ISSN:0975-9646



# Implementation of Enhanced Security on Vehicular Cloud Computing

RajbhojSupriya K.[1], Pankaj R. Chandre[2]

[1]*ME Comp Student,SPCOE Otur*
[2]*Assistant Professor,SPCOE Otur*

**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 attention 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.**

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

## I. INTRODUCTION

IN an work to help their vehicles competent in the market, the vehicles manufacturers are offering increasingly more potent onboard devices, including powerful computers, a large collection of wireless transceivers. These device provide a set of customers that expect their vehicles to provide unified extension of their home environment populated by refined entertainment centers, access to Internet, and other similar requirements and needs. Powerful onboard devices support new applications, including location-specific services, online gaming, and various forms of mobile infotainment.

Security and privacy problems need to be addressed if the VC concept is to be widely adopted. Traditional network systems try to prevent attackers from arriving a system. In VC, all the users, including the attackers, are equal. The attackers can be physically located on one machine. The attackers can utilize system ambiguities to reach their goals, such as obtaining confidential records and interfering with the integrity of information and the availability of resources. Suppose that an accident has taken place at center, and the accident will be reported to the VC. The driver responsible for the accident can conquer the VC and modify the accident record. In Future, when the law enforcement or the vehicle insurance company enquiry the accident, they cannot link the accident to the driver who caused it. Casually, the security issues faced in VCs may look corruptly similar to those experienced in other networks. However, a more careful analysis exposes that many of the classic security challenges are intensified by the characteristic features of VCs to the point where they can be construed as VC-specific .The main contributions of this work are to recognize
and evaluate security challenges and privacy threats that are VC specific and to propose a reasonable security structure that addresses some of the VC challenges recognized in this paper.

## II. RELATED WORK

The security challenges in VC is a new, interesting topic. Vehicles will be independently shared to create a cloud that can provide services to certified users. This cloud can provide real-time services, such as mobile systematic laboratories, intelligent transportation systems and smart electric power grids. Vehicles will share the ability of calculating power, Internet access, and storage to form conventional clouds. These researchers have only focused on providing a structure for VC computing, but as already said, the problem of privacy and security has not yet been mentioned in the literature. As pointed out by Hasan [8], cloud security becomes one of the major obstacles of a widespread adoption of traditional cloud services. Generalizing the recommendations of [8], we expect that the same problems will be present in VCs.

Now a days, vehicular ad hoc network (VANET) security and privacy have been addressed by a large number of papers. Yan *et al* [9], [10] proposed active and passive location security algorithms. Public Key Infrastructure (PKI) and digital signature-based methods have been well exposed in VANETs [11]. A certificate authority (CA) generates public and private keys for nodes.

The use of digital signature is to validate and authenticate the sender.

The main use of encryption is to reveal the content of messages only to entitled users. PKI is a method that is well suited for security purposes, particularly for roadside infrastructure. Geo Encrypt in VANETs has been proposed by Yan *et al* [12]. The idea is to use the geographic location of a movable device to create a secret key. Encrypted messages with the secret key, and the encoded texts are sent to receiving movable device. The receiving movable device must be physically present in a certain geographic region specified by the sender to be able to decrypt the message.

In recent times, some attention has been given to the general security problem in clouds, although not associated with vehicular networks [13]. The simple solution is to control 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 delivered 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 retrieving and snooping with the services on the host. Berger *et al* [17] and Murray *et al.* [18] adopted a similar solution. When a VM boots up, systeminformation such as the basic input output system (BIOS), systemprograms, and all the service applications is recorded, anda hash value is generated and transmitted to a third-party TrustCenter. For every period of time, the system will collect systeminformation of the BIOS, system programs, and all the serviceapplications and transmit the hash value of system informationto the third-party Trust Center. The Trust Center can evaluatethe trust value of the cloud. Krautheim [19] also proposeda third party to share the responsibility of security in cloudcomputing between the service provider and client, decreasingthe risk disclosure to both. Jensen *et al* [20] stated technicalsecurity issues of using cloud services on the Internet access.Wang *et al* [21], [22] proposed public-key-based homomorphismauthenticator and random masking to secure cloud data andpreserve privacy of public cloud data. The bilinear aggregatesignature has been extended to simultaneously audit multipleusers. Ristenpart*et al.* [23] resented experiments of locatingco-residence of other users in cloud VMs.

## III. PROGRAMMERS MODEL

### *A. Mathematical Model :*

Memory utilization: The experiment was done to find space saving capability. We implemented vc for Java (jdk 1.6.0),. The sizes of the client and the server programs were 75KB and 160KB, respectively.

Consider a wireless network with N systems. The software/resource to be installed is S Variable (size of S in MB).

In general the total memory occupied in the wireless network is the sum of all the memory installed on each system

Mt = N*S MB.

Where,

Mt is Temporary variable

N is Number of Systems.

Consider N-1 systems to be clients and one system as server (host) So N-1 system must installed with client program. So

Clients occupy: (*N*-1)*Sc MB.

One (At least One) system must be installed with server program. So

Server occupy : (1) * Ss MB + S MB

Then the total memory occupied in the wireless network is

Mtvc = (*N*-1)Sc + Ss + S MB.

Then the total memory saved in this wireless network is

Msvc = *NS* - ((*N*-1)Sc = Ss +S)MB.

Percentage utilization of memory on this wireless network using our concept:

((*NS*-((*N*-1)Sc + Ss + S))/*NS*)100

The database size at server side will grow dynamically so it is not taken into consideration in above calculations.

Number of systems in the lab, N = 5; Size of the software to be shared,

S=162MB(jdk1.6.0) =162MB

So, in normal lab if each system has installed this software, then total memory occupied is

M*t* = 5 *162MB = 810 MB;

Using this concept designed two utilities one for clients (i.e. client program) and one for packet sending the resource (i.e. server program)

Mtvc = (5-1) * 75KB + 1 X 160KB +162MB.608KB = 622.608 MB;

Msvc = 955 MB -622.608 = 332.292MB;

N = 622/955 = 65.13%

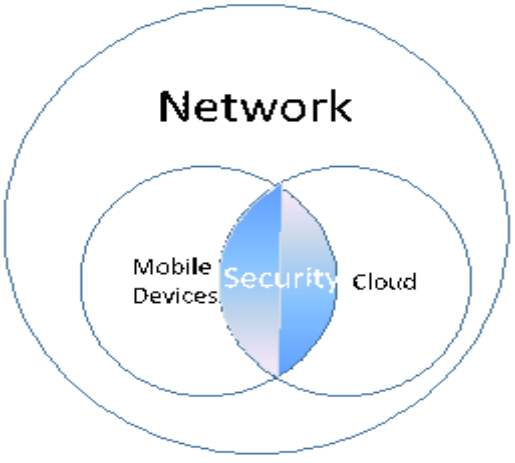


Fig 1:Mathematical Model

## IV. IMPLEMENTATION DETAILS

In a previous papers, Prof. Olariu have promoted the vision of vehicular clouds (VCs), a nontrivial extension, along several dimensions, of conventional cloud computing. In a VC, underutilized vehicular resources including computing power, storage, and Internet connectivity can be shared between renters out over the Internet to various customers. The security challenges are addressed of a novel perspective of VANETs. This system have first introduced the security and privacy challenges that VC computing networks have to face, and system also addressed possible security solutions. Although some of the solutions can leverage existing security techniques, there are many unique challenges. For example, attackers can physically locate on the same cloud server.

The below figure shows the system block diagram, theflow of how to generate the truth relationship.

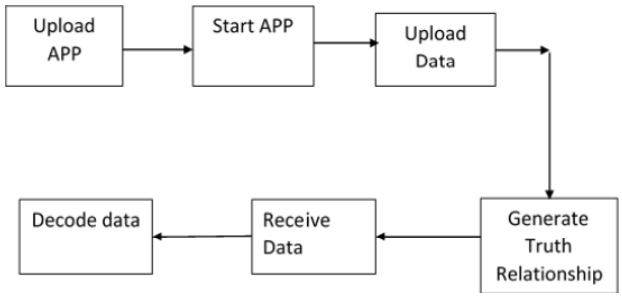


Fig 2: System Block Diagram.

The signature of the safety message can be described as follows: Following the ElGamal signature scheme defines the parameters.

1. Generate user global userset
2. If currentuser user then
3. H: a collision-free hash function;
4. p: a large prime number that will ensure that computing discrete logarithms modulo p is very difficult;
5. g smaller than p: a randomly chosen generator out of a multiplicative group of integers modulo p.

Each vehicle has long-term PKI public/private key pairs:

• private key: S;

• public key: *g, p, T,where*

*T = gSmodp.*

It should be noted that a message m can be combined as m—T, where T is the timestamp. The timestamp can ensure the freshness of the message. For each message m to be signed, three steps are followed.

1. Generate a per-message public/private key pair of Sm (private) and Tm = gSm mod p (public).
2. Compute the message digest dm = H(m|Tm) and the message signature X = $S_m$ + dmS mod (p -1), where mod is the modulo operation and | is the concatenation operator.
3. Send m, Tm, and X.

To verify the message, three steps are followed.

1. Compute the message digest dm = H(m—Tm).
2. Compute Y1 = $g^x$ and Y2 = TmTdm.
3. compare Y1 = Y2. If Y1 = Y2, then the signature is correct.

The reason is:

Y1=gX =gSm+dmS =gSmgdmS =TmgSdm =TmTdm =Y 2.

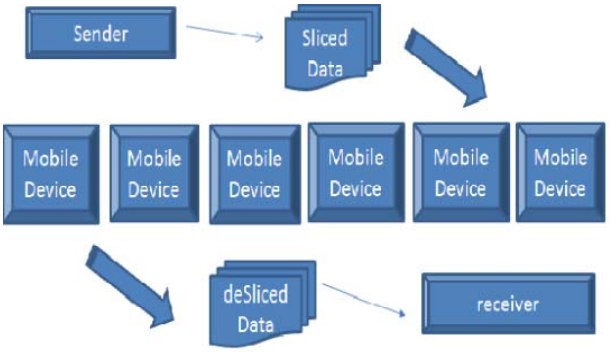


Fig 3: System Architecture

The above figure shows the system architecture how the sender sends the data then it will get sliced and passed to the mobile devices and again it will get desliced so the other usre will not be able to use the data and passed to the receiver.using it we will maintain the security of VC computing.

## V. RESULT AND CONCLUSION

We have first proposed the security and privacy challenges that VC computing networks have to face, and have also addressed possible security solutions. 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. The vehicles have high mobility, and the communication is inherently unstable and intermittent. We have provided a directional security scheme to show an appropriate security architecture that handles several, not all, challenges in VCs. Now we have investigated the brand-new area and design solutions for each individual challenge. Many applications are developed on VCs. In proposed work a special application will need to analyze and provide security solutions. 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.

## REFERENCES

[1]Gongjun Yan, Ding Wen, Stephan Olariu, and Michele C. Weigle, " Security Challenges in Vehicular Cloud Computing", *IEEE transactions on intelligenttransportation systems* Syst., 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", *IEEETrans. Parallel Distrib.* Syst., 2012.

[3]S. Olariu, M. Eltoweissy, and M. Younis, "Toward autonomous vehicular clouds", *ICST Trans. MobileCommun.* Comput., vol. 11, no. 7âAS9, pp. 1 to 11, Jul.âASSep. 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 rulebased 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" *IEEEWireless 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.ParallelDistrib.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",Centerfor 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. CÃaceres, 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.IEEE, NewYork, 2008*, pp. 151-160.

[19]F. J. Krautheim, "Private virtual infrastructure for cloud computing", *in Proc. Conf. Hot Topics CloudComput., 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, SanDiego, CA, 2010*, pp1-9.

[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.14thESORICS*, 2009, pp. 355-370.

[23] F.-Y. Wang, "Parallel control and management for intelligent transportation systems: Concepts, architectures, and applications", *IEEE Tran. 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.