), tempering and alteration of the messages en route and jamming the wireless communication channel etc.
    - *Denial of Service (DoS):* DoS attack is one of the critical attacks in ad hoc networks and in case of VCN, it can leave a severe impact on the network. In this attack, the attacker blocks the communication channel by refusing other cloud members to forward important messages to the cloud, other vehicles and RSU in the vicinity.
    - *Data Tempering:* In this attack the main motivation of the attacker is to alter and modify the messages en route to vehicles, RSU, IC and VC [17].
    - *Jamming the wireless communication channel:* This type of attack results in the complete jam of wireless medium responsible to carry the messages. Jamming of the wireless medium is the result of DoS attack most of the time.
- *Messages:* Messages contain important information about a particular event, which are usually exchanged among the vehicles and adjacent RSUs during V2V and V2I communication. Threats to these messages always exist where the main interest of an attacker is to compromise its confidentiality, integrity and authenticity (CIA). Threats in this category can be exploited in following different security aspects.
    - *Threats to Confidentiality of Message:* Confidentiality is a significant security aspect which provides secrecy by limiting access of attacker to the message. The threat caused by this aspect is the illegal monitoring of transmitted message to the clouds via V2V and V2I communication.
    - *Threats to Authenticity of Message:* The routing of accurate and authentic messages should be ensured in VCN as it involves several life saving contexts. The source and destination of messages must be known and verifiable. The threat lies to messages from this perspective is the ID theft of vehicular user from an attacker. This can lead to severe and drastic results in VCN, especially during the event of an accident.
    - *Threats to Integrity of Message:* Message transmitted from source should arrive at destination without any alteration to its content. Similarly, the nodes sending or retrieving the messages from all clouds must receive the message in its original content. The threat from this aspect is that the message can be tempered, modified or deleted from attacker in transit while carrying the transmission of message between vehicles and clouds [18]. Therefore, the integrity of message in both modes of communication i.e., V2V and V2I should be ensured.
    - *Threat to Availability of Message:* Since the main aim of vehicular network is to provide drivers safety, it should be ensured that the message transmitted from any vehicle and tier-1 and tier-2 cloud regarding any particular context is available to other neighbouring vehicles and adjacent RSU.
    - *Non-repudiation:* Non-repudiation ensures the message generated from sender and receiver is verifiable by the authorities [19]. Therefore, the senders should be responsible for the messages generated. The threat from this category is the denial of message produced by sender or denial of message reception by receiver through the clouds.
- *Vehicular Cloud:* As VC is the result of sharing of

computational and storage resources of vehicles, the main threats lies to its cloud platform itself. An adversary may attack the cloud by injecting malware into the cloud platform. Threat also lies to the important messages, as these are communicated between the vehicles through this cloud. Privacy is also one of the important security aspects which aims to ensure that the identity of the vehicular user is kept secret from an unauthorized person [20]. The threats in this regard includes revealing the vehicular user identity, its geographical location and sensitive information.

- *Infrastructure Cloud:* Since both static and mobile entities are involved in IC, the threats lies to both cloud platform and the propagating messages. The attacker may prevent the static RSU to exchange messages with other members by implementing DoS attack. Threats also exists to the messages which are communicated via IC. The possible scenario is the rouge cloud member, which becomes part of the cloud to steal important information via spoofing. This can produce threat to the privacy of the user information. This rouge cloud member must be identified and cleverly removed from the cloud.

### B. Threats to Tier-3 Cloud

In this section, we discuss the important threats related to tier-3 of VCN. As discussed earlier, tier-3 named BEC is the largest cloud involved in VCN. Therefore, it is vulnerable to different kinds of threats and the most critical among those are the data and network threats.

- *Data:* Data is one of the most important resource for any organization. In the case of VCN, sensitive vehicular data will be stored in the cloud. However, back-end cloud data is vulnerable to many threats. These threats can lead to loss or leakage of data. As a result of these threats the security properties of data such as confidentiality, integrity and availability might not be preserved [21]. Cloud Security Alliance (CSA) [22] has mentioned data threats including data breaches and data loss as the most severe threats in BECs.
    - *Data Breaches:* Data breach in BEC is the leakage of vehicular data to an unauthorized entity who does not have the legal right to view that particular data. According to CSA, 91 percent of cloud tenants consider it as a significant threat in cloud computing [22]. It can result in the loss of data security properties of confidentiality and integrity. Data breaches in BEC mostly occur due to flaws in application designing, operational issues, insider attackers, and insufficiency of authentication, authorization and audit controls. Moreover, Virtual Machine (VM) Escape attack [23] can be used to breach vehicular data in a cloud environment. Thomas R. et. al. [24] described the possibility of mapping the internal infrastructure of cloud environment. They performed experiments on Amazon EC2 cloud and showed that it is possible to identify the location of a target VM (VM processing vehicular data) in cloud.
    - *Data Loss:* Data loss is referred to the loss of vehicular data in the BEC. Data life cycle in BEC has five main stages including creation, transfer, processing, storage and destruction. Once the vehicular data has been transferred to the cloud, it will be processed by applications, and stored in the BEC storage. Data loss can occur during data transfer to and from BEC, during processing by applications or in BEC storage [25]. CSA in their survey [22] have listed data loss is the second most significant threat in cloud computing with almost 91 percent of cloud tenants considering it as a significant threat.
- *Network:* Cloud services in the infrastructure of BEC run through internal network or internet. A large number of customers use different networks and devices to connect and use the cloud resources. Business employees, contractors and partners may use an enterprise application on BEC through a mobile phone. These features of BEC mean that traditional network security methods are not enough for securing the BEC network. If the required security measures in BEC networks are not implemented they can be vulnerable to different attacks.
    - *Account or Service Hijacking:* Account or service hijacking is a term referred to an attack in which attacker steals the credentials of victims to access their vehicular data and services in cloud. This not only results in loss of confidentiality, integrity and availability of vehicular data but attacker can also use these credentials to launch attacks from victims account. Account or service hijacking is mostly done by the network attacks such as phishing, SQL injection, cross-site scripting (XSS), botnets and software vulnerabilities such as buffer overflow.
    - *Denial of Service:* Denial of Service (DOS) attacks can be launched from BEC services or from outside the BEC that consume the resources including data, storage, virtual machines and network bandwidth. This results in the unavailability of these resources to the legitimate users due to which vehicular services running on infrastructure cloud will be unable to respond to user requests. DOS attacks are very common in cloud computing and 81 percent of cloud tenants consider it as a relevant threat [22]. Another variant of DOS attack is Distributed Denial of Service (DDOS) attack in which more than one source is used to launch this attack [26].
    - *Insecure Interfaces and APIs:* Application Programming Interfaces (APIs) is a set of rules

that governs how applications communicate with each other and the underlying operating systems or libraries. All the BEC service models including IaaS, PaaS and SaaS have standard and custom APIs for their applications. Different applications can be integrated into the BEC using APIs and cloud providers have introduced APIs for their platforms [27]. Some of the widely used APIs are Amazon Web Service (AWS) API, OpenStack API, Google Compute Engine, and VMware vCloud API.

## VI. Conclusion

Vehicular Cloud Networks (VCN) is the merging of VANET technology with cloud computing that changes way of network service provisioning and helps vehicular users to use cloud according to their requirements. VCN helps the vehicular users by providing them traditional safety features of VANETs as well as the additional features to share small vehicular resources or acquire high computational capabilities. In this paper the different categories of clouds involved in VCN are explained by dividing them in a three tier architecture. This architecture explains the mechanisms through which vehicular users can use different VCN clouds including vehicular cloud, infrastructure cloud and back-end cloud. The use cases presented in the paper explain the formation of each cloud tier for different scenarios such as urban areas, rural areas and parking. This paper also provides an in-depth analysis of different security threats in each tier of VCN cloud. For tier-1 and tier-2 clouds, the threats are identified according to vehicle, adjacent infrastructure, wireless communication, important messages, vehicular clouds and infrastructure clouds. Similarly, for tier-3 cloud threats are identified as data and network threats. In our future work, we will analyse the possible security solutions that secure the VCN technology by mitigating the possible threats.

## References


[1] S. K. Bhoi and P. M. Khilar, "Vehicular Communication: A Survey," *Networks IET*, vol. 3, pp. 204–207, 2014.

[2] G. Grassi, D. Pesavento, G. Pau, R. Vuyyuru, R. Wakikawa, and L. Zhang, "VANET via Named Data Networking," in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 410–415, IEEE, 2014.

[3] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," 2011.

[4] M. Garai, S. Rekhis, and N. Boudriga, "Communication as a Service for Cloud VANETs," in *20th IEEE Symposium on Computer and Communications (ISCC'15)*, IEEE, 2015.

[5] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A Survey on Vehicular Cloud Computing," *Journal of Networks and Computer Applications*, vol. 40, pp. 325–344, 2014.

[6] S. Olariu, M. Eltoweissy, and M. Younis, "Towards Autonomous Vehicular Clouds.," *EAI Endorsed ICST Transactions on Mobile Communications and Applications*, vol. 11, p. e2, 2011.

[7] D. Bernstein, N. Vidovic, and S. Modi, "A Cloud PAAS for High Scale, Function, and Velocity mobile Applications-with Reference Application as the Fully Connected Car," in *Proceedings of the 2010 Fifth International Conference on Systems and Networks Communications (ICSNC)*, pp. 117–123, IEEE Computer Society, 2010.

[8] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, "Rethinking Vehicular Communications: Merging VANET with Cloud Computing," in *Proceedings of the 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom)*, pp. 606–609, IEEE Computer Society, 2012.

[9] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward Cloud-based Vehicular Networks with Efficient Resource Management," *IEEE Network*, vol. 27, pp. 48–55, September 2013.

[10] G. Yan, D. B. Rawat, and B. B. Bista, "Towards Secure Vehicular Clouds," in *Sixth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)*, pp. 370–375, July 2012.

[11] G. Yan, D. Wen, S. Olariu, and M. Weigle, "Security Challenges in Vehicular Cloud Computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, pp. 284–294, March 2013.

[12] F. Ahmad, M. Kazim, and A. Adnane, *Vehicular Cloud Networks: Architecture and Security*, ch. Guide to Security Assurance for Cloud Computing. Springer. DOI: 10.1007/978-3-319-25988-8 [In press].

[13] E. Lee, E.-K. Lee, M. Gerla, and S. Oh, "Vehicular Cloud Networking: Architecture and Design Principles," *IEEE Communications Magazine*, vol. 52, pp. 148–155, February 2014.

[14] Q. Alriyami, A. Adnane, and A. Kim Smith, "Evaluation Criterias for Trust Management in Vehicular Ad-hoc Networks (VANETs)," in *The 3rd International Conference on Connected Vehicles & Expo (ICCVE 2014)*, IEEE, 2014.

[15] D. K. Nilsson and U. E. Larson, "Conducting Forensic Investigations of Cyber Attacks on Automobile In-vehicle Networks," in *Proceedings of the 1st ACM international conference on Forensic applications and techniques in telecommunications, information, and multimedia*, 2008.

[16] C. Laurendeau and M. Barbeau, "Threats to Security in DSRC/WAVE," in *Proceedings of 5th International Conference on Ad-Hoc Networks and Wireless*, pp. 266–279, Springer, 2006.

[17] G. Yan, D. Rawat, and B. Bista, "Towards Secure Vehicular Clouds," in *Sixth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)*, pp. 370–375, July 2012.

[18] K. Plossl, T. Nowey, and C. Mletzko, "Towards a Security Architecture for Vehicular Ad Hoc Networks," in *IEEE First International Conference on Availability, Reliability and Security (ARES)*, April 2006.

[19] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET Security Challenges and Possible Cryptographic Solutions," *Vehicular Communications*, vol. 01, pp. 53–66, April 2014.

[20] J. Grover, M. S. Gaur, and V. Laxmi, "Trust Establishment Techniques in VANET," *Springer, Wireless Networks and Security, Signal and Communication Technology*, pp. 273–301, 2013.

[21] M. Kazim and S. Y. Zhu, "A Survey on Top Security Threats in Cloud Computing," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 6, no. 3, 2015.

[22] Top Threats Working Group *et al.*, "The Notorious Nine: Cloud Computing Top Threats in 2013," *Cloud Security Alliance*, 2013.

[23] K. Kortchinsky, "Cloudburst: A VMware Guest to Host Escape Story," *Black Hat USA*, 2009.

[24] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of my Cloud: Exploring Information Leakage in Third-Party Compute Clouds," in *Proceedings of the 16th ACM conference on Computer and communications security*, pp. 199–212, ACM, 2009.

[25] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, *et al.*, "A View of Cloud Computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[26] F. Sabahi, "Cloud Computing Security Threats and Responses," in *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, pp. 245–249, IEEE, 2011.

[27] D. Petcu, C. Craciun, and M. Rak, "Towards a Cross Platform Cloud API," in *1st International Conference on Cloud Computing and Services Science*, pp. 166–169, 2011.