International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 03, March 2017
www.ijates.com
ijates
ISSN 2348 - 7550

# SECURITY DEMANDING IN VEHICULAR CLOUD COMPUTING USING FRAUD DETECTION IN CREDIT CARD APPLICATION

**Minhaj[1], Salehafarha[2]**

## ABSTRACT

*In the Mobile Computing technology, mobile devices like smartphones and tablets were replaces personal computers by combining network connectivity, mobility and software functionality. Vehicular cloud computing also increases its popularity. Which is similar to the mobile cloud computing. There are large numbers of nodes in cloud computing, so there is more chance of leakage of data or information from the attacker. The work is to identify and analyze a number of security challenges and potential privacy threats in Clouds, identify security challenges that are specific to Clouds, e.g., challenges of authentication of highmobility, scalability, and the complexity of establishing trust relationships among multiple nodes. And to operate multiple applications on single node with secure channel*

***Keywords: Challenge Analysis, Cloud Computing, Privacy, Security, Vehicular Cloud***

## I. INTRODUCTION

Enterprises are regularly searching for a new and improvement 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 existing 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 relaxation of customary 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, boost more and more companies and service providers to adapt it and over their solutions via Cloud computing models. 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 handling power, storage, networks, and other essential 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 limitations, 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. 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.

## II. SYSTEM ARCHITECTURE

Recent years researchers have been concerned about the security of the cloud network in the implementation of vehicular cloud network. However there are other challenges like high mobility of nodes, signal attenuation, network scalability. Vehicular cloud computing also increases its popularity. People uses Laptops and other mobile devices to access the services of cloud when ever necessary at any time. So the security problem increases and the data does not remain safe the attacker attacks the data and miss use it. In recent years cloud computing becomes popular due to its simple nature. Mobile 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. As shown in the figure user can ascess to any node in the cloud and have a secure connection to the applications in a single node.

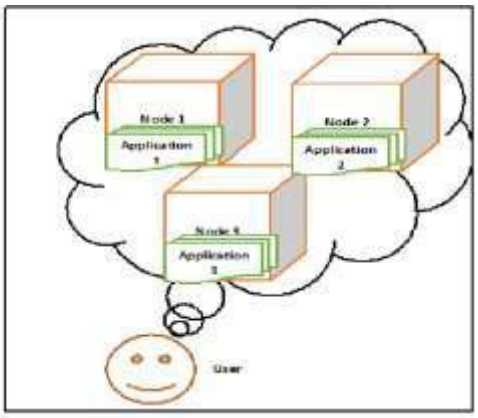


**Figure 1: System Architecture**

In this system uses different users and a node with application named credit card online transaction fraud detection in a cloud. Then the cloud sends the request to node to connect to the application which is being created. First login to the application. Then user can make the transaction as he want, when the system ask for the password the OTP is created and send to the user. So that the user can make the secure transaction. If the intruder enters the wrong password the system gets log out and fraud alert is seen on the screen and fraud report is created on the server side. Figure shows the flow of system.

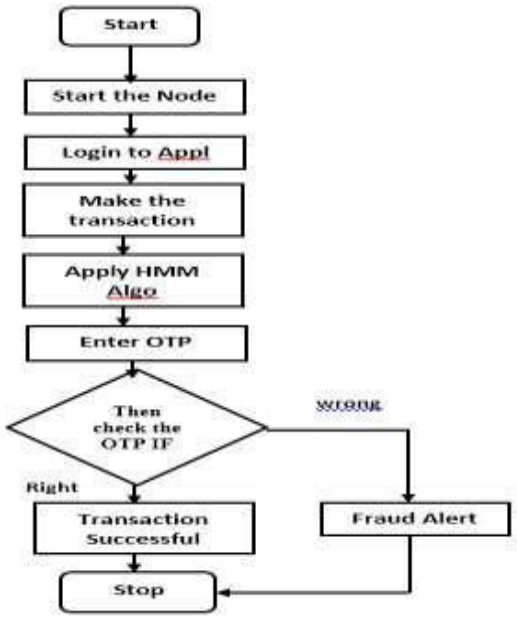


**Figure 2: System Algorithm**

1. Start.
2. Start node.
3. User connect to the cloud after successful login.
4. The user gets login to the application.
5. User makes the transaction.
6. According to the transaction done by the user the HMM predicts for the next transaction if it is greater then ask for the OTP.
7. Then OTP is created on the user side, and user enters the OTP.

## III. RESULT AND ANALYSIS

This system meets all the objectives and goals stated before at the time of enhancingthe security on vehicular cloud. The table shows the fraud report generated at admin sitewith the frauds ip Address.

**Table.1 Fraud Report**

| Alert ID | Credit Card ID | Name | Date Time | IP | UserID |
|---|---|---|---|---|---|
| 1 | 3 | a | 2015-02-18 15:41:03 | 127.0.0.1 | 3 |
| 2 | 3 | a | 2015-02-19 16:06:25 | 127.0.0.1 | 3 |
| 3 | 116 | smita | 2015-03-24 10:40:59 | 127.0.0.1 | 116 |

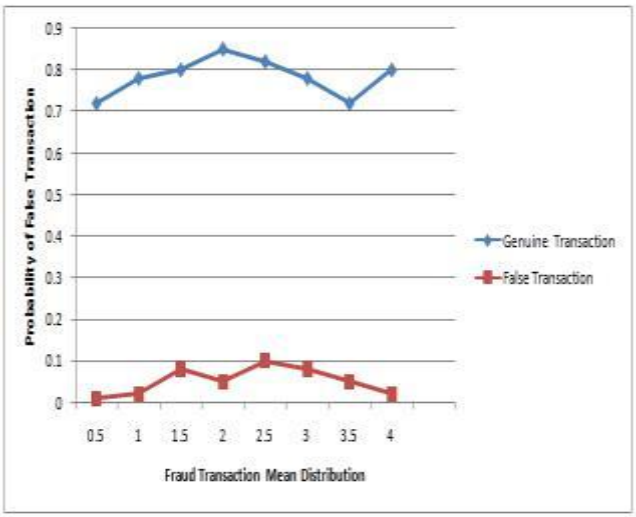


**Figure 3. False Transaction**

Fraud detection mean distribution is shown in Figure where probability of false transaction compared with that of genuine transaction.it is noted that when probability of genuine transaction is going down correspondingly probability of false transaction is going to increase and vise versa. It helps to find out the false alarm for the detection of fraud transaction. Hence, when the probability of false alarm will be more than threshold probability, then it will generate an alarm for fraudulient and also decline the transaction.

## IV. CONCLUSION AND FUTURE WORK

The system first proposed the security and privacy challenges that VC computingnetworks have to face, and have also addressed possible security solution on authentication, authorization and truth relationship. Even though some of the solutions can leverage 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. Investigated the brand-new area and design solutions for security challenge discussed above. Many applications are developed on VCs. In this work a special application is implemented to analyze and provide security solutions. 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.

Extensive work of the security and privacy in VCs will become a complex system and need a systematic and synthetic way to implement intelligent transportation systems. As a future work instead of One time Password, biometric password can be used.

## REFERENCES

[1] Gongjun Yan, Ding Wen, Stephan Olariu, and Michele C. Weigle, " Security Challengesin Vehicular Cloud Computing", IEEE transactions on intelligent transportation systemsSyst., 2012. 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", ICSTTrans. Mobile Commun. Comput., vol. 11, no. 7-9, pp. 1 to 11, Jul.-Sep. 2011.

[4] S. Olariu, I. Khalil, and M. Abuelela,"Taking VANET to the clouds" , Int. J. PervasiveComput. Commun., vol. 7, no. 1, pp. 7-21, 2011.

[5] G. Yan and S. Olariu, "A probabilistic analysis of link duration in vehicular ad hocnetworks", 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 authenticationbased 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 transportationsystems: 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 positiondetection", Comput. Commun., vol. 31, no. 12, pp. 2883- 2897, Jul. 2008, Special Issueon Mobility Protocols for ITS/VANET.

[10] G. Yan, S. Olariu, and M. Weigle, "Providing location security in vehicular ad hocnetworks" 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 f 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 TechnologyInnovation: Issues in Technology Innovation, no. 3, pp. 1-11, Oct. 2010.

[14] J. A. Blackley, J. Peltier, and T. R. Peltier,“ Information Security Fundamentals",. NewYork: Auerbach, 2004.

[15] N. Santos, K. P. Gummadi, and R. Rodrigues, “Toward trusted cloud computing", inProc. HotCloud, Jun. 2009. T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. B. Terra, “Virtual machine-basedplatform for trusted computing", in Proc. ACM SOSP, 2003, pp. 193-206.

[16] S. Berger, R. Caceres, 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.

[17] 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.

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

[19] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, “On technical security issues incloud computing", in Proc. IEEE Int. Conf. Cloud Comput., 2009, pp. 109-116.

[20] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for datastorage security in cloud computing", in Proc. IEEE INFOCOM, San Diego, CA, 2010,pp. 1-9.

[21] Q.Wang, C.Wang, J. Li, K. Ren, andW. Lou, “Enabling public verifiability and datadynamics for storage security in cloud computing", in Proc.14th ESORICS, 2009, pp.355-370.

[22] 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.

[23] 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.

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

[25] S. Olariu, T. Hristov, and G. Yan, “The Next Paradigm Shift: FromVehicular Networksto Vehicular Clouds", Networking: The Cutting Edge Directions, Wiley and Sons, 2012

[26] M. Eltoweissy, S. Olariu, and M. Younis, “ITowardsAutonomousVehicular Clouds", Proc. Int. Conf., Ad Hoc Networks (AdHocNets’10), Aug. 2010.

[27] L. Volonino and S. R. Robinson, Principles and Practice of Information Security.,Pearson Education, 2003..

[28] M. Horton and C. Mugge, HackNotes , “Network Security Portable Reference", McGraw-Hill. , Inc., 2003.

[29] J. Hubaux and S. Luo, W. Niehsen, and N. Zheng, “The security and privacy of smartvehicles", IEEE Security Privacy, vol. 2, no. 3, pp. 49-55, May/Jun. 2004.

[30] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, “ECPP: Efficient conditional privacy preservationprotocol for secure vehicular communications", Proc. IEEE INFOCOM,Apr.2008, pp. 1229-1237.

[31] I. Blake, G. Seroussi, and N. Smart, ‘Advances in Elliptic Curve Cryptography Cambridge,U.K.: Cambridge Univ. Press, 2005, ser. London Mathematical Society LectureNote Series 317.", .

[32] N. Koblitz, “Elliptic curve cryptosystems", Math. Comput., vol. 48, no. 177, pp. 203-209,1987.

[33] J. Kuchar and A. Drumm, “The Traffic Alert and Collision Avoidance System", Proc. IEEE INFOCOM,Avol. 16, no. 2, 2003, pp. 277-96.

[34] Jiafu Wan, Daqiang Zhang, Shengjie Zhao, Laurence T. Yang, and Jaime Lloret,“Context-Aware Vehicular Cyber-Physical Systems with Cloud Support: Architecture,Challenges, and Solutions", IEEE Communications Magazine, August 2014

[36] Salimbitam, Abdelhamidmellouk, and Sheralizeadally, “vanet-cloud: a generic cloudcomputing model for vehicular ad hoc networkS", Journal of The Korea Institute ofInformation Security Cryptology ,VOL.24, NO.5, Oct. 2014.

[37] Rasheed Hussain,Heekuck Oh Hanyang University, “A Secure and Privacy-Aware RouteTracing and Revocation Mechanism in VANET-based Clouds", Proc. IEEE INFOCOM,Apr. 2008, pp. 1229-1237.

[38] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, ‘Security Challenges in Vehicular CloudComputing", ,âAI IEEE Transactions on Intelligent Transportation Systems, Vol. PP,No. 99, pp.1-11, 2012.

[39] A. Thiagarajan, L. Ravindranath, K. LaCurts, S. Madden, H.Balakrishnan, S. Toledo,J. Eriksson, P. Ho, and X. Shen, “Vtrack: accurate, energy-aware road traffic delay estimationusing mobile phones", IntâAZl Conf. Embedded Networked Sensor Systems,2009,85-98.

[40] Rasheed Hussain, ZeinabRezaeifar, “On Secure, Privacy-aware, and Efficient BeaconBroadcasting among One-hop Neighbors in VANETs", IEEE MilCom,2014.

[41] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, “Rethinking vehicular communications:merging VANET with cloud computing", Proceedings of IEEE 4th International Conferenceon Cloud Computing Technology and Science (CloudCom2012),pp.606-609,2012.

[42] Rasheed Hussain and Heekuck Oh, “Cooperation-Aware VANET Clouds: ProvidingSecure Cloud Services to Vehicular Ad Hoc Networks", J Inf Process Syst ,Vol.10, No.1,pp.103 118, March 2014, pp. 1229-1237.

[43] Matko Kuna, HrvojeKolaric, Iva Bojic, Mario Kusek and GordanJezic,“Android/OSGi-based Machine-to-Machine Context-Aware System", ,University of Zagreb.

[44] Rasheed Hussain ,ZeinabRezaeifar ,Heekuck Oh, “A Paradigm Shift from Vehicular AdHoc Networks to VANET-Based Clouds", Springer Science Business Media New York2015.

[45] Fizza Abbas, Rasheed Hussain, Junggab Son and Heekuck Oh, “Privacy PreservingCloud-based Computing Platform (PPCCP) for using Location Based Services",IEEE/ACM 6th International Conference on Utility and Cloud Computing,2013.

[46] M.R.Yasmeen, “SAAS âAS A Gateway to Cost Effective Secure Vehicular Clouds",International Journal of Computer Science and Mobile Computing,Vol. 3, Issue. 4, April2014, pg.275-283.

[47] Md Whaiduzzamana,n, Mehdi Sookhak a, Abdullah Gani a, RajkumarBuyya, “Asurvey on vehicularcloud computing", Journal of Network and Computer Applications,August 2013.

[48] KayhanZrarGhafoor, “Vehicular Cloud Computing:Trends and Challenges".

[49] Md Ali Al Mamun, KhairulAnam, MdFakhrulAlamOnik, A M Esfar- E- Alam, “Deploymentof Cloud Computing into VANET to Create Ad Hoc Cloud Network Architecture",Proceedings of the World Congress on Engineering and Computer Science,2012Vol I WCECS 2012, October 24-26, 2012, San Francisco, USA.