12 Vehicular Cloud Networks: Architecture and Security

Farhan Ahmad, Muhammad Kazim, and Asma Adnane

Abstract

Cloud computing has been widely adopted across the IT industry due to its scalable, cost-effective, and efficient services. It has many applications in areas such as healthcare, mobile cloud computing (MCC), and vehicular ad hoc networks (VANET). Vehicular cloud networks (VCN) is another application of cloud computing which is a combination of cloud and VANET technologies. It is composed of three clouds named vehicular cloud, infrastructure cloud, and traditional IT cloud. In this chapter, the three clouds involved in VCN are presented using a three-tier architecture, and the security issues related to each tier are described in detail. After describing the detailed architecture of VANET, their components, and their important characteristics, this chapter presents the architecture of VCN. It is followed by the detailed analysis of the threats to which each tier-cloud of VCN is vulnerable.

Keywords

Cloud computing • Vehicular ad hoc networks • Vehicular cloud networks • Three-tier architecture • Security • Threats

12.1 Cloud Computing

Cloud computing is a model that enables users to access resources such as infrastructure (hardware, processing, memory, network, and services), platform (custom applications), and software through Internet according to their requirements. This

F. Ahmad (✉) • M. Kazim • A. Adnane
Department of Computing and Mathematics, College of Engineering and Technology, University of Derby, Derby, UK
e-mail: f.ahmad@derby.ac.uk; m.kazim@derby.ac.uk; a.adnane@derby.ac.uk

S.Y. Zhu et al. (eds.), *Guide to Security Assurance for Cloud Computing*,
Computer Communications and Networks, DOI 10.1007/978-3-319-25988-8_12

helps the businesses to reduce costs by enabling them to pay only for the services they use and saves them from investing heavily on IT infrastructure. Cloud has been widely adopted in IT industry across the world during the last decade. The major advantages that cloud provides are easy access to information and resources, less personnel training, ability to scale up or scale down the resources easily, business continuity through backup and recovery, quick deployment, and cost efficiency. As a result, all the major companies including Apple, Samsung, Google, Microsoft, and Amazon are using cloud computing for different applications.

The amount of data being transferred to cloud services such as iCloud, Dropbox, and Google Drive is increasing every day. Along with that, cloud has many applications in various areas where it is used in combination with different technologies. Mobile cloud computing is referred to as an architecture in which data storage and data processing take place outside the mobile device and in the cloud. Users can access data in cloud through wireless Internet. As a result, not only the mobile applications can be used by a large number of cloud customers, but also the mobile devices do not need to have large processing power and storage to process data. Some applications of mobile cloud computing include mobile commerce, mobile learning, mobile healthcare, and mobile gaming [48]. Many health organizations are using cloud computing to store the record of their patients anonymously.

Another application of cloud computing is in vehicular ad hoc networks (VANET). VANET is a technology that uses short-range communication protocols such as wireless local area network (WLAN) technology to create a mobile network among vehicles in an approximately 100 to 300 m distance [45]. All the participating vehicles in VANET act as wireless nodes, and they can exchange different messages among each other and adjacent roadside infrastructure to support traffic safety and make driving experience more comfortable. Some of the messages that can be exchanged between vehicles in VANET are vehicle collision warning, security distance warning, driver assistance, cooperative driving, and dissemination of road information, Internet access, map location, automatic parking, and driverless vehicles [17].

Vehicular cloud networks (VCN) is a promising technology which introduces the concept of merging VANET technology with cloud computing. This provides an unlimited computing resources and storing/downloading VANET data via the Internet. The extension of traditional computing facilities with vehicular computing resources such as storage, processing, and sensing can help drivers in new ways to overcome critical road safety and congestion issues.

Rest of the chapter is organized as follows: Section 12.2 introduces the VANET in detail including its architecture, components, and its different characteristics. Section 12.3 leads to VCN where the three-tier architecture and its operation is explained. Threats in VCN are introduced in Sect. 12.4, where different threats in each tier are explained in detail and the review questions are given in Sect. 12.5.

12.2 Vehicular Ad Hoc Networks (VANET)

VANET are considered as the backbone of intelligent transportation system (ITS) as it ensures traffic safety and traffic assistance. This section introduces the VANET architecture, its different components, and their characteristics in detail.

12.2.1 VANET Architecture

VANET is an emerging technology with its main motivations to ensure life safety and security on the roads. In VANET, the vehicles are equipped with communication interfaces, which enable the transportation of important messages between neighboring vehicles and adjacent infrastructure in the vicinity of communication range [4]. Infrastructure refers to the static entities and is mostly positioned along the roadside. In the context of VANET, this refers to *roadside units (RSUs)*. This includes a speed camera, relay node (RN), or mobile communication base station.

In VANET, the transportation of messages is carried via two modes. These are

1. Vehicle-to-vehicle (V2V) communication
2. Vehicle-to-infrastructure (V2I) communication

In V2V communication, the messages are shared with neighboring vehicles via short-range communication protocols. These include dedicated short-range communication (DSRC) technologies and wireless LAN protocols, i.e., IEEE 802.11. V2V communication results in short-range communication where it ensures communication between neighboring vehicles without any support from infrastructure. On the other hand, V2I communication ensures communication between vehicles and adjacent infrastructure with the help of RN or any mobile communication technologies such as long-term evolution (LTE). V2I communication is used for transporting messages generated by source vehicle over large geographical location.

Figure 12.1 depicts the architecture of VANET in case of an accident. It can be seen that the vehicles close to the vicinity of accident receives messages via V2V communication, while other vehicles receives messages via V2I communication.

12.2.2 Components of VANET

VANET consists of several components, i.e., vehicular user, vehicle, messages, infrastructure, wireless communication network, back-end server, and attackers.

- *Vehicular user:* Vehicular user constitutes the most important entity in VANET. The user privacy including personal data, geographical location, and confidential information must be guaranteed in VANET.
- *Vehicle:* The important assets in vehicle are its on-board unit (OBU) with communication capabilities, application unit (AU) with several applications

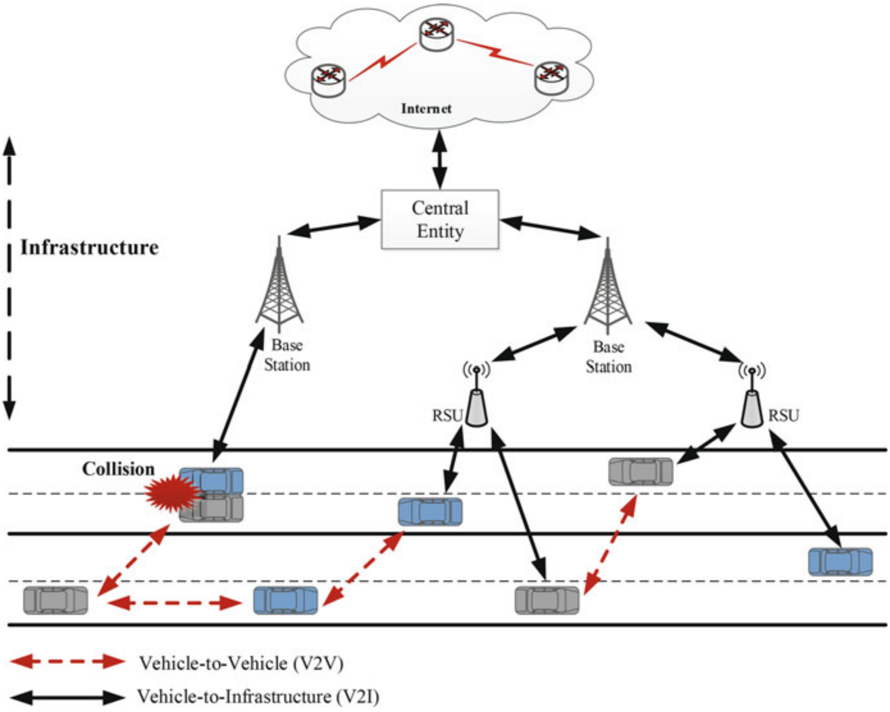

Fig. 12.1 VANET architecture; example of collision of vehicles

like collision avoidance system, and different sensors which collect information from surroundings.

- *Messages:* Messages contain various important information which are exchanged between vehicles and adjacent RSU. This contains accident warning, driver and vehicular passenger information, confidential data, weather and road traffic information, etc.
- *Infrastructure:* Infrastructure acts as a bridge for exchanging messages between vehicles and back-end server. Infrastructure also enables the messages to be transmitted over a large geographical location. This includes adjacent RSUs, speed camera, and RNs.
- *Wireless communication network:* It provides the air interface to transmit the important messages to neighboring vehicles and RSUs. In VANET, there are three types of communication.

1. In-vehicle communication between OBU and sensors via internal high-speed buses
2. Communication between two vehicles via DSRC technologies
3. Communication between vehicle and RSU via mobile communication such as LTE and RN

- *Back-end server:* Back-end server lies in the Internet domain containing the application server such as collision avoidance application server. The messages received on server are transmitted via RSU to vehicles on large geographical location.
- *Attacker:* Attacker is a temporary component in VANET; it is usually active for a short period of time. The main motivation of attacker is to manipulate the information and modify the information and vehicular network for his own benefits. The attacker must be identified and eliminated from the network intelligently.

12.2.3 Important Characteristics of VANET

VANET is designed to provide a safe and comfortable journey to the vehicular user on the road. VANET is also useful in fleet management where different vehicles have identical destination address [5, 6]. However, VANET relies on applications which depend on the availability of different vehicles and RSUs in the vicinity of source vehicle to transport the messages. These generated messages must arrive at the destination without any alteration from an attacker as this can lead to a drastic impact on the overall network operation and performance. Therefore, from security point of view, integrity of the information is one of the important aspects in VANET [7, 8].

VANET possess different unique properties which makes them different from other ad hoc networks. These are as follows:

12.2.3.1 Decentralized Systems

One of the main characteristics of VANET is the distributed and decentralized system since the occurrence of fixed infrastructure is not guaranteed in VANET. This lack of central entity poses different challenges such as secure message routing and QoS [9].

12.2.3.2 High-Speed Mobility and Dynamic Topology

VANET involves high-speed vehicles which are mostly randomly dispersed in the network. According to [10], two vehicles meet each other for a very short span of time which makes the network highly dynamic with constantly changing topology. Therefore, the availability of messages for this randomly changing topology must be ensured.

12.2.3.3 Cooperative Message Routing

Since VANET lacks centralized routing entity, the cooperation between two vehicles is necessary for message routing. Due to high-speed mobility of vehicles, the routing table cannot be maintained and updated all the time. Researchers have proposed different routing protocols in VANET which are grouped in six categories: topology-based routing, geo-cast routing, broadcast-based routing, position-based routing, infrastructure-based routing, and cluster-based routing [10–12].

12.2.3.4 Real-Time Processing

Real-time processing of information in VANET is of great importance since any delay in the important life-saving situation might affect the network severely. The information in VANET must ensure the security requirements, i.e., confidentiality, availability, authenticity, and integrity, and must ensure to process the safety messages in real-time environment [13].

12.2.3.5 User and Data Privacy

Vehicular user constitutes the most vital entity in VANET. Privacy of the vehicular user's information such as name, address, and geo-location must be secured from the malicious attacker [14].

12.3 Vehicular Cloud Networking (VCN)

VANET usually involves vehicles equipped with different communication interfaces which enable the vehicles to communicate with others via dedicated short-range communication (DSRC) or mobile communication such as long-term evolution (LTE) [15, 16]. Each vehicle posses some storage and computation resources. Due to fixed size hardware limitations of vehicles, these storage and computation resources are limited in nature. In the future, the bandwidth hungry applications such as vehicular user multimedia applications and social networking applications may not be supported by the vehicle itself. Therefore, different vehicles must cooperate together to share their resources, resulting in a newly emerging vehicular technology, called vehicular-based cloud networks (VCN).

In recent years, different research projects have been carried out which merge VANET with cloud computing. The concept of VCN was first introduced by the authors in [17] in the form of autonomous vehicular clouds (AVC). In AVC, the computing and communication resources are assigned dynamically to the users. In [18], the authors have taken a step further where they introduced a platform as a service (PaaS) model to provide multiple services to users in a highly dynamic environment. Hussain et al. proposed an architecture with multiple clouds such as vehicular cloud (VC), vehicles using clouds (VuCs), and hybrid clouds (HCs) [19]. The authors in [20] proposed a hierarchical structure of cloud computing in vehicular networks. However, security aspect of VCN is missing in existing literature. The main contribution of this chapter is twofold: Firstly, it presents a 3-tier architecture of cloud-based vehicular networks, and, secondly, it identifies threats in each tier of the architecture.

12.3.1 Vehicular-Based Cloud Networking (VCN) Architecture

The hierarchical architecture of VCN is depicted in Fig. 12.2. It is a three-tier architecture which consists of following levels:

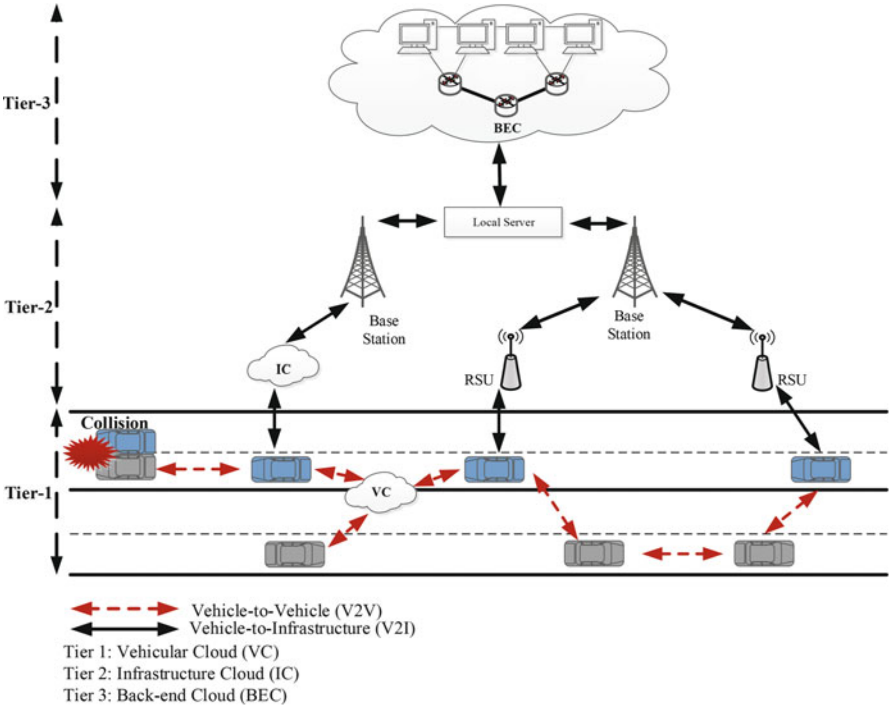
Tier-3
Tier-2
Tier-1
BEC
Local Server
Base Station
Base Station
IC
RSU
RSU
Collision
VC
Vehicle-to-Vehicle (V2V)
Vehicle-to-Infrastructure (V2I)
Tier 1: Vehicular Cloud (VC)
Tier 2: Infrastructure Cloud (IC)
Tier 3: Back-end Cloud (BEC)

Fig. 12.2 Vehicular-based cloud networking architecture

1. Tier-1 cloud: vehicular cloud (VC)
2. Tier-2 cloud: infrastructure cloud (IC)
3. Tier-3 cloud: back-end cloud (BEC)

1. ***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 information is shared between vehicles via V2V communication. Due to high mobility and dispersed distribution of vehicles in the network, the formation of VC is technically very difficult. The best example to implement VC is for fleet vehicles where the start and destination of the vehicles are mostly similar. These fleet vehicles can share their resources, resulting in a VC which can be used to serve different applications such as road information, weather information, etc.
2. ***Infrastructure cloud (IC):*** IC is initiated by adjacent RSU along the road where other vehicles request to access the services provided by the cloud. The scope of this cloud is local to small geographical area where RSU is located. Communication between two different ICs is carried out through dedicated local servers. The technically difficulty of formation of this cloud varies in different scenarios. If an extensive amount of RSU is available in a region, then different

vehicles and RSUs can share their resources resulting in IC. However, despite the fact that VCN mostly faces high-speed mobility of vehicles in the network, IC is technically formed for a very short span of time.

3. ***Back-end cloud (BEC):*** Back-end cloud is the largest 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 [20]. The scope of BEC is spread over the large geographical area to serve the vehicles.

12.3.2 Vehicular-Based Cloud Networking (VCN) Operation

To create and initiate a cloud in vehicular networks, it needs a cloud leader. If leader is a vehicle and no RSU participates in its cloud formation, then the cloud created is VC. However, if the request for cloud is initiated by RSU, then it forms IC, where other vehicles can access the resources of cloud.

The cloud leader invites other vehicles and RSUs in its vicinity by transmitting the 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) where these vehicles act as cloud members [21]. When cloud leader receives the confirmation via REP messages, it keeps its members' ID and assigns different tasks to them. 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 to maintain the cloud it created. However, if any member wishes to leave, the cloud sends the resource, leaving message to the cloud leader. In that case, the cloud leader releases that specific member and recruits new members by broadcasting REQ messages. However, in case a cloud leader no longer wants to keep the cloud, it broadcasts the cloud release message.

12.4 Threats in Vehicular-Based Cloud Networking

VCN extends the list of assets explained in Sect. 12.2.2 by adding assets related to cloud itself. This includes data, custom, and user-defined applications and infrastructure. This section introduces different threats to 3-tier structure of VCN.

12.4.1 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 lie to the vehicles, adjacent infrastructure, messages, wireless communication, and the resources which vehicles and RSU share among them. The threats can be exploited as:

12.4.1.1 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. However, there are still some threats to vehicles and its different components. The attacker can plan to access the OBU or AU of vehicle and sensors. The threat also includes the software running on AU and sensors where the 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 CAN. This can lead to drastic results, e.g., the attacker can misconfigure the sensor with its malicious code [22, 23].

12.4.1.2 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 include illegal access of attacker to its software platform and DoS attack.

12.4.1.3 Wireless Communication

Wireless communication is a medium, responsible for exchanging messages with other vehicles. This includes both V2V and V2I communication. As this wireless medium is exposed to different vulnerabilities, if offers several opportunities to an attacker to exploit it for its own benefits. The threats to wireless communication include 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:* The main motivation of the attacker is to alter and modify the messages en route to vehicles, RSU, IC, and VC in this attack [24].
- *Jamming the wireless communication channel:* This type of attack results in the complete jamming of wireless medium responsible to carry the messages. Jamming of the wireless medium is the result of DoS attack most of the time.

12.4.1.4 Messages

Messages contain important information about a particular event, which is usually exchanged among the vehicles and adjacent RSUs during V2V and V2I communication. Threats to these messages always exist where the main interest of the attacker is to compromise its confidentiality, integrity, and authenticity (CIA). The threats to information can be exploited in the 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 transmitted in V2V and V2I communication.

- *Threats to authenticity of message:* The routing of accurate and authentic message 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 which 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 the destination without any alteration to its 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 two vehicles [25]. Therefore, 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 neighboring vehicles and adjacent RSU.
- *Non-repudiation:* Non-repudiation ensures the message generated from sender and receiver is verifiable by the authorities [26]. 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.

12.4.1.5 Vehicular Cloud

As VC is the result of sharing of computation and storage resources of vehicles, therefore, the main threats lie to the 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 aim to ensure that the identity of the vehicular user is kept secret from an unauthorized person [27]. The threats in this regard include revealing the vehicular user identity, its geographical location, and sensitive information.

12.4.1.6 Infrastructure Cloud

Since both static and mobile entities are involved in IC, the threats lie to both cloud platform and the messages. The attacker may prevent the static RSU to exchange messages with other members by implementing DoS attack. Threats also exist to the messages which are communicated via infrastructure cloud. 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.

12.4.2 Threats to Tier-3 Cloud

In this section, we focus on the threats that can be used to launch attacks on the tier-3 cloud. These attacks can be launched on the vehicular data once it has been transferred to a traditional IT cloud. We do not consider the attacks on the vehicular cloud which is temporarily formed among vehicles in local area to share their data and processing.

12.4.2.1 Data Breaches

Data breach in infrastructure cloud is the leakage of vehicular data to an unauthorized entity who does not have the legal right to see that data. Data breach is a very common attack, and Cloud Security Alliance (CSA) [28] has mentioned it as the most critical threat in cloud. According to CSA, 91 % of cloud tenants consider it as a significant threat in cloud computing. It can result in the loss of data security properties of confidentiality and integrity.

Data breaches in infrastructure cloud 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 [29] can be used to breach vehicular data of other users in a cloud environment. To launch a VM escape attack, an attacker leases a VM in cloud to run a script through which he can break out of his VM and access the code of Virtual Machine Manager (VMM). Having access to the code of VMM provides root privileges to the attacker who can access the data from services processing vehicular data on cloud. Similarly, attacker will also be able to access the vehicular data if it is stored in cloud or being processed by any application.

12.4.2.2 Data Loss

Data loss is referred to the loss of vehicular data in infrastructure cloud. Data life cycle in cloud has five main stages, namely, 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 cloud storage. Data loss in cloud occurs during data transfer to and from cloud, during processing by applications or in cloud storage [30]. CSA in their survey have listed data loss is the second most significant threat in cloud computing with almost 91 % of cloud tenants considering it as a significant threat [28]. Data loss mostly occurs due to insider attacks which include data deletion, data corruption, and loss of data encryption key and other issues such as faults in storage system and natural disasters.

12.4.2.3 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 data and services in cloud [31]. This not only results in loss of confidentiality, integrity, and availability of data, but attacker can also use these credentials to launch attacks from victims' account. Account or service hijacking of vehicular data can be done by the network attacks such as phishing, SQL injection, cross-site scripting (XSS), botnets, and software vulnerabilities such as buffer overflow. In phishing attacker usually sends an email that seems to come from a legitimate authority to the user with the purpose of stealing his identity such as login credentials. XSS is done by compromising the web application to contain a malicious script which maybe a JavaScript, HTML, or flash and sending it to a benign user, while botnet is a network of interconnected computers over the Internet that can perform automated tasks such as distributed denial of service attack.

12.4.2.4 Denial of Service

Denial of service (DOS) attacks can be launched from cloud services or from outside the cloud 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 % of cloud tenants consider it as a relevant threat [28]. Another variant of DOS attack is distributed denial of service (DDOS) attack in which more than one sources are used to launch this attack [32]. Some attack sources in DDOS attack are legitimate users who are compromised by network attack such as Trojan which makes the DDOS hard to detect. Other ways of launching DOS attack include exploiting the vulnerabilities in web server, databases, and applications, resulting in unavailability of resources.

12.4.2.5 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 cloud service models including IaaS, PaaS, and SaaS have standard and custom APIs for their applications. Different applications can be integrated into the cloud using APIs, and cloud providers have introduced APIs for their platforms. Some of the widely used APIs are Amazon Web Service (AWS) API, Google Compute Engine, VMware vCloud API, and OpenStack API [33]. The security of an application in cloud depends on the security of its APIs. Insecure APIs on vehicular services can result in the violation of authentication and access control principles. Moreover, the attacker having access to data can lead to the loss of data confidentiality or integrity.

12.4.2.6 Malicious Insider

Malicious insider is an employee of the cloud organization with access to its resources and assets such as data, but he misuses his privileges to perform unauthorized actions. CSA has defined malicious insider as the employee whose actions result in the loss of security properties of confidentiality, integrity, or availability of organization's information or information systems. Having malicious insiders is a critical threat in cloud with 88 % of cloud users considering it as a relevant issue [28]. Malicious insiders can also be hobbyist attacker who exploits organizations' resources weaknesses just for fun. Moreover, lack of security measures for vehicular applications protection in cloud can also be exploited by the malicious insiders.

12.4.2.7 Abuse of Cloud Services

Abuse of cloud services in VCN is referred to the tenants who misuse the vehicular cloud services they have purchased. Misuse includes the illegal or unethical use of services by tenants that violate their contract with service provider which is called service-level agreement (SLA) [34]. Abuse of cloud services was the most common threat in cloud computing in 2010, but different security measures were introduced to prevent it, and now it is the seventh most critical threat in cloud computing. Cloud services have been used to launch different attacks over the years. A botnet attack was launched in 2009 using Amazon's EC2 services as the command and control servers for that attack [35]. Similarly, the unlimited computation power of cloud can be used to launch password-cracking attacks such as brute force, performing DOS attacks and others such as cross-site scripting.

12.4.2.8 Shared Technology Vulnerabilities

Cloud service provider's provision shared resources such as computation, network, and storage resources to different users. However, the sharing of resources such as hard disk, RAM, and GPUs might not offer perfect isolation. If isolation is not properly implemented, a malicious attacker can get unauthorized access to cloud resources, VMs, customer's data, and sensitive vehicular data. Almost 82 % of users consider shared technology vulnerabilities as a relevant threat in cloud that can have impact on IaaS, PaaS, and SaaS services models [28]. XEN is an open-source virtualization platform for cloud that has a XEN hypervisor with API toolstack and other features [36]. A vulnerability of local privilege escalation was found in XEN that can be used to launch guest to host virtual machine escape attack.

12.5 Review Questions

1. What are the main characteristics of the modes of transporting messages in VANET?
2. Identify different key infrastructure components in VANET and explain their main purpose.
3. How important is real-time processing in context of VANET?
4. What are the key differences between the clouds in three-tier architecture of VCN?
5. To which attacks is the wireless communication in VCN most vulnerable?
6. What is the difference between the threats to the authenticity of message and non-repudiation in VCN?
7. What are the main stages in data life cycle in cloud? In which stages can data loss occur?
8. Name the attacks that can be launched in tier-three cloud network to hack accounts or services.
9. How can the tier-three cloud services be misused by tenants?
10. Which shared technology vulnerability was discovered in XEN virtualization platform?

References

1. Dinh HT, Lee C, Niyato D, Wang P (2013) A survey of mobile cloud computing: architecture, applications, and approaches. Wirel Commun Mob Comput 13(18):1587–1611
2. Chandrasekaran G (2008) VANETs: the networking platform for future vehicular applications. Department of Computer Science, Rutgers University
3. Boukerche A, Oliveira HA, Nakamura EF, Loureiro AA (2008) Vehicular ad hoc networks: a new challenge for localization-based systems. Comput Commun 31(12):2838–2849
4. Ahmad F, Adnane A (2015) Design of trust based context aware routing protocol in vehicular networks. In: Ninth IFIP WG 11.11 international conference on trust management (IFIPTM'15), Hamburg
5. Ahmad F, Marwat SNK, Zaki Y, Goerg C (2014) Tailoring LTE-advanced for M2M communication using wireless inband relay node. In: Proceedings of world telecommunications congress 2014 (WTC'14). VDE, Berlin, Germany, pp 1–3
6. Ahmad F, Marwat SNK, Zaki Y, Mehmood Y, Cörg C (2014) Machine-to-machine sensor data multiplexing using LTE-advanced relay node for logistics. In: 4th international conference on dynamics in logistics (LDIC'14), Bremen
7. Mármol FG, Kuhnen MQ (2013) Reputation-based web service orchestration in cloud computing: a survey. Concurr Comput Pract Exp. doi: 10.1002/cpe.3177
8. Alriyami Q, Adnane A, Kim Smith A (2014) Evaluation criteria for trust management in vehicular ad-hoc networks (VANETs). In: The 3rd international conference on connected vehicles & expo (ICCVE 2014), Vienna. IEEE
9. Raya M, Hubaux J-P (2007) Securing vehicular ad-hoc networks. J Comput Secur 15(1):39–68
10. Li F, Wang Y, Routing in vehicular ad-hoc networks: a survey. IEEE Veh Technol Mag
11. Lin Y-W, Chen Y-S, Lee S (2010) Routing protocols in vehicular ad hoc networks: a survey and future perspectives. J Inf Sci Eng 26(3):913–932
12. Benamar M, Benamar N, Singh KD, El Ouadghiri D (2013) Recent study of routing protocols in VANET: survey and taxonomy. In: WVNT 2013: 1st international workshop on vehicular networks and telematics, Marrakech
13. Al-kahtani M (2012) Survey on security attacks in vehicular ad hoc networks(VANETs). In: 6th international conference on signal processing and communication systems (ICSPCS), Gold Coast, pp 1–9
14. Wex P, Breuer J, Held A, Leinmuller T, Delgrossi L (2008) Trust issues for vehicular ad-hoc networks. In: Vehicular technology conference, 2008. VTC Spring 2008, Singapore. IEEE, pp 2800–2804
15. Grassi G, Pesavento D, Wang L, Pau G, Vuyyuru R, Wakikawa R, Zhang L (2013) Acm hotmobile 2013 poster: vehicular inter-networking via named data. ACM SIGMOBILE Mob Comput Commun Rev 17(3):23–24
16. Grassi G, Pesavento D, Pau G, Vuyyuru R, Wakikawa R, Zhang L (2014) VANET via named data networking. In: IEEE conference on computer communications workshops (INFOCOM WKSHPS), Toronto. IEEE, pp 410–415
17. Olariu S, Eltoweissy M, Younis M (2011) Towards autonomous vehicular clouds. EAI Endorsed ICST Trans Mob Commun Appl 11:e2
18. Bernstein D, Vidovic N, Modi S (2010) A cloud PAAS for high scale, function, and velocity mobile applications-with reference application as the fully connected car. In: Proceedings of the 2010 fifth international conference on systems and networks communications (ICSNC), Nice. IEEE Computer Society, pp 117–123
19. Son J, Eun H, Oh H, Kim S, Hussain R (2012) Rethinking vehicular communications: merging vanet with cloud computing. In: Proceedings of the 2012 IEEE 4th international conference on cloud computing technology and science (CloudCom), Taipei. IEEE Computer Society, pp 606–609
20. Yu R, Zhang Y, Gjessing S, Xia W, Yang K (2013) Toward cloud-based vehicular networks with efficient resource management. IEEE Netw 27:48–55

21. Lee E, Lee E-K, Gerla M, Oh S (2014) Vehicular cloud networking: architecture and design principles. IEEE Commun Mag 52:148–155
22. Nilsson DK, Larson UE (2008) Combining physical and digital evidence in vehicle environments. In: Third international workshop on systematic approaches to digital forensic engineering (SADFE'08), Berkeley. IEEE, pp 10–14
23. Nilsson DK, Larson UE (2008) 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, Adelaide
24. Yan G, Rawat D, Bista B (2012) Towards secure vehicular clouds. In: Sixth international conference on complex, intelligent and software intensive systems (CISIS), Palermo, pp 370–375
25. Plossl K, Nowey T, Mletzko C (2006) Towards a security architecture for vehicular adhoc networks. In: IEEE first international conference on availability, reliability and security (ARES), Vienna
26. Mejri MN, Ben-Othman J, Hamdi M (2014) Survey on VANET security challenges and possible cryptographic solutions. Veh Commun 1:53–66
27. Grover J, Gaur MS, Laxmi V (2013) Trust establishment techniques in VANET. In: Wireless network security, signals and communication technology. Springer, Berlin, pp 273–301
28. Group TTW et al (2013) The notorious nine: cloud computing top threats in 2013. In: Cloud security alliance, 2013, San Francisco
29. Kortchinsky K (2009) Cloudburst: A VMware guest to host escape story. In: Black Hat USA, Las Vegas
30. Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I et al (2010) A view of cloud computing. Commun ACM 53(4):50–58
31. Choubey R, Dubey R, Bhattacharjee J (2011) A survey on cloud computing security, challenges and threats. Int J Comput Sci Eng (IJCSE) 3(3):1227–1231
32. Kazim M, Zhu SY (2015) A survey on top security threats in cloud computing. Int J Adv Comput Sci Appl (IJACSA) 6(3):109–113
33. Zafar MS, Ahmad F (2014) A study on personalization and customization mechanisms of vehicular cloud platform. In: IEEE/ACM 7th international conference on utility and cloud computing (UCC), London, pp 812–817
34. Patel P, Ranabahu AH, Sheth AP (2009) Service level agreement in cloud computing. In: International conference on Object-Oriented Programming, Systems, Languages and Applications (OOPSLA), Orlando, USA
35. Whitney L (2009) Amazon EC2 cloud service hit by botnet, outage. CNET News, vol 11
36. Matthews JN, Dow EM, Deshane T, Hu W, Bongio J, Wilbur PF, Johnson B (2008) Running xen: a hands-on guide to the art of virtualization. Prentice Hall PTR, Upper Saddle River

Farhan Ahmad received his B.Sc. degree in Electronics Engineering at COMSATS Institute of Information Technology, Abbottabad, Pakistan, in 2009 and M.Sc. degree in Communication and Information Technology at University of Bremen, Germany, in 2014. He developed his M.Sc. thesis in the domain of M2M communication and LTE-Advanced Networks. He is currently pursuing his PhD studies at the College of Engineering and Technology, University of Derby, UK, where his current research focuses on security and trust in vehicular networks, mobile communications, and information centric networking.

Muhammad Kazim is a PhD student at the University of Derby, UK. His research area in PhD is cloud computing security. Before starting his PhD, he completed his masters degree in Computer and Communication Security from the National University of Sciences and Technology, Islamabad, Pakistan, in 2014. Earlier, he completed his bachelor's degree in Information and Communication Systems Engineering also from the National University of Sciences and Technology in 2011. Other research areas of his interest are computer networks, computer security, and communication systems.

Asma Adnane joined the University of Derby as a full-time senior lecturer in Networks and Security from the University of Leicester, where she was Knowledge Transfer Partnership associate with CrowdLab as their database and security expert. Asma has a PhD in Computer Science and has published several papers on ad hoc network security and trust management. She was aso a research associate/lecturer in France at the University of Rennes, University of Nantes, and ENSI-Bourges.