Security of vehicular cloud computing: A very short review

Junyi Deng, Yanheng Liu, and Jian Wang
College of Computer Science and Technology
Jilin University
Changchun, China
djy_jimmy@126.com, {yhliu, wangjian591}@jlu.edu.cn

Lin Li
School of computer and information technology
Shanxi University
Taiyuan, China
lilynn1116@sxu.edu.cn

***Abstract*—Since the rapid development of the vehicular networking and cloud computing, a new-type hybrid cloud, Vehicular Cloud Computing (VCC), has emerged. However, the new emerging security and privacy issues need to be addressed prior to a widespread deployment. This paper characterizes VCC in an overall framework, and categorizes VCC into static, dynamic and hybrid in terms of the applicable scenario. We simply analyze the security and privacy challenges of VCC underlying each layer and each type. Some feasible solutions to the focused security issues are designed and proposed for an applicable implementation of VCC. Finally, we provide several promising open topics.**

Keywords—ANET, Cloud Computing, Vehicular Cloud Computing, Vehicular Cloud Architecture, Security, Privacy

I. INTRODUCTION

The manufacturers, drivers and researchers always expect that Vehicular Ad-Hoc Network (VANET) [1-4] can provide more useful and practical services, for instance, computing, storage, online infotainment and secure traffic control. But these expectations are hard to achieve because the vehicles' high mobility, poor computation and storage capacity, and the high cost of the mobile Internet service in VANET [5, 6].

As a consequence, Mobile Cloud Computing (MCC) [7, 8] is becoming increasingly important and will affect the structure and future of VANET [9]. When vehicles are equipped with the embedded processors, the storage devices, and the multi-modal programmable sensors, they will possess computing, storage, communication and sensing capabilities so that they could be organized into the new-style Vehicular Cloud Computing (VCC) [10-15] networks. VCC is a hybrid technology that combines VANET with MCC, which integrates large amounts of on-board resources into a huge resource pooling that provides almost unlimited compute, storage and network capability for the moving vehicles by using virtualization technology.

Though there are so many advantages about VCC, the public are still reluctant to accept it mainly due to the numerous security problems and challenges are unsolved at present [16-23]. Because it is still an urgent need to solve the security and privacy issues of VANET and CC, the security of VCC is more complicated [24-29]. In addition, the diversified development of mobile communication technologies also make the information security of VCC become the urgent issues to be addressed [30].

There are several important unsolved security issues of VCC as follow.

(1) VCC has diverse application scenarios that have the different security features in each one.

(2) There is not a standard architecture of VCC as yet. But an appropriate architecture is the basis for security and privacy protection.

(3) There are abundant new security issues in every layer of VCC architecture, which are related to VANET or CC, but the corresponding solutions and strategies are not standardized and deficient.

Therefore, in this paper, we firstly divide VCC into three categories: static VCC, dynamic VCC and hybrid VCC. Then combining with the scene classification, a complete architecture of VCC is introduced, which includes inside-vehicle layer, vehicle communication layer and vehicle cloud layer.

II. APPLICATION SCENES AND ARCHITECTURE OF VCC

A. Application Scenes of VCC

At present, vehicles has already more and more connect with people's work and life. No matter they are moving or parking, the public consider them can integrate an enormous resource pool that could provide the various services for the drivers. Therefore, according to the applicable scenarios of vehicles in the real world, we can categorize VCC into three types: static VCC, dynamic VCC and hybrid VCC. They are shown in Fig. 1.

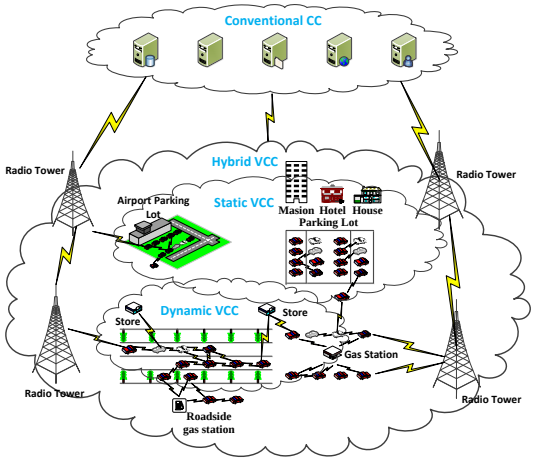

Fig. 1. Three types of VCC in the real world

B. Architecture of VCC

CC has become more prevalent in recent years, but there is not a standard architecture of it so far. Combining with the application scenes of VCC, we will introduce a complete architecture of VCC before discussing the security and privacy. It can be broken down into three layers: Inside-Vehicle Layer, Vehicle Communication Layer and Vehicle Cloud Layer, as shown in Fig. 2.

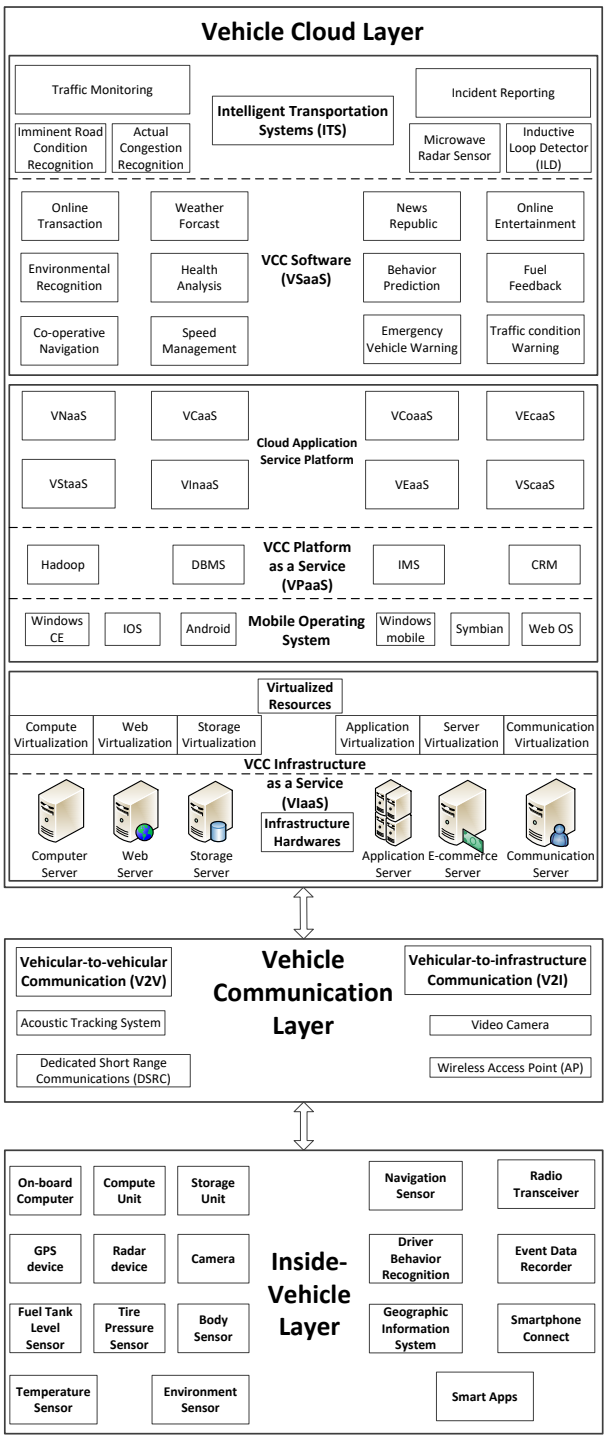

Fig. 2. The Architecture of Vehicular Cloud Computing

III. Security of Vehicle Communication Layer

After the information gathered by OBUs, they must be exchanged with others or transmitted to the vehicle cloud. This must rely on the vehicle communication layer. It will bring a great influence on the VCC security in case they are tampered during transmission, because other vehicles and the vehicle cloud are hard to judge the validity of information. Therefore, the Security of Vehicle Communication Layer is the most vulnerable portion in VCC security. The communication security and the information security are two most important issues. And that the communication security is the basic of the information security. It focuses on the security of communication channel but not involves with the data information, just provides physical security for the information validity.

In the following, we will discuss both of them in details, and the corresponding solutions and strategies to the every threat will be put forward.

A. The Communication Security

In VCC, all of vehicles and road-side infrastructures can communicate with each other by the aid of V2V and V2I channel. And that they can also contact with the vehicle cloud to share information so that VCC can provide various services for the safe and efficient driving. But it is precisely because of this several security attacks that aim to the communication of VCC at present.

All of the information in VCC are transmitted in the form of messages that are constructed from several fields. The structure of message is shown as Fig. 3.

Fig. 3. The Structure of Message

And the type of message can be divided into four kinds, as shown in Table I.

TABLE I. FOUR TYPES OF VCC MESSAGE

Name	Description
Acknowledge message	To confirm that the drivers join/leave VCC or the messages have been sent successfully.
Media message	To get the services from other vehicles or the cloud providers.
Priority message	To send/cancel the alert messages or urgent messages.
Short message	To send the alert messages or warning messages.

B. The Information Security

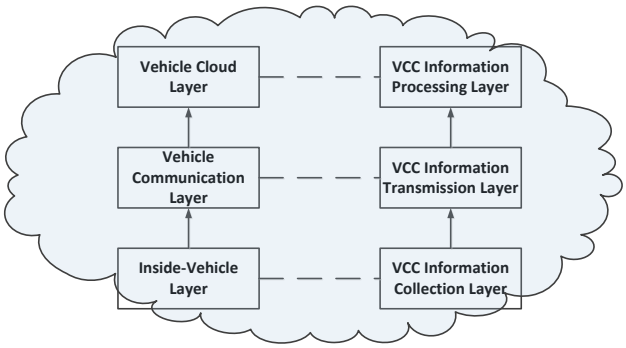

Fig. 4. The network structure of VCC

The network structure of VCC is already divided into

Inside-Vehicle Layer, Vehicle Communication Layer and Vehicle Cloud Layer. However, relative to the information of VCC network, they are Information Collection Layer, Information transmission Layer and Information processing Layer, as shown in Fig. 4.

IV. Security of Vehicle Cloud Layer

In this section, we will respectively discuss the security of three types of VCC and the security of VCC provider.

A. The Security of three types of VCC

1) Static VCC Security: In the past, the resources of parked vehicles are unexploited and wasted. But in fact, these vehicles are the best candidate resource nodes because they can contribute their own computing and storage resources to form a static VCC which is a large computing entity similar to the conventional CC [31]. Therefore, the researchers are paying more and more attention to the static vehicles so that they have become an important part of VCC, namely the static VCC.

2) Dynamic VCC Security: The biggest difference between VCC and the conventional cloud is mobility. In present, there are a large number of vehicles that spent the substantial amounts of time in the various dynamic scenes, for instance, driving on the road, being stuck in the traffic jam, even involving in a traffic accident, and so on. The vehicles in these scenes constitute the dynamic VCC. The independent structure of dynamic VCC is shown as Fig. 5.

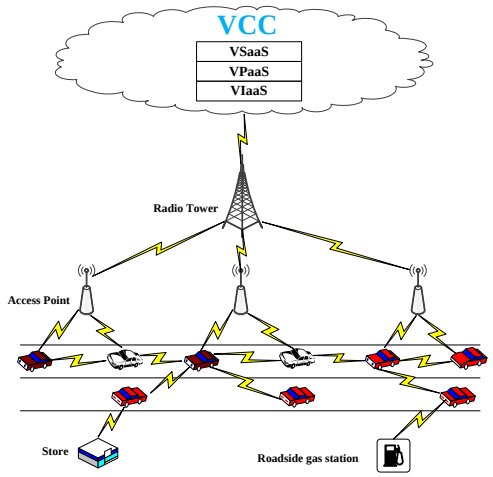

Fig. 5. The structure of Dynamic VCC

3) Hybrid VCC Security: In the real world, the whole VCC is an immense hybrid VCC. The security of it is the most complicated, including all characteristics of the static VCC and dynamic VCC.

B. Secure VCC Provider

The security of VCC provider is a vital part of the security of VCC. There are three steps to verify the providers.

(1) The VCC providers must have the appropriate levels of security assurance and post this information on the Security, Trust, and Assurance Registry (STAR).

(2) Utilizing the Consensus Assessment Initiative Questionnaire (CAIQ) and Cloud Controls Matrix (CCM) provided for free by the Cloud Security Alliance (CSA) [32]. They offer boilerplate questions established by hundreds of security professionals around the world, which provide a solid foundation for assessing the risk models and controls of a cloud provider.

V. Open Issues and Research Challenges in VCC

The mobility of VCC, the self-organization and the diversity of services make the security of VCC face with serious challenge. Although we have discussed almost all of the security problems and the relevant solutions in the previous sections, there are several important open issues and research challenges that need to delve into in the future.

A. Framework Design of VCC

VCC is a complex entity that must be optimized continually so that it can integrate all kinds of resources and services preferably. But there is not an acknowledged security framework design of VCC. Thus, the framework of VCC is still needed to perfect.

B. Security Strategy of VCC

The issues of security and privacy are the important aspects for the establishing and maintaining the trust of users to VCC. Security demands that VCC can protect the user data against the various threats. Privacy requires that the user information is isolated and transmitted in the trustworthy environment. We have summarized all kinds of security solutions in the previous sections, but many of them are not designed for VCC specially. The primary security challenges and the corresponding strategies of VCC are still needed to research.

(1) Identity authentication and authorization of users.

(2) The confidentiality and integrity of information.

(3) The security of the mobile distributed VCC storage.

(4) The security and veracity of the vehicle locations.

(5) The heterogeneity of VCC network.

C. Management Policy of VCC

The rules and the regulations of VCC must be established to operate effectively the decision system, control system and management, which must the authorities and VCC providers participate. There are some factors needed to consider.

(1) Assurance of trust management. In some situations, the VCC may require to have authority to take local action instead of a central authority. For example, when the vehicles involves a traffic jam, for rescheduling the traffic lights, a cooperation between the cloud formation and municipal or county authority needs to promote the rapid dissipation of congestion. Hence, the existence of a trust management in VCC can be useful for automated verification of actions.

(2) Essential functioning policies. Effective operational policies are needed for seamless inter-operation, decision support, establishing accountability metrics, standardization, regulations, and even local and national policy making.

(3) Federation of different clouds. In the near future, several types of clouds will emerge such as the VCC-car cloud, sensor cloud, Smartphones cloud, all clouds must interact with each other and the securities of them are protected. Hence the interoperability of different types of clouds, connection, synchronization, and reliability and security should be addressed.

VI. Conclusions and Future Expectations

VCC emerges from the convergence of powerful implanted vehicle resources, advances in network mobility and cloud computing. The combination of a massive amount of unutilized resources on board vehicles, such as internet connectivity, storage and computing power, can be rented or shared with various customers over the internet, similar to the usual cloud resources. Several of these resources can dynamically provide us support for alleviating traffic incidents and emergencies. VCCs can lead to a significant enhancement in terms of safety, security and economic viability of our society. But the issues of security and privacy hinder the development of VCC and the acceptation by the people.

In the paper, we present a comprehensive structure of VCC. The taxonomy, application scenarios, security and privacy issues and the relevant strategies of VCCs also have been proposed and discussed. However, abundant security areas of VCC still remain unexplored by researchers including: the unified security framework of VCC, security and privacy of data sharing, unstable communication links, physical location attacks, and the synchronization of VCC federation.

A series of subsequent researches are required to create the unified security structure of VCC and the corresponding strategies for meeting the security and privacy challenges. Hence, we need a concerted effort among industry and academia and the close cooperation of the auto industry and the government. The following work is solving the unresolved problems including designing the special communication protocols, enhancing the security strategies and formulating the management policies for VCC.

Acknowledgment

This work is supported in part by the National Natural Science Foundation of China (Grant No. 61373123), and in part by the Jilin Province Science and Technology Development Plan (Key Science and Technology Tackling) Project (Grant No. 20160204041GX).

References

[1] Zeadally S., Hunt R., Chen Y., Irwin A., and Hassan A.: 'Vehicular ad hoc networks (VANETS): status, results, and challenges', Telecommunication Systems, August 2012, Volume 50, (Issue 4), pp. pp 217-241

[2] Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H., and Zedan, H.: 'A comprehensive survey on vehicular Ad Hoc network', Journal of Network and Computer Applications, 2014, 37, (0), pp. 380-392

[3] Hartenstein, H., and Laberteaux, K.P.: 'A tutorial survey on vehicular ad hoc networks', Communications Magazine, IEEE, 2008, 46, (6), pp. 164-171

[4] Yue, L., Jun, B., and Ju, Y.: 'Research on Vehicular Ad Hoc Networks', in Editor (Ed.)^(Eds.): 'Book Research on Vehicular Ad Hoc Networks' (2009, edn.), pp. 4430-4435

[5] Akbari Torkestani, J.: 'Mobility prediction in mobile wireless networks', Journal of Network and Computer Applications, 2012, 35, (5), pp. 1633-1645

[6] Yang, Q., Dijiang, H., and Xinwen, Z.: 'VehiCloud: Cloud Computing Facilitating Routing in Vehicular Networks', in Editor (Ed.)^(Eds.): 'Book VehiCloud: Cloud Computing Facilitating Routing in Vehicular Networks' (2012, edn.), pp. 1438-1445

[7] Anirban, M.: 'High-Performance Mobile Internet', in Editor (Ed.)^(Eds.): 'Book High-Performance Mobile Internet' (2014, edn.), pp. 8-11

[8] Xu, Q., Segupta, R., Jiang, D., and Chrysler, D.: 'Design and analysis of highway safety communication protocol in 5.9 GHz dedicated short range communication spectrum', in Editor (Ed.)^(Eds.): 'Book Design and analysis of highway safety communication protocol in 5.9 GHz dedicated short range communication spectrum' (IEEE, 2003, edn.), pp. 2451-2455

[9] Bazzi, A., and Masini, B.M.: 'Taking advantage of V2V communications for traffic management', in Editor (Ed.)^(Eds.): 'Book Taking advantage of V2V communications for traffic management' (IEEE, 2011, edn.), pp. 504-509

[10] Olariu, S., Khalil, I., and Abuelela, M.: 'Taking VANET to the clouds', In Proceedings of Int. J. Pervasive Computing and Communications, 2011, pp. 7-21

[11] Olariu, S., and Weigle, M.C.: 'Vehicular networks: from theory to practice' (CRC Press, 2010. 2010)

[12] Olariu, S., Hristov, T., and Yan, G.: 'The next paradigm shift: from vehicular networks to vehicular clouds', Basagni, S. and Conti, M. and Giordano, S. Stojmenovic, I),(Eds), Mobile Ad hoc networking: the cutting edge directions, Wiley and Sons, New York, 2012

[13] Hossain, M.A.: 'A survey on sensor-cloud: Architecture, applications, and approaches', International Journal of Distributed Sensor Networks, 2013, 2013

[14] Gerla, M.: 'Vehicular Cloud Computing', in Editor (Ed.)^(Eds.): 'Book Vehicular Cloud Computing' (2012, edn.), pp. 152-155

[15] Son, J., Eun, H., Oh, H., Kim, S., and Hussain, R.: 'Rethinking Vehicular Communications: Merging VANET with cloud computing'. Proc. Proceedings of the 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom)2012 pp. Pages

[16] Takabi, H., Joshi, J.B.D., and Ahn, G.J.: 'Security and Privacy Challenges in Cloud Computing Environments', IEEE Secur. Priv., 2010, 8, (6), pp. 24-31

[17] Kaufman, L.M.: 'Data Security in the World of Cloud Computing', IEEE Secur. Priv., 2009, 7, (4), pp. 61-64

[18] Zissis, D., and Lekkas, D.: 'Addressing cloud computing security issues', Futur. Gener. Comp. Syst., 2012, 28, (3), pp. 583-592

[19] Kandukuri, B.R., Paturi, V.R., Rakshit, A., and Ieee: 'Cloud Security Issues' (Ieee, 2009. 2009)

[20] Hashizume, K., Rosado, D., Fernández-Medina, E., and Fernandez, E.: 'An analysis of security issues for cloud computing', J Internet Serv Appl, 2013, 4, (1), pp. 1-13

[21] Behl, A., and Behl, K.: 'An analysis of cloud computing security issues', in Editor (Ed.)^(Eds.): 'Book An analysis of cloud computing security issues' (2012, edn.), pp. 109-114

[22] Duncan, A., Creese, S., and Goldsmith, M.: 'An overview of insider attacks in cloud computing', Concurrency and Computation: Practice and Experience, 2014, pp. n/a-n/a

[23] Polze, A., and Tröger, P.: 'Trends and challenges in operating systems—from parallel computing to cloud computing', Concurrency and Computation: Practice and Experience, 2012, 24, (7), pp. 676-686

[24] Subashini, S., and Kavitha, V.: 'A survey on security issues in service delivery models of cloud computing', Journal of Network and Computer Applications, 2011, 34, (1), pp. 1-11

[25] Sood, S.K.: 'A combined approach to ensure data security in cloud computing', Journal of Network and Computer Applications, 2012, 35, (6), pp. 1831-1838

[26] Waqar, A., Raza, A., Abbas, H., and Khurram Khan, M.: 'A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata', Journal of Network and Computer Applications, 2013, 36, (1), pp. 235-248

[27] Wang, C., Ren, K., Lou, W.J., and Li, J.: 'Toward Publicly Auditable Secure Cloud Data Storage Services', IEEE Netw., 2010, 24, (4), pp. 19-24

[28] Wang, Q.A., Wang, C., Ren, K., Lou, W.J., and Li, J.: 'Enabling Public Auditability and Data Dynamics for Storage Security in Cloud

Computing', IEEE Trans. Parallel Distrib. Syst., 2011, 22, (5), pp. 847-859

[29] Arshad, J., Townend, P., and Xu, J.: 'A novel intrusion severity analysis approach for Clouds', Future Generation Computer Systems, 2013, 29, (1), pp. 416-428

[30] Fonseca, A., and Vazão, T.: 'Applicability of position-based routing for VANET in highways and urban environment', Journal of Network and Computer Applications, 2013, 36, (3), pp. 961-973

[31] Arif, S., Olariu, S., Jin, W., Gongjun, Y., Weiming, Y., and Khalil, I.: 'Datacenter at the Airport: Reasoning about Time-Dependent Parking Lot Occupancy', Parallel and Distributed Systems, IEEE Transactions on, 2012, 23, (11), pp. 2067-2080

[32] Kelley, D.: 'Understanding the CSA Cloud Controls Matrix and CAIQ', http://searchcloudsecurity.techtarget.com/feature/Understanding-the-CSA-Cloud-Controls-Matrix-and-CAIQ, 2014