Volume 5, Issue 5, May 2015 **ISSN: 2277 128X**

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey of Enhanced Security on Vehicular Cloud Computing

Rajbhoj Supriya K.
ME Computer Dept., SPCOE
Otur, India

Dr. S. V. Gumaste
Professor Dept., Computer SPCOE
Otur, India

Abstract— In a VC, underutilized vehicular resources including computing power, data storage, and Internet connectivity can be shared between rented out over the Internet to various customers. If the VC concept is to see a wide adoption and to have significant societal impact, security and privacy issues need to be addressed. The main contribution is to detect and examine a number of security challenges and potential privacy threats in VCs. Even though security issues has received the consideration in cloud computing and vehicular networks, we identified security challenges that are special to VCs, e.g., challenges of authentication of high-mobility vehicles, scalability and the complexity of establishing trust relationships among multiple players caused by intermittent short- range communications. We begin by describing the VC models, i.e.ad-hoc-based models and demonstrate algorithms to improve the scalability of security schemes and establishing trust relationships among multiple players caused by intermittent short- range communications.

Keywords: Challenge analysis, cloud computing, privacy, security, vehicular cloud.

I. INTRODUCTION

Cloud computing is everywhere. Enterprises are regularly searching for a new and advance method to increase their profits and reduce their costs. Those enterprises need different technologies that let them grow and do not strain them financially. From the present technologies, Cloud computing has emerged as a promising solution providing on demand access to virtual 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 utilities such as water and electricity to its users. There are various advantages of Cloud computing, such as cost effectiveness, scalability, and ease of management, encourage more and more companies and service providers to adapt it and over their solutions via Cloud computing models.

computing allows user to change their location at the time of accessing services from cloud. So laptops, other mobile devices becomes popular. Clients can access cloud services while moving from one location to another. With Cloud based services on one side offering affordable and centralized computing resources, and mobile devices on the other side, demanding for a centralized pool of resources to make up for their lack of processing power, now there is a connection between those two technologies that will allow future development in both areas of research. Investigate the brand-new area an design solutions for each individual challenge namely for Authentication, Authorization and truth relationship. Many applications can be developed on Clouds. There are thousands of node in cloud computing and multiple applications in a single node. Know that multiple applications on single node is not working and secure. so these problem is solved by using the third channel operator which enhances the security on cloud application of fraud detection on credit card online transaction. Now when user makes the online transaction on credit card to the merchant it should be secure. To maintain these security the system is implemented which enhances the security on vehicular cloud using the secure channel operator and third channel operator. These introduces the concept of applying the security on application which runs under cloud service. As the user makes the transaction the system ask for the OTP which is secure only on server and user side. The fraud cannot get the OTP created and he will be unable to make the fraud transaction. In such a way the security of authentication, authorization and truth relationship is maintained.

Vehicular cloud 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 and truth relationship. Many applications can be developed on Clouds. There are thousands of node in cloud computing and multiple applications in a single node. know that multiple applications on single node is not working and secure. so these problem is solved by using the third channel operator which enhances the security on cloud application of fraud detection on credit card online transaction. Now when user makes the online transaction on credit card to the merchant it should be secure. To maintain these security the system is implemented which enhances the security on vehicular cloud using the secure channel operator and third channel operator. These introduces the concept of applying the security on application which runs under cloud service. As the user makes the transaction the system ask for the OTP which is secure only on server and user side. The fraud cannot get the OTP created and he will be unable to make the fraud transaction. In such a way the security of authentication, authorization and truth relationship is maintained. This dissertation becomes successful to enhance the vehicular cloud security.

II. LITERATURE SURVEY

The security challenges in VC(vehicular cloud) are a new, exciting, and unexplored topic. Users will be autonomously pooled to create a cloud that can provide services to authorized users.users will share the capability of computing power, Internet access, and storage to form conventional clouds. These researchers have only focused on providing a framework for VC computing, but as already mentioned, the issue of security and privacy has not yet been addressed in the literature. As pointed out by Hasan [1], cloud security becomes one of the major barriers of a widespread adoption of conventional cloud services. Extrapolating from the conclusions of , it is anticipate that the same problems will be present in VCs.[7,8]

Recently, vehicular ad hoc network (VANET) security and privacy have been addressed by a large number of papers. Yan et al. proposed active and passive location security algorithms. Radar can be employed as a"virtual eye",and onboard radar can detect the location of vehicles. Public Key Infrastructure (PKI) and digital signature-based methods have been well explored in VANETs . A certificate authority (CA) generates public and private keys for nodes. The purpose of digital signature is to validate and authenticate the senderl[5][9]. The purpose of encryption is to disclose the content of messages only to entitled users. PKI is a method that is well suited for security purposes, particularly for roadside infrastructure. GeoEncrypt in VANETs has been proposed by Yan et al[12].Their idea is to use the geographic location of a vehicle to generate a secret key. Messages are encrypted with the secret key, and the encoded texts are sent to receiving vehicles. The receiving vehicles must be physically present in a certain geographic region specified by the sender to be able to decrypt the message.[10].

Recently, Olariu et al. [4], [3], [26],[27] proposed to refer to a dynamic group of vehicles whose excess computing, sensing, communication, and storage resources can be coordinated and dynamically allocated to authorized users, as a vehicular cloud. One of the characteristics that distinguishes vehicular clouds from conventional clouds is the dynamically changing amount of available resources that, in some cases, may fluctuate rather abruptly. In this work, they envision a vehicular cloud involving cars in the long-term parking lot of a typical international airport. The patrons of such a parking lot are typically on travel for several days, providing a pool of cars that can serve as the basis for a datacenter at the airport. They anticipated a park and plug scenario where the cars that participate in the vehicular cloud are plugged into a standard power outlet and are provided Ethernet connection to a central server at the airport. In order to be able to schedule resources and to assign computational tasks to the various cars in the vehicular cloud, a fundamental prerequisite is to have an accurate picture of the number of vehicles that are expected to be present in the parking lot as a function of time.[2]

A new privacy preservation scheme, named pseudonymous authentication-based conditional privacy (PACP), which allows vehicles in a vehicular ad hoc network (VANET) to use pseudonyms instead of their true identity to obtain provably good privacy. In Dijiang Huang scheme, vehicles interact with roadside units to help them generate pseudonyms for anonymous communication. In setup, the pseudonyms are only known to the vehicles but have no other entities in the network. In addition, scheme provides an efficient revocation mechanism that allows vehicles to be identified and revoked from the network if needed. Thus, they provide conditional privacy to the vehicles in the system, that is, the vehicles will be anonymous in the network until they are revoked, at which point, they cease to be anonymous.[6] Recently, some attention has been devoted to the general security problem in clouds, although not associated with vehicular networks [13]. The simple solution is to restrict access to the cloud hardware facilities. This can minimize risks from insiders [14]. Santos et al. [15] proposed a new platform to achieve trust in conventional clouds. A trust coordinator maintained by an external third party is imported to validate the entrusted cloud manager, which makes a set of virtual machines (VMs) such as Amazon's E2C (i.e., Infrastructure as a Service, IaaS) available to users. Garfinkel et al. [16] proposed a solution to prevent the owner of a physical host from accessing and interfering with the services on the host. Berger et al. [17] and Murray et al. [18] adopted a similar solution.

When a VM boots up, system information such as the basic input output system (BIOS), system programs, and all the service applications is recorded, and a hash value is generated and transmitted to a third-party Trust Center. For every period of time, the system will collect system information of the BIOS, system programs, and all the service applications and transmit the hash value of system information to the third-party Trust Center.[25]. The Trust Center can evaluate the trust value of the cloud. Krautheim [19] also proposed a third party to share the responsibility of security in cloud computing between the service provider and client, decreasing the risk exposure to both. Jensen et al. [20] stated technical security issues of using cloud services on the Internet access.

Wang et al. [21], [22] proposed public-key-based homomorphic authenticator and random masking to secure cloud data and preserve privacy of public cloud data. The bilinear aggregate signature has been extended to simultaneously audit multiple users. Ristenpart et al. [23] presented experiments of locating co-residence of other users in cloud VMs.Given its paramount importance, information security in wireless networks has received a great deal of attention. In this article focuses on the security of location information in vehicular ad hoc networks (VANETs). As vehicles are highly mobile, most VANET applications require trustworthy location information in order to function.

III. CONCLUSION

The system have obtainable the challenges arises due to the vehicular networks. The system first suggested the security and privacy challenges that VC computing networks have to face, and have also addressed possible security key on authentication, authorization and truth relationship. Even though some of the solutions can force existing security techniques, there are many distinctive challenges. For example, attackers can physically locate on the same cloud server. Directional security scheme is provided to show an appropriate security architecture that handles several, not all, challenges in VCs. Considered the brand-new area and design solutions for security challenge discussed above. Many applications are developed on VCs. In future work a special application is implemented to analyze and provide security solutions. So these difficulty is solved by using the third channel operator which enhances the security on cloud application of fraud detection on credit card online transaction. Widespread work of the security and privacy in VCs will become a complex system and need a systematic and synthetic way to implement intelligent conveyance systems.

ACKNOWLEDGE

We would like to thank Our Principal Dr.G.U.Kharat for valuable guidance at all steps while framing this paper. Throughout the work he motivated and we must admit that the work would not have been accomplished without guidance and encouragement. I take this opportunity to express my sincere thanks to my respected and helpful guide Dr.S.V.Gumaste. for his guidance, support, encouragement and advice.

REFERENCES

[1] Gongjun Yan, Ding Wen, Stephan Olariu, and Michele C. Weigle ," Security Challenges in Vehicular Cloud Computing*", IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 14, NO. 1,* MARCH 2013.

[2] 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

[3] 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.

[4] 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.

[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] 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.

[7] 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.

[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. Cloud Comput.*, 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. IEEE INFOCOM*, 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] 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.

[24] 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.

[25] 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.