Security Challenges Addressed in Vehicular cloud computing

Ms. RajbhojSupriya K.
ME Computer Dept, SPCOE
Otur,India

Dr..S.V.Gumaste
ProfesorDept, Computer SPCOE
Otur,India

***Abstract*—In a series of recent papers, Prof. Olariu and his co-workers have supported the vision of vehicular clouds (VCs), a nontrivial lee way, along several dimensions, of conventional cloud computing. In a VC, underutilized vehicular resources including Computing control, stowage, and Internet connectivity canbe shared between users out over the Internet to various customers. Noticeably, if the VC concept is to see a extensive Assumption and to have significant common impact, security and privacy issues need to be addressed. The main contribution of this work is to categorize and evaluate a number of security challenges and potential privacy threats in VCs. Although security issues have received attention in cloud computing and vehicular networks, we identify security challenges that are specific to VCs, e.g., challenges of authentication of high-mobility vehicles, scalability and single interface, tangled identities and locations, and the complexity of establishing trust relationships among multiple players caused by Irregular short-range communications. Moreover, we provide a security organization that addresses several of the challenges discussed.**

***Index Terms*—Challenge analysis, cloud computing, privacy, security, vehicular cloud.**

I. INTRODUCTION

Enterprises are regularly searching for a new and improvement method to increase their earnings and reduce their costs. Those creativities need different technologies that let them grow and do not strain them financially. From the current technologies, Cloud computing has emerged as a promising solution providing on demand access to effective computing resources, platforms, and applications in a pay-as-you-go manner. Cloud service customers can use what they require and pay only for what they use. As a result of this, Cloud computing has raised the delivery of IT services to a new level that brings the comfort of traditional benefits such as water and electricity to its users. There are various advantages of Cloud computing, such as cost usefulness, scalability, and simplicity of management, encourage more and more companies and service providers to adapt it and over their solutions via Cloud computing models.Vehicularcloud computing also increases its popularity. People use Laptops and other
mobile devices to access the services of cloud. So the security problem increases and the data does not remain safe the attacker attacks the data and missuse it. So to Investigate the brand-new area and design solutions for each individual challenge namely for Authentication, Authorization, truth relationship,scalability etc.

II. CONCEPTUAL OVERVIEW OF VEHICULAR CLOUDS

1. Cloud computing

Clouds provide three types of services namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS Clouds offer computing resources such as processing power, storage, networks, and other fundamental computing resources. The underlying Cloud infrastructure is managed by a provider. However, users have the flexibility to select their virtual machine images and to deploy these applications. In the PaaS model, providers supply clients with tools and services to develop software applications. In addition to the IaaS restrictions, PaaS users do not have the ability to manage or control their virtual machine images and servers. SaaS providers allow customers to use the applications such as web based email, calendar or word editor running on a Cloud infrastructure. Neither the infrastructure nor the application are controlled by users in this model.

2. Vehicular cloud

Similar to VANETs, there are two types of VCs.In the first type called *Infrastructure-based VC*, users will
be able to access services by network communications involvingthe roadside infrastructure. In the second type called*Autonomous VC* (AVC), users can be organized on-theflyto form VC in support of emergencies and other ad hocevents. VCs

ISSN: 2278 – 7798

provide services at three levels, i.e., application, platform,and infrastructure. Service providers use the levels differentlybased on what and how the services are offered. VCs provide a cost-efficient way to offer comprehensiveservices. For example, a cheaper vehicle with network accesscan access a Virtual Machine with strong computation, communication,sensing capability, and large storage. Many applications such astraffic news, road conditions, or intelligent navigation systemscan be provided by a Virtual Machine.

III. SECURITY CHALLENGES

1. Authentication

Security authentication in the VC includes verifying useridentity and message integrity. To conduct authentication, thereare some metrics that can be adopted.

1) Ownership: A user owns some unique identity (e.g.,identity card, security token, and software token).

2) Knowledge: A user knows some unique things [e.g.,passwords, personal identification number and humanchallenge response (i.e., security questions)].

3) Biometrics: These include the signature, face, voice, and fingerprint.However, it is challenging to authenticate vehicles due tohigh mobility. First, high mobility makes it hard to authenticatemessages with a location context.

2. Scalability

Security schemes for VCs must be scalable to handle aDynamically changing number of users. Security schemesmust handle not only regular traffic but special traffic as well, e.g., the large volume of traffic caused by special events The dynamics of traffic produces dynamic demands on security.For example, imagine a downtown area with several supermarkets and stores that take orders from users, complete with credit card information. To protect credit card information, comprehensive cryptographic algorithms must be applied. However, the comprehensive algorithms decrease the efficiency of communication response time. Therefore, better algorithms and, perhaps, less comprehensive security schemes are needed to speed up the response time.

3. Truth relationship

Trust is one of the key factors in any secure system. A trustrelationship can exist in several ways. The network serviceproviders and the users have access to trust. There willbe a large number of government agents, e.g., the Departmentof Motor Vehicles (DMV) and the Bureau of Motor Vehicles (BMV) are trusted organizations. The relationship betwen the BMV and vehicle drivers is identity uniqueness and legitimacy. However, the large population creates challenges to building trust relationships to all the users at any time. There will be occasional exceptions. In addition, drivers are increasingly Disturbed about their privacy. Tracking users will cause fears in most cases. As a result, aliases are often applied to users. On the other hand, a certain level of trust of identity is needed. In this paper, we assume that the VC cloud infrastructure is trusted, the VC service providers are trusted, the vast majorityof VC users are trustworthy, and the attackers have the same privileges as normal users.

4. SINGLE-USER INTERFACE

Single-user access interface is another challenge to VCs. When the number of service accesses in a cloud increases, the number of Virtual Machines that provide the service will increaseto guarantee quality of service. More Virtual Machines will be created and allotted. With the increase in Virtual Machines, security apprehensions grow as well. When the number of service accesses decreases, the number of Virtual Machiness that provide the service will decrease to improve resource utilization. Some VMs will be destroyed and recycled.To achieve scalability, a simple solution is to clone and expand the service in a different cloud. However, asingle interface obviously makes scalability even more difficult.

IV. Attacker's Target

The main targets of an attacker are given as follows:

1. confidentiality, such as identities of other users, valuabledata and documents stored on the VC, and the location of the VMs, where the target's services are executing;
2. integrity, such as valuable data and documents stored onthe VC, executable code, and result on the VC;
3. availability, such as physical machines and resources,privileges, services, and applications.

One possible form of attack is given below:

1. Find the geographic location of the target vehicle andphysically move close the target machine;
2. Narrow down the possible areas where the target user'sservices are executing by mapping the topology of VC;
3. Launch multiple experimental accesses to the cloud, andfind out if

ISSN: 2278 – 7798

the target user is currently on the same VM;

4. Request the services on the same VM where the targetuser is on;
5. Use system leakage to obtain higher privilege to collectthe assets.Due to the features of the VC, there are several challenges

V. CONCLUSION

In this paper, we have addressed the security challenges of aUniqueviewpoint of VANETs, i.e., taking VANETs to clouds.We have first introduced the security and privacy challengesthat VC computing networks have to face. While some of thesolutions can leverage existing security techniques, there aremany unique challenges. For example, attackers can physicallylocate on the same cloud server. The users have high Mobility, and the communication is inherently unstable and Irregular. We have provided a directional security scheme toIllustration an appropriate security architecture that handles several, not all, challenges in VCs. In future work, we will investigate the brand-new area and design solutions for each individualchallenge. Many applications can be developed on VCs. As future work, a specific application will need to analyze and provide security solutions. Extensive work of the security and privacy in VCs willbecome a complex system and need a systematic and synthetic way to implement intelligent transportation systems. Only with joint efforts and close cooperation among different Societies such as law enforcement, government, the automobile industry, and academics can the VC computing networks provide solid and feasible security and privacy solutions.

References

[1] S. Arif, S. Olariu, J. Wang, G. Yan, W. Yang, and I. Khalil, "Datacenter at the airport: Reasoning about time-dependent parking lot occupancy," *IEEE Trans. Parallel Distrib. Syst.*, 2012, [Online].
Available:https://csdl2.computer.org/csdl/trans/td/preprint/ttd2012990021-abs.html, to be published.

[2] S. Olariu, M. Eltoweissy, and M. Younis, "Toward autonomous vehicular clouds," *ICST Trans. Mobile Commun. Comput.*, vol. 11, no. 7–9, pp. 1– 11, Jul.–Sep. 2011.

[3] S. Olariu, I. Khalil, and M. Abuelela, "Taking VANET to the clouds," *Int. J. Pervasive Comput. Commun.*, vol. 7, no. 1, pp. 7–21, 2011.

[4] L. Li, J. Song, F.-Y. Wang, W. Niehsen, and N. Zheng, "IVS 05: New developments and research trends for intelligent vehicles," *IEEE Intell.Syst.*, vol. 20, no. 4, pp. 10–14, Jul./Aug. 2005.

[5] G. Yan and S. Olariu, "A probabilistic analysis of link duration in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1227–1236, Dec. 2011.

[6] H. Xie, L. Kulik, and E. Tanin, "Privacy-aware traffic monitoring," *IEEE Trans. Intell. Transp. Syst.*, vol. 11, no. 1, pp. 61–70, Mar. 2010.

[7] D. Huang, S. Misra, G. Xue, and M. Verma, "PACP: An efficient
pseudonymous authentication based conditional privacy protocol for vanets," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 736–746, Sep. 2011.

[8] R. Hasan, *Cloud Security*. [Online]. Available: http://www.ragibhasan. com/research/cloudsec.html [9] G. Yan, S. Olariu, and M. C.Weigle, "Providing VANET security through active position detection," *Comput. Commun.*, vol. 31, no. 12, pp. 2883–2897, Jul. 2008, Special Issue on Mobility Protocols for ITS/VANET.

[10] G. Yan, S. Olariu, and M. Weigle, "Providing location security in vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 16, no. 6, pp. 48–55, Dec. 2009.

[11] J. Sun, C. Zhang, Y. Zhang, and Y. M. Fang, "An identity-based
security system for user privacy in vehicular ad hoc networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, Sep. 2010.

[12] G. Yan and S. Olariu, "An efficient geographic location-based security mechanism for vehicular ad hoc networks," in *Proc. IEEE Int. Symp. TSP*, Macau SAR, China, Oct. 2009, pp. 804–809.

[13] A. Friedman and D. West, "Privacy and security in cloud computing," *Center for Technology Innovation: Issues in Technology Innovation*, no. 3, pp. 1–11, Oct. 2010.

[14] J. A. Blackley, J. Peltier, and T. R. Peltier, *Information Security Fundamentals*. New York: Auerbach, 2004.

[15] N. Santos, K. P. Gummadi, and R. Rodrigues, "Toward trusted cloud computing," in *Proc. HotCloud*, Jun. 2009.

[16] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. B. Terra, "Virtual machine-based platform for trusted computing," in *Proc. ACM SOSP*, 2003, pp. 193–206.

[17] S. Berger, R. Cáceres, K. A. Goldman, R. Perez, R. Sailer, and L. van Doorn, "VTPM: Virtualizing the trusted platform module," in *Proc. 15th Conf. USENIX Sec. Symp.*, Berkeley, CA, 2006, pp. 305–320.

[18] D. G. Murray, G. Milos, and S. Hand, "Improving XEN security through disaggregation," in *Proc. 4th ACM SIGPLAN/SIGOPS Int. Conf. VEE*, New York, 2008, pp. 151–160.

[19] F. J. Krautheim, "Private virtual infrastructure for cloud computing," in *Proc. Conf. Hot Topics Cloud Comput.*, 2009, pp. 1–5.

[20] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in *Proc. IEEE Int. Conf. CloudComput.*, 2009, pp. 109–116.

[21] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proc. IEEEINFOCOM*, San Diego, CA, 2010, pp. 1–9.

[22] Q.Wang, C.Wang, J. Li, K. Ren, andW. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in *Proc.14th ESORICS*, 2009, pp. 355–370.

[23] 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 *Proc. 16th ACM Conf. CCS*, 2009, pp. 199–212.

[24] SIRIT-Technologies, White paper. DSRC technology and the DSRC industry consortium (DIC) prototype team.

[25] D. Wen, G. Yan, N. Zheng, L. Shen, and L. Li, "Toward cognitive vehicles,"
IEEE Intell. Syst. Mag., vol. 26, no. 3, pp. 76–80, May–Jun. 2011.

[26] Microsoft, The stride threat model. [Online]. Available: http://msdn.microsoft.com

[27] Fed. Fin. Inst. Examination Council, Authentication in an Internet banking environment 2009. [Online]. Available: http://www.ffiec.gov/pdf/ authentication_guidance.pdf

[28] J. Douceur, "The sybil attack," in *Proc. Rev. Papers 1st Int. Workshop Peer-to-Peer Syst.*, 2002, vol. 2429, pp. 251–260.

ISSN: 2278 – 7798

[29] G. Yan, W. Yang, E. F. Shaner, and D. B. Rawat, "Intrusion-tolerant location information services in intelligent vehicular networks," *Commun.Comput. Inf. Sci.,*, vol. 135, pp. 699–705, 2011.
[30] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469– 472, Jul. 1985.
[31] *The NIST Definition of Cloud Computing*, Nat. Inst. Stand. Technol., Gaithersburg, MD, Sep. 2011.
[32] J. Li, S. Tang, X. Wang, W. Duan, and F.-Y. Wang, "Growing artificial
transportation systems: A rule-based iterative design process," *IEEE*
Trans. Intell. Transp. Syst., vol. 12, no. 2, pp. 322–332, Jun. 2011.
[33] F.-Y. Wang, "Parallel control and management for intelligent transportation systems: Concepts, architectures, and applications," *IEEE Trans.Intell. Transp. Syst.*, vol. 11, no. 3, pp. 630–638, Sep. 2010.

ISSN: 2278 – 7798