A Privacy Preserving V2I Service Access Management System for Vehicular Clouds

Youngho Park[1], Chul Sur[2], and Kyung-Hyune Rhee[1]*
[1]Pukyong National University, Busan, Republic of Korea
{pyhoya, khrhee}@pknu.ac.kr
[2]Busan University of Foreign Studies, Busan, Republic of Korea
kahlil@bufs.ac.kr

Abstract

Vehicular cloud computing is a technological paradigm shifting which takes advantage of cloud computing to provide vehicles with useful computing resources and services. With the rapid advancement of intelligent vehicles and Intelligent Transportation System infrastructures, some researches on the literatures have put forth a vision of the combination of vehicular network with could computing in recent. However, little efforts have concentrated on security features for vehicular cloud services. In particular, privacy is one of the critical security issues in vehicular cloud as well as vehicular communications since a third-party entity may be involved in cloud service management and operations. In this paper, we design a privacy preserving vehicle-to-infrastructure cloud access management system in which neither global eavesdropper nor any single system management entity can trace a vehicle for service provision. We make use of pre-loaded pseudonyms to generate anonymous service access tokens for vehicles and RSU local revocation check to reduce the size of revocation list in the system.

Keywords: vehicular cloud, vehicular network, vehicle-to-infrastructure, privacy preservation

1 Introduction

For the last decade, Vehicular Ad Hoc Networks (VANETs) have received lots of attentions and research efforts have been devoted to vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. The promise of emerging vehicular networking technologies has led to convergence with Intelligent Transportation System (ITS) and new types of applications ranging from driving safety and convenience to entertainment services. With support of vehicular communications, vehicles can not only prevent roadway crashes through safety application and make a driving plan from realtime traffic conditions but also access to remote server on the Internet through roadside units (RSUs).

Furthermore, the rapid advances in intelligent vehicles and information technologies in recent motivate researchers to investigate a new paradigm of vehicular cloud computing. Vehicular cloud computing is a conceptual paradigm shifting which takes advantage of cloud computing to provide vehicles (or drivers) with useful computing resources and services, and a few researches have put forth the vision of the combination of vehicular network with cloud computing [2, 1, 11, 18, 8]. Keeping up with this trend, some major car companies in collaboration with IT companies introduce their conceptual car-cloud service models through the Internet. Therefore, we can expect that vehicular cloud computing is natural technological shifting in the near future. However, little efforts have concentrated on security features for cloud-based vehicular networking services, but the authors proposed a privacy preservation protocol for secure navigation on vehicular cloud [16].

Research Briefs on Informaiton & Communication Technology Evolution (ReBICTE), Vol. 1, Article No. 6 (January 15, 2015)
*Corresponding author: Department of IT Convergence and Application Engineering, Pukyong National University, Busan, Republic of Korea, Tel: +82-51-629-6247

In particular, privacy is one of the critical security issues in vehicular cloud services as well as vehicular communications since a third-party entity may be involved in cloud management and operations. From application viewpoint, when we consider that vehicular cloud services are served on vehicular networks, vehicular cloud computing can inherit some security defenses from the existing VANET-based security mechanisms on one hand. In the meantime, a variety of researches on privacy preservation in VANET-based application have been proposed [13, 9, 14, 10, 12, 15]. Most of the existing conditional privacy preservation protocols in vehicular networks are implemented by using a pseudonym-based technique [13, 15] or using a group signature scheme [9, 10]. Group signatures can be used to build conditional privacy preservation, however, the signature size and computation cost are relatively long and high. In pseudonym-based techniques, a vehicle possesses a lot of unlinkable pseudonym certificates traced by only a trusted authority and frequently changes its pseudonym to avoid tracking, but the size of revocation list gets long proportional to the number of pseudonyms used in the system. Another problem in most of pseudonym-based techniques is to put a single authority or single traceable entity in the system in which the entity may be a security breach of inside attack to leak sufficient information.

In this paper, we propose an anonymous service access management system in cloud-based vehicular networks to allow legitimate vehicles to connect to cloud service focusing on a V2I communication with RSUs. More specific, we design a system based on anonymous service access tokens to prevent vehicles (or drivers) privacy from not only outsiders but also inside system management entities while the vehicles access cloud site through RSUs on the roads. In the proposed system, we basically make use of pseudonyms for anonymous access to V2I cloud service, but we remedy the problem of a single management entity and devise RSU local revocation lists to reduce the size of revocation list. The remainder of this paper is organized as follows. We briefly present a cloud-based vehicular network model in Section 2 and outline the system architecture in Section 3. The operations of the proposed system is presented in Section 4. We discuss the proposed system in Section 5, and finally conclude this paper in Section 6.

2 Background

Before presenting the proposed system architecture, in this section, we briefly show the abstraction of vehicular cloud computing considered in the paper. With the development of electronic devices and information technologies for intelligent vehicles and transportation infrastructures, a few researches have presented the strategy for effective resource management to deploy vehicular cloud computing [18, 8, 11]. We consider the cloud-based vehicular network architecture of [18] shown in Figure 1 as our V2I cloud service application at a high level. The formation of vehicular cloud network is divided into roadside cloud among a set of RSUs and central cloud in the Internet.

- Roadside cloud is a local cloud site established among a set of RSUs and dedicated local servers. Roadside cloud is locally accessible only to nearby vehicles passing through the radio coverage of the RSUs. Such roadside cloud can collect and provide local-interesting information services to vehicles through the RSUs such as traffic condition and available parking lot, etc.

- Central cloud is a set of interconnected and virtualized computing resources in parallel and distributed fashion in the Internet to provide complicated computation, massive data storage, and a variety of platforms. A vehicle can access a central cloud by V2I connection through RSUs on the roads.

Note that a pervasive V2I cloud environment integrating ITS infrastructures and efficient cloud resource management strategies to deal with vehicle mobility are required to implement vehicular cloud

services. However, the details of such cloud configurations and resource management are beyond the scope of this paper but we can refer to [18].

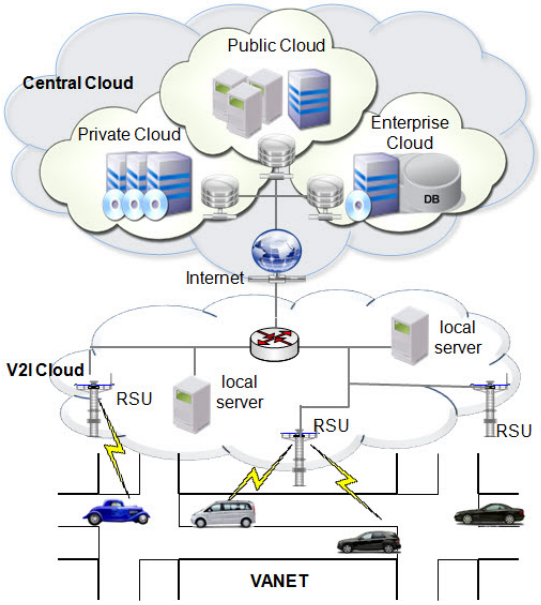

Figure 1: Cloud-based vehicular networking architecture.

3 System Model

3.1 Architecture

To provide privacy preserving V2I cloud access on VANETs, we consider a security credential management system architecture which consists of master authority (MA), transportation manager (TM), service manager (SM), and road side units (RSUs) deployed on the roads as shown in Figure 2. The detailed role of each system component is as follows:

- MA is responsible for registering vehicles and managing cryptographic parameters for all entities in the system to generate anonymous V2I cloud service access tokens. Each vehicle registers its alias to the MA, and the alias will be used in service enrollment to the SM instead of real identity.
- TM is in charge of the registration of RSUs and generates service access tokens which guarantee the privilege of vehicle's V2I cloud service access to the RSUs. That is, a vehicle obtaining access tokens bound with RSUs can connect to V2I cloud service provided by the RSUs on the system.
- SM handles the requests of vehicles service enrollment and mediates not only generating anonymous service access tokens for the requesting vehicles but also revoking pseudonyms of misbehaving vehicles in the system.
- RSUs installed on the roadside are subordinated to the TM, and a set of adjacent RSUs configures local cloud in which dedicated local cloud servers are attached to the RSUs. After checking the validity of V2I service access tokens given by vehicles, RSUs provide legitimate vehicles with locally interesting service processed in the local cloud or allow the vehicles to connect to the Internet for accessing central cloud service.

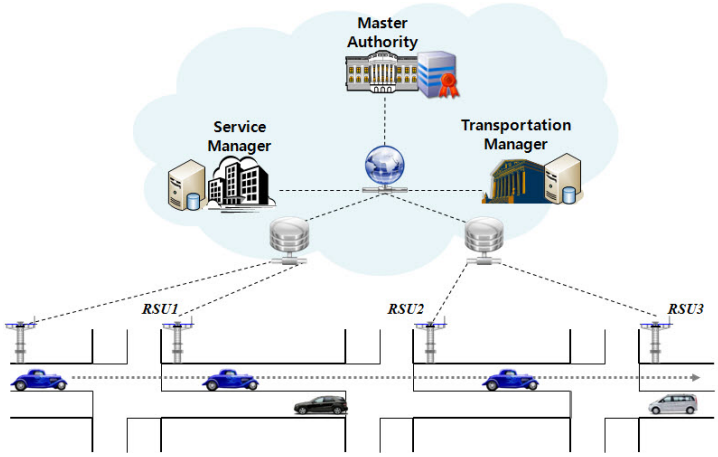

Figure 2: System architecture.

In addition, we make the following assumptions in order to clarify our system model :

- MA, TM, and SM are interconnected through fixed secure channel with reliable communication links without packet loss. They are trustable to each other so that they do not cheat the messages sent to other management entities.
- Each RSU is bootstrapped with its own public and private key pair protected by some security techniques such as tamper proof module [13].
- TA can inspect all RSUs so that RSUs will not disclose any inner information without the authorization of the TM.
- Vehicles equip with on-board unit (OBU) incorporated with embedded computer, wireless network interface, GPS receiver, car navigation system, and digital maps.
- Public system parameters configured by the MA for cryptographic operations are already known to all system components, and vehicles store public keys of MA, TM, and SM in their OBUs.

3.2 Security Considerations

Since most privately owned vehicles can be regarded as personal devices, the system should be designed to make tracking vehicles hard. To design a privacy preserving V2I service access management system, we consider the following security objectives.

- *Authentication and Authorization* : Only a legitimate vehicle which has service access rights should access V2I cloud service through RSUs in the system.
- *Identity Privacy* : The real identity of a vehicle should be kept secret from outsiders (or other vehicles) as well as system components for privacy preservation during the service provision.
- *Unlinkability* : It should be difficult for eavesdroppers to tell whether two messages captured at physically different locations is sent from the same vehicle.
- *Traceability* : The system should have the ability to reveal the real identity of a misbehaving vehicle in case of suspicious events.

In our system architecture, we consider two types of attacks to the privacy of vehicles accessing to V2I cloud service through RSUs on the roads.

- One is attack on vehicle's privacy from global eavesdroppers which can capture any message transmitted on VANETs.
- The other is insider attack on vehicle's privacy from a system management entity.

In general, one basic idea to prevent any management entity from gathering sufficient information to track vehicles is to organizationally separate the functionalities of the system among different entities [7, 17]. Even though anonymous service access tokens are managed by the system components in our system, any single entity (MA, TM, or SM) should not be capable of revealing the real identity of a vehicle from a pseudonym in normal operations. Therefore, all system components need to collude to gain enough information to trace a vehicle.

4 Proposed V2I Cloud Access Management System

In this section, we design a privacy preserving V2I service access management system using anonymous service tokens. In our system, in brief, each vehicle registering its service alias to the MA selects some RSUs, to which the vehicle wants to connect on driving, and pseudonyms to be used in V2I service through each RSU. A vehicle requests service access tokens for its pseudonyms to the SM by the service enrollment procedure. SM forwards the requesting vehicle's pseudonyms to the TM, then TM returns service access tokens generated from the pseudonyms bound with RSUs. Obtaining the service access tokens, each vehicle can authenticate itself to RSU for V2I service access on VANETs. In the proposed system, however, SM does not know which RSUs the requesting vehicle will visits and TM does not know actual pseudonyms which the requesting vehicle will use in each RSU's service. Table 1 shows the notations used in describing the proposed system.

Table 1: Notations and descriptions.

notation	description
sk_i, pk_i	private and public key pair of an entity i
SK_{id}	ID-based private key for the given id
vid_i	i-th vehicle V_i's real identity
$alias_i$	alias of V_i for service enrollment
$PIDL_i$	pseudonym list of V_i used in V2I service access
BIL_i	blinded pseudonym list of V_i
RSU_j	j-th road-side unit identity
$Enc_k()$	encryption under key k
$Dec_k()$	decryption under key k
$idSig_{SK_{id}}()$	ID-based signature under the SK_{id}
$idVrf_{id}()$	ID-based signature verification for a given id

4.1 Setup

In our system, service access token generation is a variant of identity-based cryptographic primitives using bilinear maps. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be the bilinear map groups [3] with the same prime order q, and P be a generator of $\mathbb{G}_1$, respectively.

1. MA chooses a random $a \in \mathbb{Z}_q^*$ as its master secret key, computes the corresponding public key $P_A = aP$, and configures system parameters $params = \{\mathbb{G}_1, \mathbb{G}_2, q, \hat{e}, P, P_A, H_1\}$, where $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is a bilinear map, $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$ is a cryptographic hash function, respectively. The *params* are publicly known to all entities in the system.

2. For vehicles registration to the MA, each vehicle V_i with vid_i chooses its $alias_i$ and gives $\langle vid_i, alias_i \rangle$ to the MA. Then, MA provides $SK_i = aH_1(alias_i)$ to V_i and stores $\langle vid_i, alias_i \rangle$ lists. The $alias_i$ of V_i will be used in V_i's service enrollment phase to the SM instead of real identity.

3. TM and SM choose $t \in \mathbb{Z}_q^*$ and $s \in \mathbb{Z}_q^*$ as their secret keys and publish the corresponding public keys $P_T = tP$ and $P_S = sP$, respectively.

4.2 Enrollment

In order for a vehicle to get V2I cloud access service through RSUs, each vehicle should be enrolled to the SM for vehicle's desired service and obtain service access tokens.

1. A vehicle V_i selects RSUs on its travel routes (eg. daily driving path between home to work) and configures ordered RSU list $Path_i = \{RSU_1, ..., RSU_n\}$ and V_i's pseudonyms list $PIDL_i = \{pid_1, ..., pid_n\}$ which will be used in access to RSU's service (i.e., pid_l is used in RSU_l's service).[1] V_i selects a random $r \in \mathbb{Z}_q^*$ and computes rP, $X = SK_i + rH_1(alias_i)$, blinded pseudonyms list $BIL_i = \{BI_1, ..., BI_n\}$ where $BI_l = rH_1(pid_l)$ $(1 \leq l \leq n)$, and then sends the following enrollment request message to the SM:

   $$req = \{Enc_{pk_{SM}}(alias_i, k), rP, X, Enc_{pk_{MA}}(PIDL_i), Enc_{pk_{TM}}(Path_i), BIL_i, ts\}, idSig_{SK_i}(req)$$

   where ts is the timestamp and k is a symmetric key which will be used for SM to give encrypted service access tokens to V_i later. By encrypting RSUs list as $Enc_{pk_{TM}}(Path_i)$, V_i hides its travel path from SM so that SM cannot know which RSUs the requesting vehicle will connect to.

2. Upon receiving V_i's request, SM first decrypts the $Enc_{pk_{SM}}(alias_i, k)$ and checks the validity of the $alisa_i$ as $\hat{e}(X,P) = \hat{e}(H_1(alias_i), P_A)\hat{e}(H_1(alias_i), rP)$ using MA's public key P_A and then verifies $idSig_{SK_i}(req)$ using the $alias_i$ [5, 6]. The correctness of the checking $alias_i$ can be shown as follows:

$$\begin{aligned}
\hat{e}(X,P) &= \hat{e}(SK_i + rH_1(alias_i), P) \\
&= \hat{e}(SK_i, P)\hat{e}(rH_1(alias_i), P) \\
&= \hat{e}(aH_1(alias_i), P)\hat{e}(H_1(alias_i), rP) \\
&= \hat{e}(H_1(alias_i), aP)\hat{e}(H_1(alias_i), rP) \\
&= \hat{e}(H_1(alias_i), P_A)\hat{e}(H_1(alias_i), rP)
\end{aligned}$$

   If it holds, SM computes enrollment transaction tag for V_i as $tag_i = hash(req, idSig_{SK_i}(req))$ and then sends $\{BIL_i, Enc_{pk_{TM}}(Path_i), tag_i\}$ to the TM.

3. TM decrypts $Enc_{pk_{TM}}(Path_i)$ to obtain the demanded RSUs list $Path_i = \{RSU_1, ..., RSU_n\}$ of V_i and computes tokens $TRL_i = \{TR_1, ..., TR_n\}$ from $Path_i$ and $TBL_i = \{TB_1, ..., TB_n\}$ from the BIL_i where $TR_l = tH_1(RSU_l)$ and $TB_l = tBI_l = t(rH_1(pid_l))$ $(1 \leq l \leq n)$, respectively. TM returns $\{TRL_i, TBL_i\}$ to the SM and stores $\langle tag_i, \{RSU_1, ..., RSU_n\} \rangle$.

[1] We assume that the selection of RSUs would be possible because modern vehicles can equip with navigation system with digital maps.

4. SM computes daily access token $DT = sH_1(service|date)$, where *service* means the service provided by the SM and *date* is the current date, and encrypts the tokens as $CT = Enc_k(TRL_i, TBL_i, DT)$. SM provides $\{CT, Sig_{sk_{SM}}(CT)\}$ to V_i and sends $\{alias_i, Enc_{pk_{MA}}(PIDL_i), tag_i\}$ to the MA, then MA will store $\langle alias_i, tag_i, \{pid_1, ..., pid_n\}\rangle$ after decrypting $Enc_{pk_{MA}}(PIDL_i)$.

5. When receiving $\{CT, Sig_{sk_{SM}}(CT)\}$ from the SM, V_i verifies $Sig_{sk_{SM}}(CT)$ using SM's public key pk_{SM}. If it holds, V_i recovers $\{TBL_i, TRL_i, DK\}$ by $Dec_k(CT)$ and computes access token AT_l to each $RSU_l \in \{RSU_1, ..., RSU_n\}$ on its travel routes as follow:

   $$AT_l = r^{-1}TB_l + TR_l + DT = tH_1(pid_l) + tH_1(RSU_l) + sH_1(service|date)$$

   V_i maintains pseudonyms and access tokens list for each RSU as $\langle RSU_l, pid_l, AT_l\rangle$ $(1 \leq l \leq n)$.

4.3 V2I Service Access

When a vehicle V_i passes through an RSU_l's service area and wants to access desired service, V_i can anonymously authenticate itself to the RSU_l using the access token AT_l as follows:

1. V_i retrieves (pid_l, AT_l) pairs for the RSU_l from its tokens list, chooses a random $x \in \mathbb{Z}_q^*$ and computes xP. V_i constitutes a service request message $srv\_req = \{service, Enc_{pk_{RSU_l}}(pid_l), xP\}$ and sends $\{srv\_req, \sigma\}$ to RSU_l, where *service* means the service description which the vehicle wants to receive and $\sigma = AT_l + xH_1(srv\_req)$ is the signature using the access token AT_l [6].

2. Upon receiving the service request message, RSU_l decrypts $Enc_{pk_{RSU_l}}(pid_l)$ using its private key to obtain V_i's pseudonym pid_l and checks the revocation lists distributed by the SM for the current date service period. If pid_l does not appear in the revocation list, then RSU_l verifies the signature σ as $\hat{e}(P, \sigma) = \hat{e}(P_T, H_1(pid_l))\hat{e}(P_T, H_1(RSU_l))\hat{e}(P_S, H_1(service|date))\hat{e}(xP, H_1(srv\_req))$. The correctness of the verification can be shown as follows:

$$\begin{aligned}
\hat{e}(P, \sigma) &= \hat{e}(P, AT_l + xH_1(srv_req)) \\
&= \hat{e}(P, AT_l)\hat{e}(P, xH_1(srv_req)) \\
&= \hat{e}(P, tH_1(pid_l))\hat{e}(P, tH_1(RSU_l))\hat{e}(P, sH_1(service|date))\hat{e}(P, xH_1(srv_req)) \\
&= \hat{e}(tP, H_1(pid_l))\hat{e}(tP, H_1(RSU_l))\hat{e}(sP, H_1(service|date))\hat{e}(xP, H_1(srv_req)) \\
&= \hat{e}(P_T, H_1(pid_l))\hat{e}(P_T, H_1(RSU_l))\hat{e}(P_S, H_1(service|date))\hat{e}(xP, H_1(srv_req))
\end{aligned}$$

   If it holds, RSU_l accepts V_i's request and allows to connect to V2I cloud service.

4.4 Revocation and Tracing

Even though an anonymous authentication is indispensable for privacy preservation, when suspicious events occurs it is required to track misbehaving vehicles and revoke access tokens in order to deny the misbehaving vehicles' service access. In our proposed system, MA, TM, and SM are involved in tracking a real identity from a suspicious vehicle's pid_l as follows:

1. If pid_l of a misbehaving vehicle is detected, SM first reports pid_l to the MA.

2. MA searches its database storing $\langle alias_i, tag_i, \{pid_1, ..., pid_n\}\rangle$ lists in enrollment phase to find the $alias_i$ and tag_i matching to $pid_l \in \{pid_1, ..., pid_n\}$. MA can retrieve the real identity vid_i matching to $alias_i$ from $\langle vid_i, alias_i\rangle$ lists, and adds $alisa_i$ to system blacklist so that SM does not accept enrollment request from the $alias_i$ any more. Then, MA returns tag_i and $\{pid_1, ..., pid_n\}$ to SM.

3. SM can make a revocation list for the current service date period by appending all $\{pid_1, ..., pid_n\}$ and distribute the revocation list to all RSUs. Even though this approach is simple, the size of revocation list is proportional to the number of revoked *pid*s in the system. To reduce the size of revocation list, we adopt another approach in which distributes local revocation list to each RSU. SM requests TM to return RSU lists $\{RSU_1, ..., RSU_n\}$ matching to tag_i and, from $\{RSU_1, ..., RSU_n\}$ and $\{pid_1, ..., pid_n\}$ pairs of tag_i, provides each RSU_l with a local revocation list RL_l containing only *pid*s related to each RSU_l.

5 Security

We design a privacy preserving authentication mechanism for V2I service access through RSUs local sites. In this section, we discuss the security of the proposed system.

- *Authentication and Authorization* : For a vehicle V_i to access RSU_l's cloud site, V_i must authenticate itself to the RSU_l by using service access token $AT_l = tH_1(pid_l) + tH_1(RSU_l) + sH_1(service|date)$ issued in enrollment phase. A service access token AT_l is computed from the guarantees of TM's and SM's signatures [4] for the given pid_l used at RSU_l for the current service period, and this token is issued to only a legitimate vehicle validated by the SM in service enrollment phase. Unregistered vehicle cannot generate a valid service access token without forging TM's and SM's signature. Therefore, no vehicle can be authenticated and illegally connect to RSU's service site unless the vehicles obtain service access tokens in service enrollment.

- *Identity Privacy* : In the proposed system, an attacker cannot obtain vehicle's real identity from eavesdropping on vehicle's transmissions for service enrollment and V2I service access through RSUs. For a vehicle V_i, instead of using the real identity, V_i uses $alias_i$ for service enrollment to the SM and pid_l for accessing to RSU_l's service, which are encrypted under SM's and RSU_l's public key, respectively. Therefore, the attacker cannot directly infer the real identity from eavesdropping on the protocol. Moreover, even if the attacker can compromise SM or RSUs, neither the compromised SM nor RSUs can reveal the real identity from $alias_i$ and *pid*s without the help of the MA because SM and RSUs do not have identity matching information. In addition, to hide the actual *pid*s, since blinded pseudonyms by the V_i in the form of $rH_1(pid_l)$ are given to the TM for generating service access tokens from V_i's pseudonyms and RSUs list, TM cannot know V_i's pseudonyms used in V2I service access assuming the discrete logarithm problem on elliptic curves is hard.

- *Unlinkability* : When we assume the attack of global eavesdroppers which can observe any messages transmitted in VANETs, the attackers may try to find whether any two messages observed in different RSUs service range are sent by the same vehicle to track the moving location of the vehicle. In the proposed system, when a vehicle connects to RSU_j's site for V2I service access, the vehicle sends its pseudonym pid_j encrypted with RSU_j's public key and signature generated by the access token AT_j valid in only RSU_j's site which do not contain any plain identity related information. Therefore, it is hard for the attacker to tell that two messages observed at RSU_j's and RSU_k's sites were originated from the same vehicle. Consequently, no single management entity can track a vehicle accessing V2I cloud service in normal operations due to the identity privacy and unlinkability.

- *Trace and revocation* : Even though it is hard for a single management entity to track the identity of a vehicle in normal operations, it is possible not only to trace the real identity but also to revoke pseudonyms of a misbehaving vehicle in collaboration with all system components when

suspicious events occur. If a *pid* of a suspicious event is reported by RSUs, all management entities are involved in tracing and revocation procedures in the way that, from the reported *pid*, MA searches matching pseudonym in $\langle alias_i, tag_i, \{pid_1, ..., pid_n\}\rangle$ lists and reveals the real identity of the *alias* in $\langle vid_i, alias_i\rangle$ lists, and TM returns RSUs list $\{RSU_1, ..., RSU_n\}$ relating to the *pid*. Then, SM updates RSU local revocation list from $\{pid_1, ..., pid_n\}$ and $\{RSU_1, ..., RSU_n\}$ pairs and distributes the revocation list to each RSU.

6 Conclusion

In this paper, we designed a privacy preserving vehicle-to-infrastructure service access management system for vehicular cloud based on anonymous service access tokens. Even though the service access tokens are derived from vehicle's pseudonyms making use of identity-based cryptographic primitives, neither outsiders nor any single management entity can track a vehicle for the service provision. Moreover, the proposed system can reduce the size of revocation list by devising RSU local revocation lists in which the entries are not the whole revoked pseudonyms but limited to pseudonyms bound with each RSU.

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

[1] Hassan Abid, Luong Thi Thu Phuong, Jin Wang, Sungyoung Lee, and Saad Qaisar. V-cloud: vehicular cyber-physical systems and cloud computing. In *Proc. of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL'11), Barcelona, Spain*, pages 165:1–165:5. ACM, 2011.

[2] Mahmoud Abuelela and Stephan Olariu. Taking vanet to the clouds. In *Proc. of the 8th International Conference on Advances in Mobile Computing and Multimedia (MoMM'10), Paris, France*, pages 6–13. ACM, 2010.

[3] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Advances in Cryptology - CRYPTO 2001, LNCS*, volume 2139, pages 213–229. Springer, August 2001.

[4] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In *Advances in Cryptology - ASIACRYPT 2001, LNCS*, volume 2248, pages 514–532. Springer, December 2001.

[5] Jae Cha Choon and Jung Hee Cheon. An identity-based signature from gap diffie-hellman groups. In *Public Key Cryptography - PKC 2003, LNCS*, volume 2567, pages 18–30. Springer, December 2002.

[6] Craig Gentry and Alice Silverberg. Hierarchical id-based cryptography. In *Advances in Cryptology - ASIACRYPT 2002, LNCS*, volume 2501, pages 548–566. Springer, December 2002.

[7] Taekyoung Kwon, Jung Hee Cheon, Yongdae Kim, and Jae-Il Lee. Privacy protection in pkis: A separation-of-authority approach. In *Information Security Applications, LNCS*, volume 4298, pages 297–311. Springer, 2007.

[8] Euisin Lee, Eun-Kyu Lee, Mario Gerla, and Soon Y. Oh. Vehicular cloud networking: Architecture and design principles. *IEEE Communications Magazine*, 52(2):148–155, February 2013.

[9] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, and Xuemin Shen. Gsis: A secure and privacy preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology*, 56(6):3442–3456, November 2007.

[10] Rongxing Lu, Xiaodong Lin, Haozin Zhu, Pin-Han Ho, and Xuemin Shen. Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications. In *Proc. of the 28th IEEE International Conference on Computer Communications (INFOCOM'08), Phoenix, AZ, USA*, pages 1229–1237. IEEE, April 2008.

[11] Stephan Olariu, Tihomir Hristov, and Gongjun Yan. The next paradigm shift: From vehicular networks to vehicular clouds. *Mobile Ad Hoc Networking: The Cutting Edge Directions*, pages 645–700, 2013.

[12] Youngho Park, Chul Sur, Chae-Duk Jung, and Kyung-Hyune Rhee. An efficient anonymous authentication protocol for secure vehicular communications. *Journal of Information Science and Engineering*, 26(3):785–800, May 2010.

[13] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, January 2007.

[14] Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran. Amoeba: Robust location privacy scheme for vanet. *IEEE Journal on Selected Areas in Communications*, 25(8):1569–1589, October 2007.

[15] Yipin. Sun, Rongxing Lu, Xiaodong Lin, and Xuemin Shen. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. *IEEE Transactions on Vehicular Technology*, 59(7):3589–3603, September 2010.

[16] Chul Sur, Youngho Park, and Kyung-Hyune Rhee. An efficient and secure navigation protocol based on vehicular cloud. *International Journal of Computer Mathematics*, 2014.

[17] William Whyte, Andre Weimerskirch, Virendra Kumar, and Thorsten Hehn. A security credential management system for v2v communications. In *Proc. of the 2013 IEEE Vehicular Networking Conference (VNC'13), Boston, MA, USA*, pages 1–8. IEEE, December 2013.

[18] Rong Yu, Yan Zhang, Stein Gjessing, Wenlong Xia, and Kun Yang. Toward cloud-based vehicular networks with efficient resource management. *IEEE Network*, 27(5):48–55, September 2013.

Author Biography

Youngho Park received his M.S.and Ph.D. degrees in Department of Computer Science and Information Security from Pukyong National University, Republic of Korea in 2002 and 2006, respectively.He is currently a post doctor course researcher in Department of IT Convergence and Application Engineering, Pukyong National University. His research interests are related to applied cryptography and communication security; secure vehicular ad hoc network, authentication, key management.

Chul Sur received his M.S. and Ph.D.degrees in Department of Computer Science from Pukyong National University,Republic of Korea in 2004 and 2010, respectively.He is currently a lecturer in the Division of Digital Media Engineering,Busan University of Foreign Studies. His research interests are related with applied cryptography, network security, and secure e-commerce.

Kyung-Hyune Rhee received his M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology(KAIST), Daejon Korea in 1985 and 1992, respectively. He worked as a senior researcher in Electronic and Telecommunications Research Institute (ETRI), Daejon Korea from 1985 to 1993. He also worked as a visiting scholar in the University of Adelaide, the University of Tokyo, and the University of California, Irvine. He has served as a Chairman of Division of Information and Communication Technology, Colombo Plan Staff College for Technician Education in Manila, the Philippines. He is currently a professor in the Department of IT Convergence and Application Engineering, Pukyong National University, Busan Korea. His research interests center on key management and its applications, mobile communication security and security evaluation of cryptographic algorithms.