Towards Secure Virtual Machine Migration in Vehicular Cloud Environment

Nkenyereye Lewis and Kyung Hyune Rhee

1Department of IT Convergence and Application Engineering, Pukyong National University, Republic of Korea
{nkenyele,khrhee}@pknu.ac.kr

Abstract. In Vehicular Cloud (VC), Storage as Service (STaaS) is different from other services in vehicle cloud environment for the fact that it involves the migration of virtual OBU to be used by a data center, thus requiring more security issues to be addressed. In this paper, we propose a Secure Virtual Machine Migration Protocol Steps which can achieve secure handling in vehicular environment. Based on a scenario of a parking lot where the RSU is considered as Group Manager and the vehicles group members, we argue that ID-based Encryption and group signature can achieve secure OBU VM-vTPM based migration in cloud environment.

Keywords. Vehicular cloud, virtual machine migration (VMM) and VM-vTPM.

1 Introduction

In Vehicular Cloud computing, the communication, storage and computing resources available in the vehicles are generally not fully utilized. Due to the small size and the inexpensive price of storage, it is projected that the on board unit of vehicles will have multiple Tera-bytes of storage which can be used for storage as a service in vehicular cloud by renting their capabilities to some vehicles or companies which require additional storage to run their applications [1]. The fundamental of cloud computing comprises virtualization of hardware resources such as storage, network and memory provided through virtual machine migration (VMM). Virtualization technology allows separation between operating systems from hardware on which they run using VMM trough a hypervisor, thus easing the transfer of VMs between different physical hosts. The combination of a hardware based root of trust such as Trust Platform Module (TPM) on virtual machine based system have being widely adopted in IT industry. A virtual TPM (vTPM) can run in a separate VM, inside its corresponding VM or in the hypervisor such as Xen hypervisor [5]. In vehicular cloud environment, migrating on board unit (OBU) virtual machine brings in other security concerns such as the privacy and security of the vehicle’s owner. The key contributions of this work include, first the description of specific scenario by which secure OBUs virtual machine migration can be beneficial, second we describe the security requirements of
secure OBUs VMM and finally we propose an approach to achieve the security requirements in such scenario.

2 Application Model

Several research including Olariu et al.’s have proposed Vehicular Cloud Computing services, formation perspective and applications [1] but customized scenarios for hiring vehicles storage capacities as a data center has gotten little attention the literature. The authors in [1] confirmed that many parking lot in places such as airports, malls avail excessive computing and storage capabilities which can used by data centers as remote collocated servers, or companies around those places to run their applications. As described in the figure 1, data center can make use of a RSU as a remote collocated sever where by which the RSU recruits vehicles to avail their storage capacities. Our concern in this paper is to provide a secure protocol for migrating OBUs virtual machine to the Group Manager in order to be used by the data center. We consider the case of a parking lot whose probability of vehicles duration have been confirmed such as [1], then the RSU will send a message to vehicles entering the parking to avail their storage capacities. Each vehicle would join or leave the group as it enters the parking.

![Parking based Data Center Scenario](image)

Fig. 1. Parking based Data Center Scenario.
3 Security Requirements

Our goal is to design a secure scheme that provide OBUs Virtual Machine Migration to the Group Manager (RSUj) to be used by a Data Center to satisfy the following security requirements:

- **Identity privacy preserving of vehicles**: The real identity of a vehicle availing its storage capacity to a datacenter through the RSU should be kept anonymous from other vehicles in the group as well as from RSU which is the group manager.
- **VM integrity and authentication**: Each vehicle should be authenticated before it can issue a request to join a group of vehicles availing their storage capacities and communication between RSU and vehicles must be verified.
- **The migration of the VM-vTPM must be protected during the transmission and no one can modify VM or vTPM without being detected.**
- **Unlinkability**: The Group Manager (RSU) will be able to know if a group signature on the transmission of VM-vTPM was computed by the same group member.
- **Exculpability**: Neither RSU nor a vehicle can sign messages on behalf of other vehicle in the parking. Also, the RSU together with other vehicles in the parking cannot transfer the responsibility of any group signature to any member.
- **Traceability**: Though real identity of a group member should be hidden from other vehicles and RSUs, TA should have the ability to obtain a vehicles real identity so that the vehicle owner can be paid for availing its storage capacity for the Data Center. Also TA is able to provide proofs in case of disputes.

4 Proposed Approach

In this section, we present our approach to secure virtual machine migration in vehicular cloud. When we describe our approach, we make the following assumptions and consider ID-based encryption with pseudonym [6] and group signature scheme [2] to cope with the aforementioned security requirements.

- We consider a public key infrastructure (PKI) for initial vehicles and RSU authentication. Each vehicle \( vi \) has a conventional pseudonym based public key \( PIDi \) and a conventional private key \( VSKi \) and is given a TA_signed certificate \( Certv \); RSUs which act as group manager have a simple public key, private key and a TA signed certificate \( RSUj \); \( VRSUj \) and \( Cert_{RSU} \) respectively.
- Parking lots are equipped with sensor to inform RSU when a new vehicle enters the parking so that the RSU can broadcast a hello message to the vehicle.
- All vehicles have a tamper proof device(OBUs) equipped with a Trust Platform Module ver 2.0, with a several tera-bytes of hard disk and are running a same operating system.
Such as other server racks in the data center, RSUs are equipped with several server racks on which are installed type I hypervisor such as Xen [4]. RSU is considered as a remote server of the data center.

Data Center is a company which offers storage as a service such as Pacnet Seoul. The communication between the data center and RSU is secure. We consider a hypervisor based VM-vTPM system such as of [4].

Suppose RSU receives a message from the sensor that a vehicle is entering the parking:

RSU broadcast based on the sensor installed on the entrance of the parking, a request to use \( v_i \) storage, then \( v_i \) request to be a member of the group headed by RSU.

RSU verifies the certificate of \( v_i \) and sends a request to TA in order to generate part of member group public key and private key.

TA verifies the message sent by RSU and generates part of the group public key and private key for \( v_i \).

RSU verifies the message sent by TA and generate the rest of public and private group keys for \( v_i \) and send the message to \( v_i \).

\( v_i \) verifies the message from RSU and generate a group signature for his vehicle virtual machine migration with his pseudonym identity.

5 Conclusion

In this paper we presented a protocol towards a secure OBU virtual machine migration based on vehicular cloud which can bring be beneficial for the full usage of OBU storage capabilities. Using ID based encryption with group signature can suite a scenario such a parking based data center for a VM-vTPM based migration. In future, we shall fully describe the protocol and evaluate it based on the computation time and simulation.

Acknowledgement. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A4A01009848).

References