Vehicular Cloud Computing and Its Security Challenges

Bindushree M R(1) Vijayalaxshmi R Pati(2)

(1) PG student, M Tech ,CNE, Dr.AIT, Bangalore
(2) Assistant professor, Dr. AIT, Bangalore

***Abstract*-Vehicular networking has become a significant research area due to its specific features and applications such as standardization, efficient traffic management, road safety. Vehicles are expected to carry relatively more communication systems, on board computing facilities, storage and increased sensing power. Hence, several technologies have been deployed to maintain and promote Intelligent Transportation Systems (ITS). Recently, a number of solutions were proposed to address the challenges and issues of vehicular networks. Vehicular Cloud Computing (VCC) is one of the solutions. VCC is a new hybrid technology that has a remarkable impact on traffic management and road safety by instantly using vehicular resources, such as computing, storage and internet for decision making. The main contribution of this work is to identify a number of security challenges and potential privacy threats in VCs.**

I. INTRODUCTION

Vehicular Cloud Computing is a new technological shifting, which takes advantage of cloud computing to serve the drivers of VANETs with a pay as you go model. Thus, the objectives of VCC are to provide several computational services at low cost to the vehicle drivers; to minimize traffic congestion, accidents, travel time and environmental pollution; and to ensure uses of low energy and real time services of software, platforms, and infrastructure with QOS to drivers.

Obviously, security and privacy issues need to be addressed if the VC concept is to be widely adopted. Conventional networks attempt to prevent attackers from entering a system. However, in VC, all the users, including the attackers, are equal. The attackers and their targets may be physically colocated on one machine. The attackers can utilize system loopholes to reach their goals, such as obtaining confidential information and tampering with the integrity of information and the availability of resources.

The main contribution of this work is to understand vehicular cloud computing and identify a number of security challenges and potential privacy threats in VCs

II. VEHICULAR CLOUDS

There are two types of VCs. In the first type called *Infrastructure-based VC*, drivers will be able to access services by network communications involving the roadside infrastructure. In the second type called *Autonomous VC* (AVC) [4], vehicles can be organized on-the-fly to form VC in support of emergencies and other ad hoc events. VCs provide services at three levels, i.e., application, platform, and infrastructure. Service providers use the levels differently based on what and how the services are offered. The fundamental level is called *Infrastructure as a Service* (IaaS), where infrastructure such as computing, storage, sensing, communicating devices, and software are created as VMs. The next level is *Platform as a Service* (PaaS), where components and services (such as httpd, ftpd, and email server) are provided and configured as a service. The top level is called *Software as a Service* (SaaS), where applications are provided in a "pay-as-you-go" fashion.

A. Three-Tier Vehicle Cloud Architecture

With the aid of modern technologies such as MEMS, wireless communication techniques, Internet and cloud computing etc, we can imagine that future road transportation system will be more powerful, intelligent, flexible and convenient for both drivers and administrative centers.

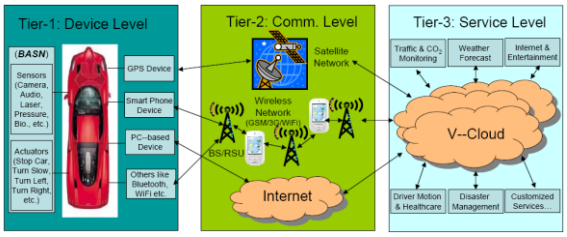

Figure 1. Three tier V-Cloud architecture[2]

Figure 1, shows novel three-tier V-Cloud architecture from functioning point of view.

In the tier-1, there are various devices module ranging from sensors, actuators, GSP, smart phone and pc-based devices. It is worth mentioning that many of these tiny devices can form a body area sensor network (BASN) within a short range. Some of the devices may be equipped with the car while many others may be hand-held devices or attached on the driver to monitor the physical health information.

In tier-2, The wireless communication can b classified into 3 groups: 1) communication to satellite network via GPS devices; 2) communication to GSM/3G/WiFi wireless networks via smart phone or other devices; 3) communication to the Internet via PC or navigation

devices. It is worth noting that the communication with base station (BS) or road side unit (RSU) is part of group 2.

In tier-3, we can the core service module which is enabled by cloud computing technique. Here, we just list several representative services such as road traffic monitoring, CO2 pollution detection, Internet access, Entertainment, driver mood & health monitoring etc. Many other customized services like parking, dining, reminding can also be developed based on driver's requirement or preference.

B. Applications of VC Computing

In this section, we review several possible applications of VCs.

- *Vehicle maintenance:* Vehicles receive software updates from cloud whenever vehicle manufacturers upload a new version of software.
- *Traffic management:* Drivers can receive traffic status reports (e.g., congestion) from VCs.
- *Road condition sharing:* Road conditions such as flooding areas and black ice on the roadway can be shared in VCs. Drivers will be alerted if there are serious road conditions.
- *Accident alerts at intersections:* Under demanding driving conditions such as fog, heavy storm, snow, and black ice, drivers can order this service to alert them of possible accidents at intersections. Infrastructure, e.g., a tall building, can include high-precision radar to detect car accidents. This infrastructure will cover the whole intersection and frequently scan the intersection. An intelligent algorithm will be applied to each scan result to predict the possibility of accidents.
- *Safety applications:* Applications related to life-critical scenarios such as collision avoidance and adaptive cruis control require strong security protection, even from surrounding environmental security threats.
- *Intelligent parking management:* Vehicles will be able to book a parking spot using the VC. All the parking information will be available on clouds without central control. Requests from different physical places can be transferred to the most desired parking lots.
- *Planned evacuations:* In some disasters such as a hurricanes and tsunamis, VCs will be instrumental in organized evacuations.

III. SECURITY CHALLENGES IN A VEHICULAR CLOUD

A. Security and Privacy Attacks in VC

a) Attacker Model: Traditional security systems are often designed to prevent attackers from entering the system. However, security systems in the VC have a much harder time keeping attackers at bay, because multiple service users with high mobility can share the same physical infrastructure. In the VC environment, an attacker can equally share the same physical machine/infrastructure as their targets, although both of them are assigned to different VMs. To this point, attackers can have more advantages than the attackers on traditional systems. In addition, the attackers are physically moving from place to place as vehicles are mobile nodes. It is much harder to locate the attackers.

The main targets of an attacker are given as follows:

1) confidentiality, such as identities of other users, valuable data 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 on the VC, executable code, and result on the VC;
3) availability, such as physical machines and resources privileges, services, and applications.
4) non-repudiation , the assurance that entities cannot deny receiving or sending a message that originated from them.
(5)Authentication: Determining whether someone or something is, who or what it is claimed to be.
(6) Privacy: The user's privacy should be preserved.
(7) Real-time constraints: Some applications, such as accident alerts, require real-time or near real-time communication.

b) Threats: The threats in the VC are given here.

1) *Spoofing user identity:* The attackers pretend to be another user to obtain data and illegitimate advantages. One classic example is the "man-in-the-middle attack,"
2) *Tampering:* The attackers alter data and modify and forge information.
3) *Repudiation:* The attackers manipulate or forge the identification of new data, actions, and operations.
4) *Information disclosure:* The attackers uncover personally identifiable information such as identities, medical, legality, finance, political, residence and geographic records, biological traits, and ethnicity.
5) *Denial of Service:* The attackers mount attacks that consume system resources and make the resources unavailable to the intended users.
6) *Elevation of privilege:* The attackers exploit a bug, system leakage, design flaw, or configuration mistake in an operating system or software application to obtain elevated access privilege to protected resources or data that are normally protected from normal users.

B. Authentication of High-Mobility Nodes

The authentication in VC contains verifying the authentication of users and the integrity of messages. The VC environment is more challenging than vehicular network and cloud computing, due to the high mobility of nodes. In addition, verifying the authentication of transmitting messages by using location based authentication methods in VC is difficult because of high mobility of nodes. For example, the authentication of accident alert messages associated with the location of

vehicles and time of the accident cannot be verified easily because the location of vehicles is changing

C. Secure Location and Localization

Location information plays a vital role in VC to transmit data and create connections because most applications in vehicular systems rely on location information such as traffic status reports, collision avoidance, emergency alerts, and cooperative driving. Therefore, the security of location information and localization should be provided among vehicles.

There are three models to validate and integrate the location information in a VC. An active location integrity model is the first approach and validates vehicle locations by using devices such as radar. The second model is passive location integrity which is based on filtering the impossible locations and building previous location of neighbouring vehicles without using radar. The last location integrity method is a general location integrity model that calculates the high accuracy location from the low resolution location by filtering the malicious location in VC.

D. Scalability

Security schemes for VCs must be scalable to handle a dynamically changing number of vehicles. Security schemes must handle not only regular traffic but special traffic as well, e.g., the large volume of traffic caused by special events (e.g.,football games, air shows, etc.)

E. 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 VMs that provide the service will increase to guarantee quality of service. More VMs will be created and assigned. With the increase in VMs, security concerns grow as well. When the number of service accesses decreases,

the number of VMs that provide the service will decrease to improve resource utilization. Some VMs will be destroyed and recycled. These procedures are transparent to vehicles. Vehicles

only see one access interface and do not need to know the changing of VMs.

F. Heterogeneous Network Nodes

Conventional cloud computing and fixed networks often have homogeneous end users. As it turns out, vehicles have a large array of (sometimes) vastly different onboard devices. Some high-end vehicles have several advanced devices, including a Global Positioning System (GPS) receiver, one or more wireless transceivers, and onboard radar devices. In contrast, some economy models have only a wireless transceiver. Some other vehicles have different combinations of GPS receivers, wireless transceivers, and radar. Different vehicle models have different device capabilities such as speed of processor, volume of memory, and storage. These heterogeneous vehicles as network nodes create difficulties to adapting security strategies.

G. VC Messages

1) Safety Messages: The initial motivation of VANET was the dissemination of traffic safety messages. Based on the emergency level, there are three types of safety messages.

1) Level one: public traffic condition information.
2) Level two: cooperative safety messages.
3) Level three: liability messages.

2) Confidential Messages:

To ensure the confidentiality of a sensitive message, the message will be both signed and encrypted.

IV. CONCLUSION

VCC emerges from the convergence of powerful implanted vehicle resources, advances in network mobility, ubiquitous sensing 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.In this paper, we proposed three-tier V-Cloud architecture with brief explanation, potential application and we have addressed the security and privacy challenges that VC computing networks have to face. If these challenges are over come the VCC can be the next technological shifting paradigm that provides technologically feasible and economically viable solutions by converging intelligent vehicular networks towards autonomous traffic, vehicle control and perception systems.

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. 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.] Whaiduzzaman M, et al. A survey on vehicular cloud computing. Journal of Network and Computer Applications (2013),http://dx.doi.org/10.1016/j.jnca.2013.08.004

[4.] Mario Gerla Computer Science Department, UCLA Los Angeles, CA 90095 gerla@cs.ucla.edu, "Vehicular Cloud Computing"

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

[6.] Jin Wang, Tinghuai Ma, Jinsong Cho, Sungyoung Lee "Real Time Services for Future Cloud Computing Enabled Vehicle Networks", Kyung Hee University, Computer Engineering Department, Korea,