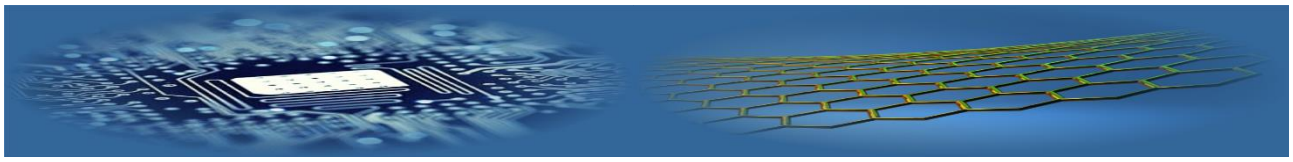


Security challenges of vehicular cloud computing applications: from software architecture viewpoint

Hanieh Kashfi*, Fereidoon Shams Aliee

Faculty of Computer Science and Engineering, Shahid Beheshti University, Tehran, Iran

**Corresponding author: Kashfi.hanieh@gmail.com*

Received 13 May 2017, www.cmnt.lv

Abstract

The use of vehicular ad-hoc network is considered by researchers in recent years. Although these networks have been deployed in real world offering appropriate services to their users, researches show that their current architecture have different development and management problems. It seems that cloud computing due to its scalability and other features is an appropriate technology to compensate the shortcomings. By moving the vehicular ad-hoc network to the cloud, we have the new technology of vehicular cloud network. Considering quality attribute is the best approach to improve the vehicular cloud network applications' software architecture. Among the quality attributes, security is so important and the lack of security in the system causes the rejection of these technologies by users. This paper studies vehicular cloud networking security. In order to achieve the security in vehicular cloud network applications, first of all a list of applications is prepared. Then applications are categorized to identify various security threats. To confront the existing threats, various security tactics are provided. Finally an approach to increase the security in vehicular cloud applications is proposed.

Keywords:

Vehicular cloud computing,
VANET,
Security,
Software Architecture

1 Introduction

In recent years due to the vast number of vehicles on the roads, researchers concentrate on the vehicular cloud network applications. Using tiny embedded sensors in vehicles, wireless communication models and computing and storage capabilities, the future generation of vehicles are moving toward more intelligence [1]. The sensors collect various information from their surroundings and share them with their neighbourhood vehicles through the vehicle to vehicle or vehicle to infrastructure connections [2]. To support the variety of such network applications, some of which require a lot of computing power and bandwidth, vehicles and road side units work together to share resources that make the temporary cloud. The combination of temporary cloud spaces with the common cloud results in network performance. This creates vehicular cloud networking [2].

Cloud networks faced different security challenges [4]. With the increase in the number of vehicles, regard to the use of thousands of different sensors in the vehicle, the security aspects are more important. Hostile attacks to the cloud infrastructure to prevent the vehicle from accessing the cloud or intercepting transmitted data are among the threats that affect these networks [5]. With the advent of ever-increasing applications in these networks, using software architecture tactics to design a secure software to transmit data among vehicles is a good strategy. Before using software architecture tactics, application classification and extracting their common features can help us to provide a security model for the applications.

We covered the following objectives in this paper:

- Vehicular cloud network applications classification.
- Reviewing the key features of applications in terms of security.
- Proposing new approaches in these networks to increase efficiency and improve security.

The remainder of the paper is organized as follows. In section 2 we describe an overview of related work. Section 3 presents the definitions and basic concepts of vehicular cloud networks. Section 4 offers the categorization of applications and some of their features related to the security. In section 5 different software architecture tactics to solve security problems are applied. Section 6 provides fog computing case study and finally section 7 concludes the article and presents future works.

2 Related work

In 2012 the first idea of an ad-hoc cloud network architecture was presented [6]. This study focuses on the architecture of vehicular ad-hoc network to develop a running cloud model. Authors of [1] investigate that how the vehicular ad-hoc network expanded with vehicular cloud and data-driven networks. Vehicular cloud combines the mobile cloud model with vehicular networks and then changes the network services delivery modes. On the other hand, data-driven networks change the method of data routing and its propagation. According to this, a new network system is created for vehicles that are behind each of these concepts. In fact this article examines the architecture and functionality of this phenomenon and the design principles is discussed. Recent studies have not considered the role of software architecture and quality attribute. In [7] Authors detects and analyses some of security challenges and potential threats for privacy in vehicular cloud. This study pointing out some of security

threats and providing a security plan, presents appropriate security architecture. This studies future work is about establishing a systematic way to implement intelligent transportation systems. The authors of [2] introduce the vehicular cloud network with the combination of three kinds of clouds which are 1) vehicular cloud 2) infrastructure cloud 3) Back-End cloud. In addition the importance of security, privacy and trust in the systems which are used in vehicular cloud networks is discussed. So the paper which describes the security in vehicular cloud network, Investigated various threats relates to every layer of vehicular cloud network. No attention is paid to the security needs in available vehicular cloud network applications.

This study provides a list of vehicular cloud network applications and their potential threats and uses the software architecture to realize the security quality attribute in vehicular cloud networks.

3 Vehicular cloud networks

Vehicular ad-hoc network is responsible for communication between vehicles. A vehicle can communicate and exchange information with its peer (V2V - Vehicle to vehicle communication) or with the infrastructure like RSU - Road Side Unit (V2I - Vehicle to Infrastructure) [1]. With the advent of cloud computing concepts, computing, communication and data storage resources are provided as services. Vehicular cloud network is formed with the combination of cloud computing and vehicular ad-hoc networks. According to various applications of vehicular ad-hoc networks and cloud computing, there will be so many applications to develop with the combination of these two technologies [2].

Software architecture has a great affect in designing and developing vehicular cloud network applications. In software architecture in addition to the functionality, quality attribute like performance, availability, security, usability and etc. must be taken to the account. One of the most important quality attribute of the vehicular cloud networks is security. In this part, first we introduce architecture of the vehicular cloud networks and various applications and then security threats associated with these networks are discussed.

3.1 VEHICULAR CLOUD NETWORK ARCHITECTURE

Vehicles and sensors in an area produce different content and data. These data is stored and searched in cloud and is processed and used by the neighbours in the lifetime [8]. Figure 1 shows the architecture of vehicular cloud networks. According to figure 1, three main concepts of the vehicular cloud networks are vehicles, communication and the cloud.

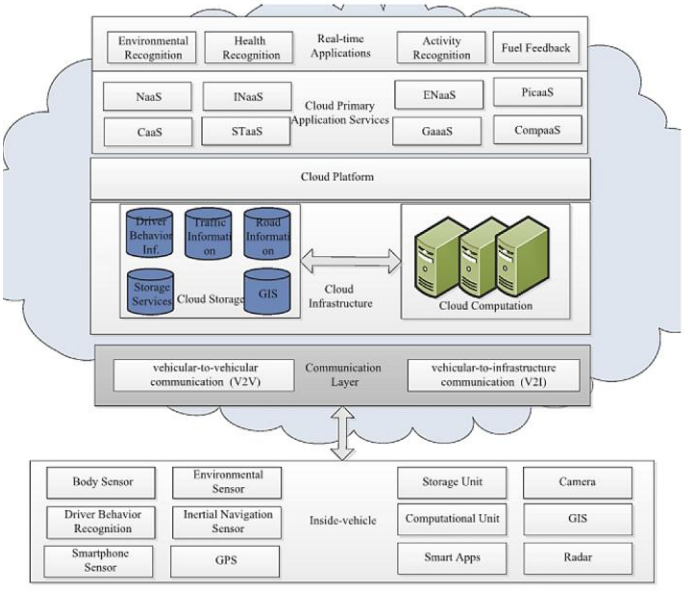


FIGURE 1 Vehicular cloud network architecture [8]

3.2 VEHICULAR CLOUD NETWORK APPLICATIONS

Since different vehicles and RSUs share their resources thorough common cloud, vehicular cloud networks offer a wide range of applications. Some of these applications include [3, 5]:

- Vehicle maintenance: Vehicles can get their software updates from the cloud whenever the developer releases a new version.
- Traffic management: Drivers can get the traffic reports from the vehicular cloud.
- Sharing road condition: You can share road condition such as floods or icy road in the vehicular cloud. According to this drivers will be warned about dangerous conditions in their chosen routes.
- Accident warnings at intersections: In certain driving conditions such as fog, severe storms, snow and etc. drivers can use this service if they want to be alerted about potential accidents. A high-rise building with radars that should cover all intersections at specified intervals can be used as an infrastructure for this service. To predict the likelihood of accidents, using an intelligent algorithm is inevitable.
- Security applications: Applications related to critical scenarios in life like collision avoidance need strong security protection.
- Intelligent parking management: Vehicles using vehicular cloud networks will be able to reserve a

place in parking lots for themselves. All parking's information will be accessible in the cloud without central control.

- Planned evacuation of residents: In some natural disasters such as hurricanes and tsunamis, clouds vehicles can be used as a tool to organize evacuation.

3.3 VEHICULAR CLOUD NETWORK APPLICATION SECURITY THREATS

Vehicular cloud networks security threats according to the classification in [9] are:

- Spoofing User Identity: Attackers pretend to be another user to obtain illegal information and benefits. A classic example of this attack "man in the middle" in which attackers pretend to be Alice when communicating with Bob and vice versa. As a result, both Bob and Alice send decrypted messages to their attackers.
- Tampering: In this type of attack, the attacker modifies data or creates his/her own data.
- Repudiation: Attacker try to impersonate new data or manipulate data, activity and operation.
- Information Disclosure: In this threat, attackers try to discover and disclosure of identifying information such as identity, legal, finance, politics, accommodation and biological traits and racial and geographic data records involved.
- Denial of service attack: The invaders poured out their attacks as a large number of questions toward the running system. As a result, the system resources for the users will be inaccessible.
- Elevation of Privilege: in this threat, attackers exploit a defect in the system, system leaks, design flaw or error in the configuration of the operating system or software application to illegally raise the privileges and accessibilities to the protected resources and data.

According to the security triangle [10] confidentiality, integrity and availability, a classification for existing threats is presented in figure 2.

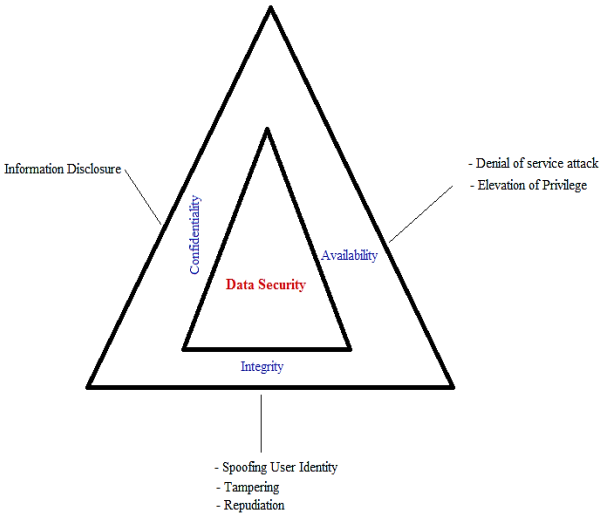


FIGURE 2 Vehicular cloud networks security threats

4 Vehicular cloud networks application security

Due to the advances of the vehicular cloud networks, the number of applications in this field will grow. Investigating the existing software and applications, determines the role of the software architecture to meet the expectations of quality attributes. Therefore noticing applications and their security threats is necessary to provide the appropriate tactics for security in software architecture [11]. In this study, vehicular cloud network applications are classified according to their type of usage. This categorization is presented in Table 1. Some other columns like data importance, related units in the application, delay sensitivity and propagation type are added to better introduce the applications. In Table 2 Each group of applications are related to the threats type and suggested tactics using Table 1.

TABLE 1 Characteristics of vehicular cloud applications

Application type	Application	Associated units	Data importance	Delay sensitivity	Casting type
Safety	Accident alert	V2I V2V	Public	Delay-sensitive	Broadcast
	Security threat alert	V2I	Public	Delay-sensitive	Geocast
	danger on the road alert	V2I V2V	Public	Delay-sensitive	Broadcast
	scope of work and repair alert	V2I V2V	Public	Delay-sensitive	Broadcast
Management	Bandwidth Management	V2BEC*	Public	Insensitive to delay	Multicast
	Remote traffic management	V2I	Public	Delay-sensitive	Broadcast
	Intelligent Parking Management	V2I	Public	Insensitive to delay	Unicast
Controlling	Visual control of urban areas	V2I	Public	Insensitive to delay	Geocast
	Control of drains in times of crisis and natural disasters	V2I	Public	Delay-sensitive	Geocast
	Congestion Control	V2I	Public	Delay-sensitive	Broadcast
Business	commercials	V2I	Public	Insensitive to delay	Broadcast
Infotainment	Multimedia file sharing	V2V	Private	Delay-sensitive	Unicast
Public Services	Highway information	V2I	Public	Insensitive to delay	Broadcast
	Emergency passing vehicles alert	V2V	Public	Delay-sensitive	Broadcast
	Road condition sharing	V2V V2I	Public	Delay-sensitive	Broadcast
	Vehicle maintenance	V2I	Public	Insensitive to delay	Multicast
	Vehicle and traffic real time tracking	V2I	Private	Delay-sensitive	Unicast

*Back-End Cloud

5 Proposed approach

In all the considered applications in Table 1 delay sensitivity factor is studied. Looking to the values of this column, we can understand that some of vehicular cloud network applications are time sensitive and this means that if they do not be effective in a certain time, they won't be effective any more. Considering the relationship between vehicular cloud network and human life and health, the concept of time sensitivity becomes clearer. It seems offering an approach to solve the delay problem in this technology is essential. Vehicular cloud networks application as a security tool in this technology is one of the most important benefits of vehicular cloud networks. It is obvious that most of these applications are delay sensitive. In scheduling security attacks, malicious vehicle receives messages but before sending the message to the others, adds an amount of time to the original message to cause a delay. Of course, the way of eliminating the possibility of time adding in the messages is maintaining data integrity. However, if the delay is due to infrastructural issues, the possibility of this should be minimized. Fog computing is a new technology that provides delay sensitive services to meet the needs of delay-sensitive scenarios. Fog computing called distributed computing concepts that expands the services that are provided by the cloud to the network edge. In addition, fog computing supports mobility of the computing resources, communication protocols, cloud integration and distributed data analysis, which is associated with lower delay. Due to the characteristic of the fog computing, it seems that using it in the vehicular cloud network systems to reduce delay and increase security would be an appropriate approach.

6 Case study: intelligent traffic lights and connected vehicles

Cameras at intersections seeing ambulance lights can change traffic lights automatically and open the road for ambulance. Using the common cloud, information is expected to be transferred to the central cloud infrastructure and then the result of changing the colour of traffic light would be applied [12]. On the other hand if a cyclist or pedestrian is detected by sensors in intersections or near the traffic lights, it is possible to measure the speed and distance of approaching vehicles and changes the colour of smart light. In this case, time is an important factor. Transferring all of this information to the cloud (as well as information on neighbourhood traffic lights) will cause delay. This distance may create vulnerability so the hostile person can cause traffic lights inappropriate performance by adding a small delay. On the other hand if information transmission is multi hop and with the help of other vehicles, the risk of delay would be more, because of the hostile vehicle. In this scenario, fog computing can greatly reduce the vulnerability and minimize the additional delays on the path. Fog can extend the services provided by the cloud to the edge of the network. Hence, we can reduce transmission delays and even moderate multi hop transmission by using fog computing. The important difference between cloud and fog that causes delay reduction and limits the hostile access are summarized in Table 3 [13].

TABLE 2 Threats and tactics to solve vehicular cloud application Security

Application type	Threats	Security dimension	Solution (Tactics)
Safety	- Tampering - Repudiation	- Integrity	- Maintain integrity - Authenticate users
Management	- Tampering - Repudiation - Denial of service attack - Elevation of Privilege - Spoofing User Identity	- Integrity -Availability	- Maintain integrity - Authenticate users - Authorize users - Limit exposure - Limit access
Controlling	- Denial of service attack - Elevation of Privilege - Spoofing User Identity - Information Disclosure	- Integrity - Availability - Confidentiality	- Maintain integrity - Authenticate users - Authorize users - Limit exposure - Limit access - Maintain data confidentiality
Business	- Tampering - Repudiation - Elevation of Privilege - Spoofing User Identity	- Integrity -Availability	- Maintain integrity - Authenticate users - Authorize users - Limit exposure - Limit access
Infotainment	- Tampering - Repudiation - Denial of service attack - Information Disclosure - Spoofing User Identity	- Integrity - Availability - Confidentiality	- Maintain integrity - Authenticate users - Authorize users - Limit exposure - Limit access - Maintain data confidentiality
Public Services	- Tampering - Repudiation - Denial of service attack - Information Disclosure	- Integrity - Availability - Confidentiality	- Maintain integrity - Authenticate users - Authorize users - Limit exposure

TABLE 3 Difference between cloud and fog computing [13]

Requirement	Cloud Computing	Fog Computing
Latency	High	Low
Delay Jitter	High	Very low
Location of server nodes	Within the internet	At the edge of the local network
Distance between the client and the server	Multiple hops	One hop
Security	Undefined	Can be defined

7 Conclusions

The importance of the security quality attribute in vehicular cloud network due to important applications is clear. In this article we examined the security quality attribute in vehicular cloud networks, from the perspective of software architecture. Security requirement of each application with their features is extracted. By providing different categorization for application and threats, a mapping between threats and usable software architecture tactics is achieved. Finally an approach to improve security in vehicular cloud networks is proposed.

As a future work, Table 1 and Table 2 provide an overview to offer a security model or framework for vehicular cloud networks. This model can be developed by studying information and data security reference model and customizing it for vehicular cloud networks.

References

[1] Grassi F, Pesavento D, Pau G, Vuyyuru R, Wakikawa R, Zhang L 2014 VANET via Named Data Networking *IEEE Conference on Computer communications Workshops (INFOCOM WKSHPS)* 410–5

[2] Ahmad F, Kazim M, Adnane A, Awad A 2015 Vehicular Cloud Networks: Architecture, Applications and Security Issues *IEEE/ACM 8th International Conference on Utility and Cloud Computing* 571-6

[3] Whaiduzzaman M, Sookhak M, Gani A, Buyya R 2014 A Survey on Vehicular Cloud Computing *Journal of Networks and Computer Applications* **40** 325–44

[4] Brodkin J 2008 *Gartner: Seven cloud-computing security risks* http://www.networkworld.com/news/2008/070208-cloud.html

[5] Lee E., Lee EK, Gerla M, Oh S 2014 Vehicular Cloud Networking: Architecture and Design Principles *IEEE Communications Magazine* **52** 148–55

[6] Al Mamun, MA, et al. 2012 Deployment of Cloud Computing into VANET to Create Ad Hoc Cloud Network Architecture *Proceedings of the World Congress on Engineering and Computer Science* **1**

[7] Yan G, Wen D, Olariu S, Weigle M 2013 Security challenges in vehicular cloud computing *IEEE Trans. Intell. Transp. Syst* **14**(1)

[8] Muhammad K, Soyturk M, Avcil M, Kantarci B, Matthews J 2016 From Vehicular Networks to Vehicular Clouds in Smart Cities *Smart Cities and Homes: Key Enabling Technologies Elsevier* 149-71

[9] *Microsoft The stride threat model* https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

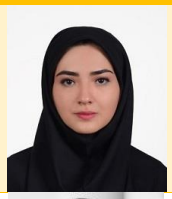
[10] *Confidentiality, Integrity & Availability* http://ishandbook.bsewall.com/risk/Methodology/CIA.html

[11] Bass L, Clements P, Kazman R 2003 Software Architecture in Practice *Addison-Wesley Longman Publishing Co., Inc., Boston, MA*

[12] Stojmenovic I, Sheng W 2014 The fog computing paradigm: Scenarios and security issues *IEEE Federated Conference on Computer Science and Information Systems (FedCSIS*)

[13] More P 2015 Review of Implementing Fog Computing *International Journal of Research in Engineering and Technology* **4** 335-8

AUTHORS



Hanieh Kashfi, Tabriz, Iran

Current position, grades: MSc Student at Computer Science and Engineering Faculty, Shahid Beheshti University, Tehran, Iran
University studies: Information Technology
Scientific interest: Internet of Things, Software Architecture, Enterprise Architecture, Cloud Computing
Experience: She is working in ISA Lab

Fereidoon Shams Aliee, Tehran,Iran

Current position, grades: Associate professor at Computer Science and Engineering Faculty, Shahid Beheshti University, Tehran, Iran
University studies: Software Engineering
Scientific interest: Software Architecture, Enterprise Architecture, Service Oriented Architecture, Agile Methodologies, Ultra-Large-Scale (ULS) Systems and Ontological Engineering
Experience: He is heading two research groups namely ASER (Automated Software Engineering Research) (aser.sbu.ac.ir) and ISA (Information Systems Architecture) (isa.sbu.ac.ir) at Shahid Beheshti University