Secure Emergency Services Protocol over Vehicular Cloud Computing

Lewis Nkenyereye and Kyung Hyune Rhee*
Department of IT Convergence and Application Engineering,
Pukyong National University, Republic of Korea
{nkenyele, khrhee}@pukyong.ac.kr

Abstract

Natural disasters such as typhoon or earthquake requires an efficient disaster rescue system in order to minimize the losses. Vehicular cloud Computing (VCC) which integrates cloud computing within the vehicular ad hoc networks (VANETs) offers a suitable platform especially for disaster assistance and rescue teams (DART) which use vehicles to reach the disaster locations. Current protocols for disaster services cover the assignment of rescue mission to the vehicles heading to the disaster scenes. However, some disasters such as earthquakes and tsunamis can repeatedly happen within a short interval, requiring the disaster documents to be updated continuously for better rescue services. In this paper we present a secure protocol for emergency services over vehicular cloud computing which enables the DART vehicles to access disaster scenes and have updated information of disaster scenes during their activities. The proposed protocol is not based on bilinear operations unlike the existing secure rescue services. We make use of linear secret sharing scheme (LSSS) coupled with attribute based encryption (ABE), geo-encryption and ID-based signature to guarantee the security objectives. We verify the efficiency of the proposed protocol through performance evaluations.

Keywords: ID-based Signature, Attribute based Encryption, Linear Secret Sharing Scheme, Vehicular Cloud Computing

1 Introduction

Recently thousands of people were killed of an earthquake in Nepal and other countries in the world have experienced several natural disasters. After the Haiti earthquake in 2010, reports revealed that the disaster rescue system needed to be improved through the information and communication technologies [1]. The main transportation entities used for disaster rescue missions are vehicles, helicopters and small airplanes including drones. For the last two decades, cloud computing (CC) has emerged as one of the most influential paradigms in the IT industry, and has attracted extensive attention. Cloud computing is even predicted to be the fifth primary utility among the human being necessities after water, gas, electricity and telephone [13]. Vehicular cloud Computing (VCC) is a new technological paradigm integrating the concept of cloud computing with a vehicular environment [4]. VCC uses a cloud computing to serve the users of vehicles in vehicle ad hoc networks (VANETs) with different services in order to minimize traffic congestion, accidents, travel times, environmental pollution, etc.

Disaster assistance and rescue teams (DARTs) are normally group of people who are committed on a disaster field as soon as an alert is given by the disaster rescue center (DRC). In the conventional system, a report of the disaster scene is transmitted to the team leader through email (or a hard copy) and further information is communicated by portable radio transceivers within the team. %DART normally move out by separate vehicles within different groups such as the first medical aid group, fire-fighters

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 2, Article No. 3 (July 15, 2016)

*Corresponding author: A12-1305, Daeyeon Campus, Pukyong National University, Yongso-ro 45, Nam-gu, Busan 48513, Republic of Korea Tel: +82-51-629-6247

and psychologist group. Occasionally, DARTs need real time (updated) information to efficiently provide their services. Disaster scene information available to DRC is likely to be shared among different entities such as medical teams, fire teams which could have various degrees of sensitivity. In this case, the concept of VCC can be appropriately used to share information to vehicle-based groups. Additionally, it would require robust isolation, strong security concepts and controlling access mechanisms. Access control is one of the common and fundamental requirements for all types of cloud users. However, conventional access control models cannot be applied in the VCC environment due to the different access domains and mobility [7]. Moreover other security properties need to be considered in order to encourage all the stakeholders to embrace the VCC architecture based technology and specifically secure protocols for rescue services.

Several studies have addressed potential security and privacy issues in VANETs [2] [14] [8]. However these protocols do not address the rescue services over VCC. *Sun et. al* [10] proposed a location-based secure and dependable disaster rescue network by exploiting the stored location information for post disaster rescue and preserving location privacy in normal network operations. However, their protocol is not built on Vehicle using Clouds architecture and lacks of detailed security mechanisms. Among the relevant works for rescue services based on vehicle communications, *Yeh et al,* [12] presented an attribute based access control for emergency services over VANETs. Their scheme presented a protocol to securely assign vehicles to disaster scenes based on attribute based encryption. Their proposed scheme uses attribute based encryption both for the recruitment of available emergency vehicles and assignment of chosen vehicles to the disaster scene. This requires a huge computational time knowing that the decryption of ABE ciphers is dependent of the number of attribute within the cipher text. Moreover their scheme is built based on expensive bilinear pairing cryptographic primitives which are time consuming operations. On the other hand, *Yeh et al,* protocol only covers the assignment of vehicles to disaster location but sometimes the disasters might continue to occur during a disaster mission which would require updated information for DART. In this paper, we present a secure protocol for emergency services over vehicular cloud which allows DART vehicles to securely access disaster documents as they are heading to the disaster scenes, then DRC will later if necessary broadcast the newly updated disaster documents geo-encrypted under the scene location, thus only DART vehicles within the location can access the document. Our contribution for this paper can be summarized as follows:

- We present an application model for a secure emergency services over vehicular cloud computing which securely assigns DART vehicles to rescue scenes; but also provides DART with updated information for the disaster scene during the mission. We also define the security requirements for the proposed protocol.
- We construct a secure protocol for rescue services over vehicular cloud. We make use of ID-based signature [16], linear secret sharing scheme [3] and attribute based encryption [11] to achieve the security goals.
- We provide on-site disaster services issuance based on geo-encryption [9].
- We provide the performance of the protocol based on the security analysis and computational cost.

2 Preliminaries

We briefly present the constitution of a key policy attribute encryption scheme which forms the basis of our proposed system. In order to design the proposed system, we consider a lightweight attribute encryption scheme and refer to [11] for concrete description of the algorithms.

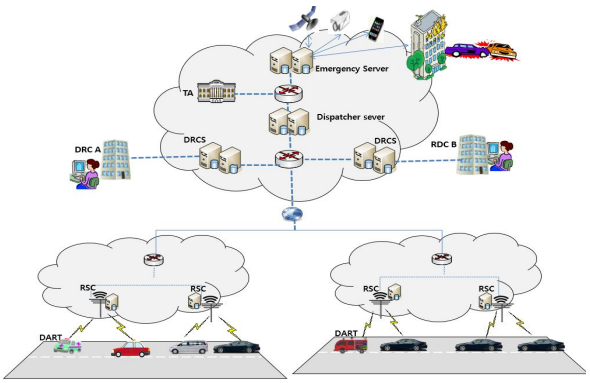

Figure 1: System Architecture.

- ABE.Setup(): This algorithm outputs attribute master key *amk* and public key parameters *abe.params*.
- ABE.Encrypt(m, γ, *abe.params*): This algorithm outputs the ciphertext C by taking as input a message m, an attributes set γ, and public parameter *abe.params*.
- ABE.KeyGen(*amk*, Γ): Given an access structure Γ, this algorithm outputs the decryption key D corresponding to the access structure.
- ABE.Decrypt(C, D, *abe.params*): This algorithm decrypts the cipehrtext C if the attribute set γ satisfies the access structure Γ.

3 Proposed System

In this section we describe the communication entities within our protocol which are made of TA, ES, DRCS, RSC and DART vehicles which communicate through the on-board unit (OBU) as shown in figure 1:

- Trusted Authority (TA): It is in charge of the registration of all entities (DRCS, RSC and DART vehicle) inside our system and issues cryptographic materials during the system initialization.
- Emergency server (ES): It is a server in the cloud which receives raw information from different media such as satellite, camera, video recorder, or even auto-recorded voice mail. We assume that ES applies data mining operations and sends the data to different DRCS.
- Disaster Rescue Center Server (DRCS): It is a server located in the cloud controlled by a DRC which offers disaster rescue services through DART vehicles.
- Road Side Cloud (RSC): RSC are databases located along the roads and accessible by the vehicles. They permit the communication between the vehicles and the DRCS. RSC are assumed to be semi-trusted entities with sufficient computational capabilities.
- DART vehicles: DART possesses vehicles which are used by the DRC to communicate to DART through DRCS. For instance, DART in charge of building damage assistance can have five vehicles. The disaster reports (DR) should be accessed by authorized DART vehicles. DRs are sent to OBUs of DART through RSC. DART are also equipped with AntiSpoof GPS receivers.

Our protocol should satisfy the following security requirements:

- Authentication and Authorization: Each DART vehicle should be authenticated before it can receive a disaster report (DR) from DRCS. This would prevent any unauthorized vehicle to open or access confidential disaster reports.
- Fine grained access control: Through fine-grained access control based on LSSS, only selected and authorized vehicles should access a disaster report.
- Confidentiality: Disaster reports sent by DRCS to DART vehicles should be kept confidential against eavesdroppers.
- On-site location based disaster report access: Once on the disaster scene, the updated disaster documents should only be accessed by a vehicle within the specified geographic location. This would fasten the communication and reduce the possibility of the updated disaster documents being eavesdropped by the attackers.

3.1 System Setup

In order to initialize the system, TA performs the followings to generate system parameters and issues keys to each vehicle participating in the system:

- Let $\mathbb{G}$ be a group of order q and a generator $P \in \mathbb{G}$. TA choose a master secret key $s \in Z_q^*$ and computes its public key as $PK_{TA} = s \cdot P$. TA picks a random $b \in \mathbb{Z}_q^*$ as an ID-based signature generation secret and set $P_{TA} = b \cdot P$ as the corresponding public key.
- TA runs ABE.Setup() to generate *amk* and *abe.params*, and publishes the public system parameters $\langle G, q, P, PK_{TA}, P_{TA}, abe.params, H_1 \rangle$ where $H_1 : \{0,1\}^* \rightarrow Z_q^*$ is a cryptographic hash function.
- For each vehicle v_i, TA assigns access structure Γ_i and generates decryption key D_i by using ABE.KeyGen(*amk*, Γ_i). TA provides v_i with $\langle D_i, b \rangle$ securely.

3.2 Credential Generation

Periodically, DART vehicles get credentials from DRCS. This helps DRCS to make a list of on-duty vehicles periodically (24 hours based). To acquire a rescue credential from $DRCS_j$, v_i first generates a signing key according to ID-based key generation as follows:

- Picks $r \in \mathbb{Z}_q^*$ and compute $R = r \cdot P$
- Computes $c_1 = H_1(P_{TA}, VID_{v_i}, R)$.
- Computes $c_2 = r - c_1 \cdot b (mod\ q)$
- Computes $c = H_1(P_{TA}, VID_{v_i}, c_1 P_{TA} + c_2 P)$
- Generates $SK_{v_i} = \{c, c_1, c_2\}$

v_i composes a rescue credential request $rcm = \{VID_{v_i}, Dtask, k, Ts\}$ representing t the identity, daily allocation task, session key and the time stamp respectively. The daily allocation task may contain information which is unusual such as an ambulance which has been requested to go and assist in another city different from its common working location. v_i generates its signature on the above message as follows:
v_i computes $W = w \cdot P$ where $w \in Z_q^*$, then computes $n = H_2(P_{TA}, VID_{v_i}, rcm, W, c_1)$ and

$\mu = w - n \cdot c_2 (mod\ q)$ and return $\sigma_{v_i} =< c, c_1, W, \mu >$ and sends $L =< \sigma_{v_i}, crm >$ to $DRCS_j$ via RSC encrypted under $DCRS_j$ public key.

$DRCS_j$ performs the following before it issues the credential:

- $DRCS_j$ decrypts L using its private key.
- $DRCS_j$ checks if the time stamp Ts in the message is not out-dated. In case the difference between the attached time stamp compared to the current time is lager than the threshold, the message is discarded.
- $DRCS_j$ computes $n = H_1(P_{TA}, VID_{v_i}, crm, W, c_1)$ and verifies if $c = H_1(P_{TA}, VID_{v_i}, c_1 P_{TA} + n^{-1}(W - \mu P))$ and rejects in case the equality does not satisfy. The verification works because of the following holds:

$$\begin{aligned} c &= H_1(P_{TA}, VID_{v_i}, c_1 P_{TA} + c_2 P) \\ &= H_1(P_{TA}, VID_{v_i}, c_1 P_{TA} + n^{-1}(nc_2 P)) \\ &= H_1(P_{TA}, VID_{v_i}, c_1 P_{TA} + n^{-1}(wP - wP + nc_2 P)) \\ &= H_1(P_{TA}, VID_{v_i}, c_1 P_{TA} + n^{-1}(wP - (wP - nc_2 P))) \\ &= H_1(P_{TA}, VID_{v_i}, c_1 P_{TA} + n^{-1}(wP - (w - nc_2)P)) \\ &= H_1(P_{TA}, VID_{v_i}, c_1 P_{TA} + n^{-1}(W - \mu P)) \end{aligned}$$

$DRCS_j$ composes a rescue credential $CRE_{v_i} = \{CreKN, Ts\}$ representing respectively the credential keynote and the time stamp, then performs the following:

- $DRCS_j$ computes $C = Enc_k\{CRE_{v_i}\}$ where k is a symmetric key sent during credential request and sends C to v_i. In non-rushing hours, $DRCS_j$ forwards the list of generated credentials and their respective identities to TA.

3.3 Rescue Service Issuance

When a disaster happens, $DRCS_j$ broadcast an alert beacon for DART vehicles within their coverage through RSCs. Upon receiving the alert beacon, each DART vehicle v_i sends an availability message for rescue mission as follows:

- Compose the availability message as $M_{av} = \{CRE_{v_i}, VID_{v_i}, ts, Dtask, k_1\}$ representing respectively the credential, its identity, the time stamp, the daily task type and a session key for a symmetric encryption such as AES. v_i generates a signature on M_{av} and sends it to $DRCS_j$ as described in Section 3.2.
- $DRCS_j$ verifies the signature as described in section 3.2, then checks if the credential corresponds to the identity of v_i.
- For a rescue message rm, $DRCS_j$ defines the attribute set γ, generates the ciphertext crm using ABE.Encrypt(rm, γ, $abe.params$), and sends crm to v_i.
- Upon receiving the crm, v_i can recover the rescue message rm as ABE.Decrypt(crm, D_i, $abe.params$).

3.4 On Site Rescue Service Issuance

During a rescue activity, $DRCS_j$ might receive updated disaster documents for example a new building which has just collapsed. In that case, a geo-encryption which allows only emergency vehicles within the specific geographic location to access the updated disaster information, is performed as follows:

- Depending on the exact location of the disaster, $DRCS_j$ computes a Geo-lock for the message rm as $gk = H_1(lat_{v_i}||long_{v_i}||vel||ts||k_1)$ with $\{lat_{v_i}, long_{v_i}, vel, ts\} = pvt$ representing v_i's latitude, longitude, velocity, the time stamp and k_1 the shared secret respectively.
- $DRCS_j$ broadcasts $< rm_2 >$ through RSC where $rm_2 = Enc_{gk}(rm_1)$.

To decrypt the message, appropriate v_i performs the following:

- Generate its pvt using an anti spoof GPS receiver $pvt^{'} = \{lat^{'}_{v_i}, long^{'}_{v_i} vel^{'}, ts^{'}\}$.
- Generates $gk^{'} = H_1(lat^{'}_{v_i}||long^{'}_{v_i}||vel^{'}||ts^{'}||k_1)$ which equals to gk for $pvt = pvt^{'}$.
- Decrypt the message rm_2 using $gk^{'}$.

4 Performance

In this section, we evaluate the performance of the proposed protocol based on the security analysis along with the computation cost.

4.1 Security

According to the aforementioned security objectives, we analyze and discuss the security of the proposed protocol.

- Authentication: During the credential request phase, a vehicle sends a credential request which as $rcm = \{VID_{v_i}, Dtask, k, Ts\}$ on which an ID-based signature $\sigma_{v_i} =< c, c_1, W, \mu >$ is attached. Since the signing key $SK_{v_i} = \{c, c_1, c_2\}$ is only known by v_i and can be recomputed by TA, we argue that v_i signature can not be forged by any attacker, then the proposed protocol is secure against forgery attacks.
- Authorization: $DRCS_j$ provides periodic credentials to DART vehicles. When a emergency occurs, unless v_i's possesses a valid credential $CRE_v = \{CreKN, Ts\}$, v_i can not receive the disaster report to head to the disaster scene. Thus, we confirm that the credential authorization can not allow any attacker to impersonate the emergency vehicles.
- Fine-grained access control: In our protocol, a disaster report message is sent to available vehicle using ABE.Encrypt. No vehicle which does not satisfy the access structure Γ can recover the disaster report. Even DART vehicles which share a number of attributes set can not collude together to recover the secret which allow the decryption of the disaster report. During the decryption phase based on the root or child node, unless v_i possesses the correct attributes set, the decryption process output $\perp$.

- On-site location based disaster report access : During a disaster mission, any updated disaster information is geo-encrypted with a geo-location key $gk = H_1(lat_{v_i}||long_{v_i}||vel||ts||k_1)$. v_i has to be a registered DART vehicle, then it has to be located within the specified perimeter ($pvt = pvt^{'}$) to receive a disaster document during the rescue mission.

4.2 Computational cost

In this section, we evaluate the performance of our protocol in terms of computational cost. Note that we ignore the time complexity involved in setup because it is assumed to be done offline and occasionally. Let T_{mul} and T_{pair} denote the time required to perform one point scalar multiplication and one pairing operation over an elliptic curve respectively. Also let T_{as-enc}, T_{as-dec}, T_{sig}, T_{ver} be the time required to perform asymmetric encryption, asymmetric decryption, signature generation and signature verification respectively. These operations dominate the speed of signature generation and signature verification and we neglect all others operations such as addition and one-way hash function [15]. We consider the implementation parameters in [5] [6] with embedding degree 6, with $\{\mathbb{G}, q\}$ represented by 161 bits and 160 bits respectively. The implementation was executed on a *3.5-GHz, core i-5, 16GB RAM* desktop computer. The obtained results are shown in table 1. Table 2 shows the computational cost of our protocol

Notation	Operations	time (ms)
T_{pair}	bilinear pairing	2.82
T_{mul}	point scalar multiplication	0.78
T_{as-enc}	asymmetric encryption	1.17
$T_{as-decc}$	asymmetric decryption	0.61
T_{sig}	signature generation	1.56
T_{ver}	signature generation	3.12

Table 1: Measurement of cryptographic operations

compared to [12]. In our protocol we eliminated the attribute based encryption for disaster rescue mission assignment as it is in [12] and used credentials for the authorization of emergency vehicles during the recruitment phase. Moreover, the proposed protocol is not built on expensive bilinear pairing operations, Thus the computational overhead of the proposed protocol is more than 50 % lesser than [12]. Note that we assumed that the minimum number of attribute within an access structure Γ equals to 4 (d=4). Even though we consider a bigger number of attributes set (d=10), the proposed protocol still performs better than [12] as described in table 2.

Phase/Issuance	ABACS [12]	Proposed
Credential	$dT_{pair} + 2T_{mul}$	$T_{sig} + T_{ver} + T_{as-enc} + T_{as-dec}$
Service	$dT_{pair} + 2T_{mul}$	dT_{mul}
Total cost (ms, d=4)	25.68	12.7

Table 2: Computational cost of ABACS and proposed protocol

To evaluate the receiving ratio of v_i, we estimate the required coverage range (denoted by C_{RSC}) over which an RSC successfully transmits the message *rm* to v_i . The minimal required coverage range of an RSC is calculated as:
$C_{rg} = v \times T_{t-round}$ where $T_{t-round}$ is the total cost described in table 2.

We further estimate the receiving ratio, denoted as R_{rat}, by considering the coverage range C_{RSC} of an RSC and the short waiting period ξ. The following formula can be applied to calculate the receiving

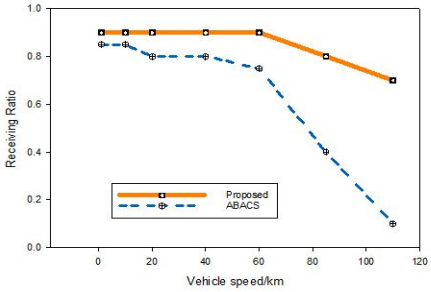

Figure 2: Receiving ratio of a rescue vehicle for d=4

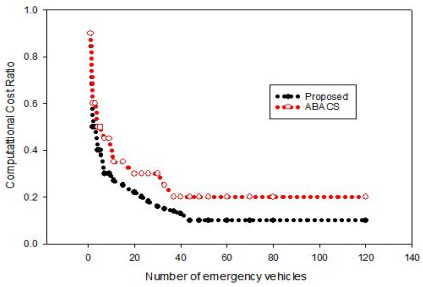

Figure 3: Computational cost ratio vs emergency vehicles (a=5)

ratio as described in [12]:
$R_{rat} = \frac{C_{RSC}}{C_{rg} \times \xi} = \frac{C_{RSU}}{v \times T_{t-round} \times \xi}$ where $C_{RSC} \geq R_{rg}$.

$$R_{rat} = \begin{cases} 1 & \text{if } \frac{C_{RSU}}{T_{t-round}} \cdot \frac{1}{v \times \xi} \geq 1; \\ \frac{C_{RSC}}{T_{t-round}} \cdot \frac{1}{v \times \xi} & \text{otherwise.} \end{cases}$$

In figure 2, with d = 4 and with the computational overhead described in Table 2, we show the receiving ratio with respect to the speed of vehicle. The proposed protocol achieves better performance with 0.9 receiving ratio for vehicles moving at 60 km/h. For a speed of 120 km/h, the worst receiving ratio goes to 0.7 for the proposed protocol, better than 0.17 for [12]. Figure 3 shows the relationship between the computational cost ratio and the number of emergency vehicles, when we assume that the number of vehicles involved in the emergency mission is equal to 5 (a=5), we can see that the proposed protocol performs better than [12].

5 Conclusion and Future Work

In this paper, we proposed a secure protocol for emergency services over vehicular cloud computing. The proposed protocol uses credentials for DART authorization before assigning v_i to a rescue mission. Moreover, our protocol provides on-site disaster rescue services. Our protocol is based on the primitives of ID-based signature, attribute based encryption over linear secret sharing scheme and geo-encryption. The proposed protocol is based on point scalar multiplication over elliptic curve contrary to expensive bilinear pairing operations of existing researches in the literature. The performance evaluation of the protocol protocol confirms its efficiency.

Acknowledgments

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. NRF-2014R1A2A1A11052981).

References

[1] E. A. Cavallo, A. Powell, and O. Becerra. Estimating the direct economic damages of the earthquake in haiti. *The Economic Journal*, 120(546):298–312, July 2010.

[2] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li. Vspn: Vanet-based secure and privacy-preserving navigation. *IEEE Transactions on Computers*, 63(2):510–524, August 2012.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proc. of the 13th ACM conference on Computer and communications security (CCS'06), Alexandria, Virginia, USA*, pages 89–98. ACM Press, October 2006.

[4] R. Hussain, F. Abbas, J. Son, and H. Oh. Tiaas: Secure cloud-assisted traffic information dissemination in vehicular ad hoc networks. In *Proc. of the 13th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID'13), Delft, Netherlands*, pages 178–179. IEEE, May 2013.

[5] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. S. Shen. A novel anonymous mutual authentication protocol with provable link-layer location privacy. *IEEE Transactions on Vehicular Technology*, 58(3):1454–1466, March 2009.

[6] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for fr-reduction. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 84(5):1234–1243, May 2001.

[7] H. A. J. Narayanan and M. H. Gunes. Ensuring access control in cloud provisioned healthcare systems. In *Proc. of the 2011 IEEE Consumer Communications and Networking Conference (CCNC'11), Las Vegas, Nevada, USA*, pages 247–251. IEEE, January 2011.

[8] L. Nkenyereye, Y. Park, and K.-H. Rhee. Secure vehicle traffic data dissemination and analysis protocol in vehicular cloud computing. *The Journal of Supercomputing*, 72(6):1–21, June 2016.

[9] D. Qiu, S. Lo, P. Enge, D. Boneh, and B. Peterson. Geoencryption using loran. In *Proc. of the 2007 National Technical Meeting of The Institute of Navigation (NTM'07), San Diego, California, USA*, pages 104–115. IEEE, January 2007.

[10] J. Sun, X. Zhu, C. Zhang, and Y. Fang. Rescueme: location-based secure and dependable vanets for disaster rescue. *IEEE Journal on Selected Areas in Communications*, 29(3):659–669, March 2011.

[11] X. Yao, Z. Chen, and Y. Tian. A lightweight attribute-based encryption scheme for the internet of things. *Future Generation Computer Systems*, 49(C):104–112, August 2015.

[12] L.-Y. Yeh, Y.-C. Chen, and J.-L. Huang. Abacs: an attribute-based access control system for emergency services over vehicular ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 29(3):630–643, March 2011.

[13] Y. A. Younis, K. Kifayat, and M. Merabti. An access control model for cloud computing. *Journal of Information Security and Applications*, 19(1):45–60, February 2014.

[14] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang. Toward cloud-based vehicular networks with efficient resource management. *IEEE Network*, 27(5):48–55, September/October 2013.

[15] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen. An efficient message authentication scheme for vehicular communications. *IEEE Transactions on vehicular Technology*, 57(6):3357–3368, July 2008.

[16] R. W. Zhu, G. Yang, and D. S. Wong. An efficient identity-based key exchange protocol with kgs forward secrecy for low-power devices. *Theoretical Computer Science*, 378(2):198–207, June 2007.

Author Biography

Lewis Nkenyereye received his bachelor degree in Computer Science from Light University of Burundi], master degree in Information Technology from Uganda Christian University of Uganda in 2009 and 2012, respectively. Since September 2013, he is with the Lab of Information Security and Internet Applications, Department of IT Convergence and Application Engineering, Pukyong National University as a doctorate student. His research interests are related with cryptography and vehicular cloud security.

Kyung Hyune Rhee received his M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea in 1985 and 1992, respectively. He worked as a senior researcher in Electronic and Telecommunications Research Institute (ETRI), Republic of 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, Republic of Korea. His research interests center on key management and its applications, mobile communication security and security evaluation of cryptographic algorithms.