© 2017 IJSRSET | Volume 3 | Issue 3 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Malicious Node Detection in Vehicular Cloud Computing

Jaida Khatoon, Abhishek Bajpai, Dr. Neeraj Kumar Tiwari
Department of Computer Applications, ShriRamswaroop Memorial University(SRMU , UGC Affiliated), Lucknow Uttar Pradesh, India

ABSTRACT

In this paper, we discuss malicious node detection in mobile cloud computing. There are various methods used previously to detect malicious nodes and prevent from any kind of attack. Various security measures have been implemented already. But now combination or hybrid of 2 or more methods provide more efficient more reliable and more cost effective method to prevent from any kind of attack. Vehicular networking has become a significant research area due to its specific features and applications such as standardization, efficient traffic management, road safety and infotainment. 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. This paper presents the state-of-the-art survey of vehicular cloud computing. Moreover, we present a taxonomy for vehicular cloud in which special attention has been devoted to the extensive applications, cloud formations, key management, inter cloud communication systems, and broad aspects of privacy and security issues. Through an extensive review of the literature, we design an architecture for VCC, itemize the properties required in vehicular cloud that support this model. We compare this mechanism with normal Cloud Computing (CC) and discuss open research issues and future directions. By reviewing and analyzing literature, we found that VCC is a technologically feasible and economically viable technological shifting paradigm for converging intelligent vehicular networks towards autonomous traffic, vehicle control and perception systems.

Keywords : Vehicular Cloud Computing, Vehicular Network, Security Of Vehicular Networks, Security Challenges

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 VCC can address the convergence of ITS and the tremendous computing and storage capabilities of MCC. Further-more, VCC provides a technically feasible incorporation of the ubiquitous sensing of WSN, ITS and MCC for better road safety and secured intelligent urban traffic systems.

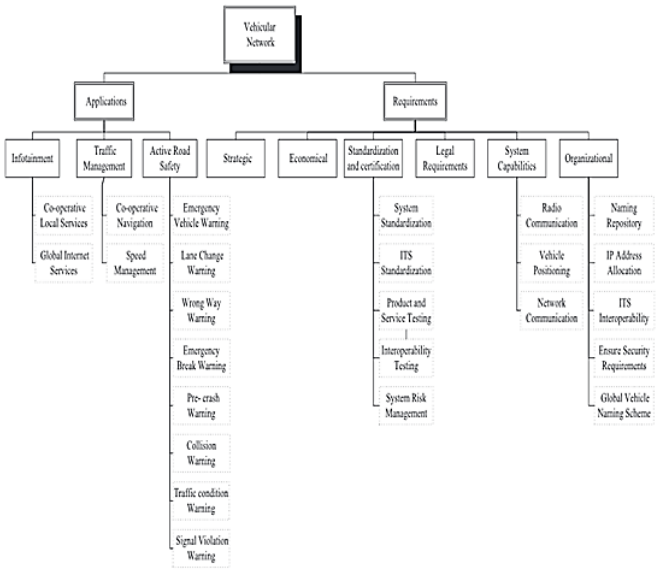

Figure. 1: Vehicular networking

We are motivated because the communication, storage and computing resources available in the vehicles are generally under-utilized. Combining these resources meaningfully will have a momentous influence on society. As such the underutilized vehicular resources including computing power, net connections and storage facilities can be pooled with those of other drivers on the road or rented to customers, similar to the way in which the resources of the present conventional cloud are provided. With current technology, Vehicular Clouds are technologically feasible and economically viable and will be the next paradigm shift. They will provide many benefits, including societal and technological impacts. The idea of a Vehicular Cloud and our emphasis is on the prospective applications and significant aspects of research challenges.

II. VEHICULAR NETWORK

For the last few years, smarter vehicles, safer, and less stressful driving experiences have been realized. Currently, ordinary vehicles have devices such as GPS, radio transceiver, small-scale collision radars, cameras, on board computers and different types of sensing devices to alert the driver to all types of road safety conditions and mechanical malfunctions. Vehicles are becoming more sophisticated with on-board storage, powerful on-board computing capabilities, significant communication capabilities and less power limitations, which are supported by hosts of sensors, actuators, on board radar and GPS

III. VEHICULAR CLOUD COMPUTING ARCHITECTURE

The Vehicular cloud computing architecture relies on three layers: inside-vehicle, communication and cloud. As illustrated in Fig. 4 , the first layer is the inside-vehicle layer, which is responsible for monitoring the health and mood of the driver and collecting information inside the car such as pressure and temperature by using body sensors, environmental sensors, smart phone sensors, the vehicle's internal sensors, inertial navigation sensors (INS), and driver behavior recognition

to predict the driver's reflexes and intentions. Then, the information collated via sensors should be sent to the cloud for storage or for use as input for various software programs in the application layer, for example, delivers health and environmental recognition applications. We assume that each vehicle is equipped with an OBU that including a built-in navigation system, with a map and the location of a RSUs. The OBUs have a broadband wireless communication to transfer data through 3 G or 4 G cellular communication devices, Wi-Fi, WiMAx, Wireless Access in Vehicular Environment (WAVE)

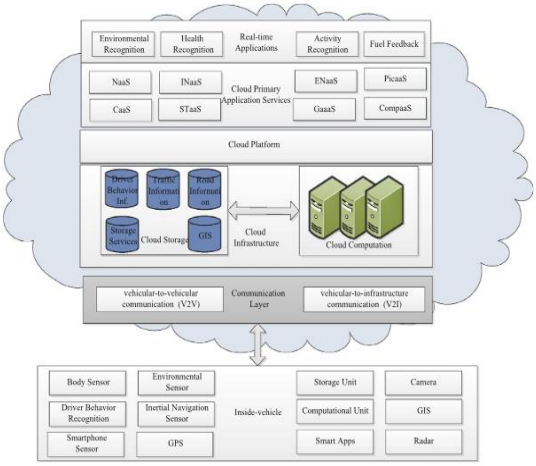

Figure 2 : VCC Architecture

IV. SECURITY OF VEHICULAR NETWORKS

A vehicular network is one of the most important technologies to implement different applications related to vehicles, traffic, and safety. There are several challenges that threaten
the security of vehicular networks. Providing security in a vehicular network is more difficult than in other networks such as WSN due to the high mobility and wide range of vehicles ,the security challenges of vehicular networks can be classified into five parts, namely, confidentiality, authentication, non-repudiation, localization and verification of data. For example, non-repudiation is the assurance that entities cannot deny receiving or sending a message that originated from them.

V. SECURITY CHALLENGES

- **Authentication**

The authentication in VC contains verifying the authentication of users and the integrity of messages. There are some studies to overcome this challenge in vehicular network such as “Probabilistic Adaptive Anonymous Authentication in Vehicular Networks ” is an authentication method for a vehicular network

- **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.

- **Vehicular public key infrastructure (VPKI)**

The wide ranges of vehicles that are registered in various countries are able to travel beyond their registration regions and require a robust key management scheme. The Vehicular Public
Key Infrastructure is one of the most important schemes to provide key management among vehicles, and it consists of three steps as follows.

Key assignment by Certificate Authorities (CAs): In this step, public and private keys are issued for each vehicle. Key assignment is generated based on a unique ID with an expiration period.

Key Verification(Authentication): In this step, the vehicle public key validation can be checked by CAs. When a vehicle i requests a public key from CAj, Pui will be issued by CAj as a public key for this vehicle. Then, CAj computes a certification (Ceri[Pui]) for this vehicle based on the vehicle public key and the ID of CAj as
follows:

Ceri½Pui = ¼PuijSignPrCAj(Pui|IDCAj)
Here, Ceri[Pui] is public key vehicle issued by CAj,PrCAj is the private key of CAj, the identity of CAj is shown by ID CAj and (Pui|IDCAj)
is signed by the private key of CAj.

- **Data security**

As mentioned in the previous section, VC provides an efficient way to exploit the utilized computation and storage resources of vehicles. Without considering the security restriction, the vehicles are able to access or alter the stored data on other vehicles. Therefore, the sensitive data that are stored in each vehicle should be encrypted (e.g., by the vehicle's private key) to protect it against the unauthorized access.

- **Network heterogeneity**

The vehicles usually have a large number of different on-board devices, including GPS, wireless transceivers, and on-board radar devices. The different vehicles are able to have a different combination of these on-board devices with different capabilities such as speed of processor, volume of memory, storage, and CPU capacity. Therefore, providing a security for these heterogeneous vehicles in VC environment is difficult because most of cryptographic algorithms are not lightweight and the vehicles need to have certain hardware conditions.

- **Access control**

Access control is a challenging aspect of the VC in which an identification of the user is checked before gaining access to the resources. In the VC, various access control levels are pre-defined and each user belongs to a specific cluster based on its role in the network

VI. CONCLUSION

We have reviewed and highlighted a recent concept of security measures of, Vehicular Cloud Computing, whose time has arrived. 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. We also advocate that, when fully realized and deployed, VCCs can lead to a significant enhancement in terms of safety, security and economic viability of our society. Thus, VCs could establish a large ad hoc federation to help mitigate many types of emergencies. In a planned or unplanned evacuation, there is possible damage to the mobile communication infrastructure, and federated VCs could help a decision support system and offer a temporary replacement for the infrastructure.

VII. REFERENCES

[1]. Abolfazli S, Sanaei Z, Ahmed E, Gani A, Buyya R. Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges. In: IEEE Communications Surveys and Tutorials, June 2013. http://dx.doi.org/10.1109/SURV. 2013.070813.00285 S , in press.

[2]. Abid H, Phuong LTT, Wang J, Lee S, Qaisar S. V-Cloud: vehicular cyber-physical systems and cloud computing. In: Proceedings of the 4th international symposium on applied sciences in biomedical and communication technologies. Barcelona, Spain: ACM; 2011. p. 1 - 5.

[3]. Aijaz A, Bochow B, Dötzer F, Festag A, Gerlach M, Kroh R, et al. Attacks on inter vehicle communication systems-an analysis; 2006.

[4]. Akbari Torkestani J. Mobility prediction in mobile wireless networks. Journal of Network and Computer Applications 2012;35:1633-45.

[5]. Al-Sultan S, Al-Doori MM, Al-Bayatti AH, Zedan H. A comprehensive survey on vehicular Ad Hoc network. Journal of Network and Computer Applications 2013

[6]. Alamri A, Ansari WS, Hassan MM, Shamim Hossain M, Alelaiwi A, Hossain MA. A survey on sensor-cloud: architecture, applications, and approaches. International Journal of Distributed Sensor Networks 2013;2013;1-18. http://dx.doi.org/10.1155/2013/917923S.

[7]. Alazawi Z, Altowaijri S, Mehmood R, Abdljabar MB. Intelligent disaster management system based on cloud-enabled vehicular networks. In: Proceedings of the 11th international conference on ITS telecommunications ITST). St. Petersburg; 2011. p. 361-8.

[8]. Anda J, LeBrun J, Ghosal D, Chuah CN, Zhang M. VGrid: vehicular adhoc networking and computing grid for intelligent traffic control. In: Proceedings of IEEE; 2005. p. 2905-9.

[9]. Arif S, Olariu S, Wang J, Yan G, Yang W, Khalil I. Datacenter at the airport: reasoning about time-dependent parking lot occupancy. IEEE Transactions on Parallel and Distributed Systems 2012;23:2067-80.

[10]. Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, et al. A view of cloud computing. Communications of the ACM 2010;53:50-8.

[11]. Baby D, Sabareesh RD, Saravanaguru RAK, Thangavelu A. VCR: vehicular cloud for road side scenarios. In: Meghanathan N, Nagamalai D, Chaki N, editors. Advances in computing and information technology. Berlin Heidelberg: Springer; 2013. p. 541 -52

[12]. Bilal SM, Bernardos CJ, Guerrero C. Position-based routing in vehicular networks: a survey. Journal of Network and Computer Applications 2013;36:685 -97

[13]. Blum JJ, Neiswender A, Eskandarian A. Denial of service attacks on inter-vehicle communication networks. In: Proceedings of the 11th international IEEE conference on intelligent transportation systems, ITSC'08 1; 2008. p. 797-802.

[14]. Boneh D, Shacham H. Group signatures with verifier-local revocation. In: Proceedings of 11th ACM conference on omputer and communications security. Washington, DC, USA: ACM; 2004. p. 168-77.

AUTHOR'S PROFILE

Jaida Khatoon Pursuing M.Tech from Shri Ramswaroop Memorial University (SRMU) Lucknow Completed B.tech from Buddha Institute of technology (UPTU),GIDA, Gorakhpur, in 2014. My Area of Interest is Vehicular Cloud Computing.