ISSN:2320-0790

An International Journal of Advanced Computer Technology

Security Scheme and Its Application towards Vehicular Computing

Maria baby[1], P. Bhuvaneshwari[2], Dr. S. Uma

[1]PG Scholar, Hindusthan Institute of Technology, Coimbatore

[2]Assistant Professor, Hindusthan Institute of Technology, Coimbatore

[3]Professor and Head, PG Department of Computer Science and Engineering, Hindusthan Institute of Technology, Coimbatore

Abstract: Cloud computing is a colloquial expression used to describe a variety of different types of computing that involves a large number of computers that are connected through real time communication network. Cloud computing is a ability to run a program on many connected computers at the same time. Another technology VANET uses moving car as nodes in a network to create a mobile network, allowing a car approximately 100 to 300 meters each other to connectand in turn, create a network with a wide range. Vehicular Computing is a similar toVANET, which have 2 types: infrastructure based VCand autonomous VC. This work is using infrastructure based VC; drivers will be able to access services by network communications involving the roadside infrastructure. Security challenges, which provides the most extensive analysis of the document in the public arena. Although security issues have received attention in cloud computing and vehicular network and identify security challenges that are specific to VCs. E.g.: challenges interface, tangled identifies and locations and the complexity of establishing trust relationships among multiple players caused by intermittent short- range communications. We provide a privacy and security in cloud computing in this paper for vehicular computing.

Keywords: Road-side infrastructure, Vehicular computing, short-range communication.

1. INTRODUCTION

Vehicle and roadside infrastructure with idle sophisticated onboard devices for long periods of time can be recruited to form a VC. A VC can be formed on the fly by dynamically integrating resources and collecting information. Vehicles can access the cloud and obtain, at the right time and the right place, all the needed resources and applications that they need or want.

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 security issues encountered in VCs may look deceivingly similar to those experienced in other networks. However, a more careful analysis reveals that many of the classic security challenges are exacerbated by the characteristic features of VCs to the point where they can be construed as VC-specific.

Cloud computing and its myriad applications that promise to change the way we think about computing and data storage have received a huge amount of attention. Cloud users do not need to install expensive hardware and software on their local machine.

In VANETs, the vehicles communicate with each other and/or with the roadside infrastructure using the Federal CommunicationsCommission-mandated DSRC, restricting the transmission range to 300–1000 m. There are two types of VANET networks: the zero-infrastructure and the infrastructure-based VANET. The zero-infrastructure VANET is created on-the-fly. 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), vehicles can be organized on-the fly to form VC in support of emergencies and other ad hoc events. The security challenges of a novel perspective of VANETs, i.e., taking VANETs to clouds.

2. LITERATURE SURVEY

The security challenges in VC are a new, exciting, and unexplored topic. Vehicles will be autonomously

pooled to create a cloud that can provide services to authorized users. This cloud can provide real-time services, such as mobile analytic laboratories, intelligent transportation systems, smart cities, and smart electric power grids. Vehicles 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.

Vehicular ad hoc network (VANET) security and privacy have been addressed by a large number of papers. Yan *et al.*, proposed activeand passive location security algorithms. Radar can be employed as a "virtual eye," andonboard 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 sender. 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*. Theiridea 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.

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. The Trust Center can evaluate the trust value of the cloud. Krautheim 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*. stated technical security issues of using cloud services on the Internet access.

A. ATTACKER MODEL IN VC

Traditional security systems are often designed to prevent attackers from entering the system. However, security systems in the VC have much harder timekeeping 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.

One possible form of attack is given below:
1) Find the geographic location of the target vehicle and physically move close the target machine;
2) narrow down the possible areas where the target user's services are executing by mapping the topology of VC;
3) Launch multiple experimental accesses to the cloud, and find out if the target user is currently on the same VM;
4) Request the services on the same VM where the target user is on;
5) Use system leakage to obtain higher privilege to collect the assets.

High mobility of vehicles is like a double-edged sword. It makes it hard for attackers to harm a specific target vehicle. First, the vehicle's access of each virtual machine can be transitory as vehicles constantly move from one district to another one, if each district is associated with a virtual machine. Additionally, attackers need to locate on which machine/infrastructure a specific target is located because all users in the VC are distributed on virtual machines.Third, the attackers must be physically co-located with the target user on the same physical machines.Finally, the attackers have to collect valuable information with certain privileges or with security tokens.

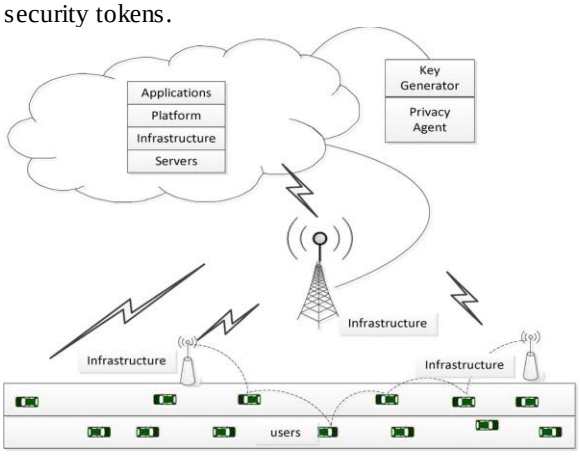

Fig.1.Vehicle often communicates through multi-hop routing.

B.KEY MANAGEMENT

1) Key Assignment and Rekeying: In VANETs, some organizations can serve as CAs: governmental transportation authorities, vehicle manufacturers, or nonprofit organizations. Initially, a vehicle will

receive a key pair from the manufacturer or some governmental authority. Key assignment is on the basis of a unique ID with a certain expiration time.
Upon expiration, the key pair has to be renewed at the local DMV/BMV. The renewal/expiration period can be the same period of vehicular state inspection, e.g., mandatory annual state inspection in many U.S. states.

2) Key Revocation: Key revocation is an important and effective way to prevent attacks. There are certain cases when key pairs will be exposed to attackers. It is obvious that an exposed key pair needs to be disabled. One of the advantages of PKI is that PKI can revoke a key pair. Vehicles will be aware that the exposed key pair has been revoked and refuse to communicate with vehicles with invalid key pairs. PKI uses certificate revocation lists (CRLs) to revoke keys. CRLs include a list of the most recently revoked certificates and are instantly distributed to vehicles. In VANETs, the infrastructures can serveas CRL distributors.

C.ESTABLISHING TRUST RELATIONSHIP

Trust is one of the key factors in any secure system. A trust relationship can exist in several ways. The network service providers and the vehicle drivers have access to trust. There will be a large number of government agents, e.g., the Department of Motor Vehicles (DMV) and the Bureau of Motor Vehicles (BMV) are trusted organizations. The relationship between the BMV and vehicle drivers is identity uniqueness and legitimacy.

In VCs, it is far more challenging to build trust relationships than in vehicular networks and conventional cloud computing.Many applications need multi-hop routing, with multiple nodes involved in communication. Therefore, the VC has inherited the challenge of establishing trust relationships among multiple vehicles, roadside infrastructure, service providers, network channels, and even the secret key generator. The VC cloud infrastructure is trusted, the VC service providers are trusted, the vast majority of VC users are trustworthy, and the attackers have the same privileges as normal users.

3. ALGORITHM

3.1 INTELLIGENT ALGORITHM

An intelligent algorithm will be applied to each scan result to predict the possibility of accidents.

4. CONCLUSION

This work planned to investigate the brand-new area and design solutions for each individual challenge and applications can be developed on Vc .It can be specific application will need to analyse and provide security solutions. It introduced the security and privacy challenges that VC computing networks have to face, and we have also addressed possible 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 Only with joint efforts and close cooperation among different organizations such as law enforcement, government, the automobile industry, and academics can the VC computing networks provide solid and feasible security and privacy solutions.

Extensive work of the security and privacy in VCs willbecome a complex system and need a systematic and syntheticway to implement intelligent transportation systems. Only with joint efforts and close cooperation among different organizations such as law enforcement, government, the automobileindustry, and academics can the VC computing networksprovide solid and feasible security and privacy solutions.

REFERENCES

[1] “Data centre at the airport: Reasoning about time-dependent parking lot occupancy,”IEEE Tans. ParallelDistrib. Sys., 2012.
[2] 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.
[3] 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.
[4] 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.
[5] F.-Y. Wang, “Parallel control and management for intelligent transportation system: Concept architectures, and applications,” IEEE Trans.Intell . Transp. Syst., vol. 11, no. 3, pp. 630–638, Sep. 2010.
[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.