ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)

https://doi.org/10.17559/TV-20170827155412
Original scientific paper

# Design of Safety Assurance System of Specific Vehicle Information using ABPRE in the Fog Computing Environment

Hyun-Jong CHA, Ho-Kyung YANG, Jin-Mook KIM, You-Jin SONG

**Abstract:** There would be high demand for technology that monitors illegal activity and detects risk with respect to vehicles on the road in a future urban traffic system, for accident prevention. However, there may be substantial overheads from the massive amount of data that would be required for the surveillance system as it would be automatically operated and used, as further advancements are made in sensor network technology and IoT (Internet of Things). In the transportation field, systems were mainly studied to measure the driver's drowsiness or mobile phone use. These systems will collect information from several mobile devices at the same time, resulting in overhead of data. Fog computing reduces the overhead of data because it uses distributed proxy servers. However, security aspects were not considered. Encryption can be done to ensure the privacy of the information on the moving vehicles. However, in order to track a specific vehicle the data of the moving vehicles should be provided decrypted or decrypted by the secondary user. In this paper, to solve security aspects, we provide a new DSS model that utilizes ABPRE (Attribute Based Proxy Re-Encryption). The proposed system encrypts data sensed from moving vehicles. The cipher is configured to re-encrypt quickly at the proxy. The proposed method allows only users with access authority via secondary user's properties to access data with attribute-based re-encryption. Therefore, safety is secured.

**Keywords:** ABPRE; Decision Support System; fog computing; safety assurance

## 1 INTRODUCTION

Sensor data is usually small, but always generates data. In order to distinguish and process the collected data, data of a location (Edge) close to the sensor (device) is collected. Also, pre-processing and real-time processing are performed, and sensor data performs other QoS (Quality of Service) control. Otherwise, measures such as installing a smart gateway in the network to handle protocol changes are necessary. In this way, it is important to have a degree of data processing within the network [1]. There are IoT (Internet of Things) and M2M (Machine-to-Machine) communications that connect sensors and devices beyond shells. In order to put the communication into practical use, data from a large number of destinations should be handled efficiently. Therefore, it is necessary to have a communication infrastructure that can be operated even if the number of data flows is greatly reduced as compared with the conventional one.

There would be high demand for technology that detects risk for each of the moving vehicles in a future urban traffic system, with stressed importance of safety. Therefore, many different types of data such as images from the vehicle camera and driver tendencies must be immediately analysed to calculate the risk, with fully automatic or driver-assisted accident avoidance.

With a structure in which data are gathered at a central server and processed and sent to each of the moving vehicles, like with the current mobile telecommunications system, there would not be sufficient time for making sophisticated judgements due to network latency and delays. However, real-time processing would be needed at the level of individual vehicles, and geographically close vehicles or vehicles that had been in a similar situation before they would need to exchange information to gather information suitable for the particular environment such as accidents that had taken place nearby and identification information.

However, it is extremely difficult to gather data passed from a large number of moving vehicles to a central server and store them in a searchable form, as indicated by surveillance cameras. It is even more difficult to summarize indexes for search efficiency of stored data. To solve the problem, extract only important information. Subsequently, by processing the data at the network edge, the amount of data on the network can be reduced. Also, a mechanism to convey only important meta information is necessary [2]. In addition, privacy protection of personal information that can be infringed when gathering mobile information is secured.

In this paper, the attribute-based encryption technique [3, 4] using proxy re-encryption technique [5] is applied among encryption methods. Proxy re-encryption technique is a method of converting a ciphertext through a proxy. In traditional public key cryptography, the plain text is encrypted with the sender's public key. Then, the ciphertext is decrypted by the recipient's private key. However, in the attribute-based proxy re-encryption method, by re-encrypting by changing the access structure of the attribute, an object having another attribute can decrypt.

In this paper, we provide an attribute-based proxy re-encryption based model to prevent information collection efficiency and privacy infringement. The proposed system collects data from locations close to mobile objects and equipment. Subsequently, the collected data is processed by a smart gateway that can perform pre-processing and real time processing. Such a process is processed by a proxy using a method of ABPRE (Attribute Based Proxy Re-Encryption). In addition, the collected data constitutes the system so that only users with specific authority can be encrypted or decrypted from among secondary users and users.

The structure of this paper is divided into five parts. In Chapter 2, we describe the technique related to the proposed system. Chapter 3 describes the proposed system and compares and analyses its performance in Chapter 4. Finally, in chapter 5 we present the finishing and future direction of research.

## 2 RELATED RESEARCHES

### 2.1 Fog Computing

Fog computing is a concept proposed by Cisco. It is a type of system in the spotlight, with the spread of IoT. IoT is where chips are embedded in all kinds of devices from household appliances to vehicles, allowing the exchange of

all sorts of data over a wired/wireless network [7]. Sensors are embedded in unmanned vehicles, eyeglasses, watches, shoes and clothes, and they communicate with a server, sending biometric data and analysing data and providing information.

Sensors are installed at various places in a building and they check the temperature or humidity and maintain pleasant conditions by the use of related devices or equipment. In addition, they are also sometimes used for security purposes. However, there would be problems in trying to store data gathered from the sensors entirely on the cloud server. Not only would there be physical challenges such as storage capacity but there would also be temporal limitations as large amounts of data would need to be constantly exchanged [8]. Fog computing was introduced to address exactly this problem. With fog computing, constantly generated data are not stored in the cloud at a remote location but processed at nearby sensors or devices like a router, with only the necessary data sent to the cloud.

Fig. 1 shows the structure of fog computing. Mobile nodes are equipped with calculation and routing capabilities while each of the computing instances are allotted a specific amount of system resources in terms of CPU speed, number of cores, memory size, and storage capacity. In other words, the computing instance of each node in a smart traffic environment is able to execute application code [6].

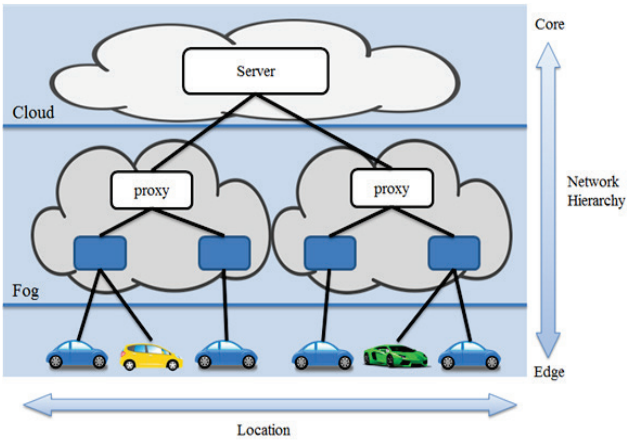


**Figure 1** The structure of fog computing

## 2.2 ABPRE

With PRE (Proxy Re-Encryption), the proxy server re-encrypts A's ciphertext so that B can decrypt it without the need to acquire any information about the plaintext. In other words, A generates a re-encryption key that delegates privileges to decrypt its ciphertext and sends it to the proxy server. Then the proxy server, using a re-encryption key, converts A's ciphertext to a ciphertext that can be decrypted with B's private key, and sends this new ciphertext to B. Then B decrypts the ciphertext with its private key. It is a technique of converting the ciphertext encrypted with A's public key so that it can be decrypted with B's private key, which is performed by a proxy.

Because the proxy is able to, using a re-encryption key, convert the ciphertext without having to decrypt it, it has no knowledge of the plaintext or A's private key. This scheme can be applied to such things as sending encrypted email and file systems [10].

Taking the sending of encrypted email as an example, in the event A is absent or the private key has been lost, the proxy can take A's encrypted email and convert it to B's encrypted email and send it. The proxy would only convert A's ciphertext to B's ciphertext without decrypting the original ciphertext. Also, B is able to decrypt the ciphertext with its own private key without the need to use A's private key.

ABPRE (Attribute-Based Proxy Re-Encryption) is a concept that has extended the original type of proxy re-encryption (public key or ID-based encryption system) to using attributes. That is, decryption privileges can be delegated to a user in an access control environment. A user (identified by attributes) can freely designate a proxy that performs re-encryption of a ciphertext from one access policy to another access policy.

As it pertains to this paper, an investigative institution must be able to decrypt the data encrypted at a moving vehicle which is to be tracked. Therefore, re-encryption is performed to that end.

## 2.3 DSS [9]

A fog-based intelligent DSS (decision support system) is a fog-based rule violation monitoring system which may be adopted in a future driver surveillance system designed to crack down on drivers that use mobile devices using driving [6, 8].

It is operated in a total of three layers. Tab. 1 shows the role of each layer. For the bottom layer, two different types of sensor are needed, global camera sensors (GCS) and local camera sensors (LCS). LCSs are installed inside a vehicle and they not only monitor driver activity but also appropriately issue warnings.

**Table 1** Activities of different layers

| Layers | Activities |
|---|---|
| Bottom layer | Detect vehicle number with the help of GCS |
| | Drivers in operation with the help of LCS detect use of mobile devices |
| | Warning of the driver for a certain period of time with the help of LCS |
| | GCS and LCS send their vehicle number and vehicle identifier to fog server |
| Middle layer | Fog server receives vehicle number and vehicle ID of GCS and LCS respectively |
| | Fog server correctly deliberately identifies vehicles that break traffic rules related to portable devices during driving |
| | Send accurate vehicle identifier information to designated cloud server |
| Top layer | The cloud server synchronizes itself with the last updated vehicle identifier information |
| | Provide decision-making based on traffic violation rules |

GCSs are installed on traffic signals, etc. and they are able to identify license plate numbers. Both GCSs and LCSs are able to communicate with the fog server that sits in the middle layer for high-speed processing. The top layer synchronizes itself with the latest data and it is made up of

a server designated by a pertinent institution that generates a decision based on traffic rules.

## 3 PROPOSED SYSTEM MODEL

This section describes the configuration of the model of the proposed system and pertinent procedures. In this paper, we propose a shared method of data utilizing ABPRE.

### 3.1 Overview of the Proposed Model

This section presents a model of a tracking method for tracking a specific vehicle in a smart traffic environment based on IoT. Fig.2 shows the structure of the proposed system model [13].

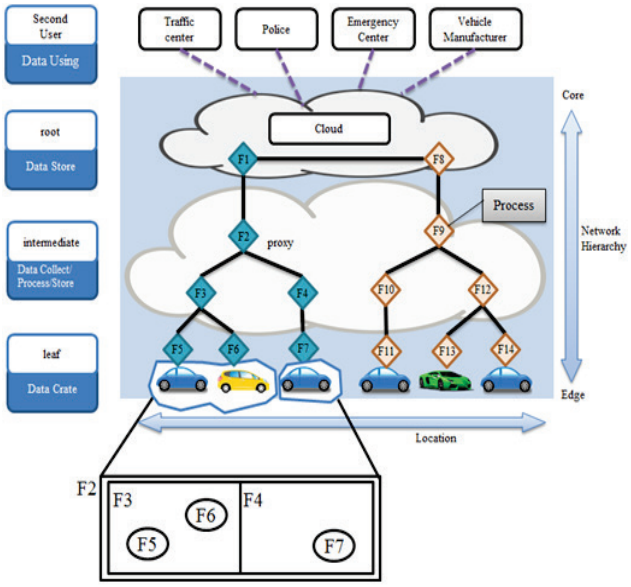


**Figure 2** The structure of the proposed system model

This model is a computing environment with a proxy node equipped with calculation and routing capabilities, based on SDN. Nodes and entities in the network can be managed by groups. In other words, F5 and F6 are included within the domain of F3, while F7 is included within the domain of F4, which are managed by F3 and F4 respectively. Furthermore, F3 and F4 are included in a bigger domain called F2.

Sensor data generated at a vehicle are received via a smart signaller in a smart traffic network. These data are encrypted for ensuring confidentiality of sensitive data such as personal data. Because data gathered at vehicles in a smart traffic environment are massive and non-structural, it is difficult to perform real-time processing with a typical cloud computing environment, and network latency may pose a problem. Therefore, a smart signaller performs as a proxy and not only gathers sensor data but also processes and stores them.

The proxy performs the processing when real-time processing is needed, such as when tracking a specific vehicle, and a re-encrypted ciphertext is provided to a secondary user (such as a police vehicle) so that only it can decrypt the ciphertext. Accordingly, the institution managing vehicle data can delegate decryption privileges with respect to a specific vehicle to be tracked to a secondary user such as the police, which is then able to decrypt the data. That is, the generator of vehicle data encrypts using the access structure of vehicle data as the key, which allows decryption to be done only according to what the administrative institution has defined. Then, decryption privileges are delegated to the police and decryption can be done with the police's private key.

### 3.2 Service Scenario

The scenario is created, assuming that a user is driving a vehicle. Fig. 3 shows the scenario of the proposed system.

- The user's information is collect by wearable device and vehicle device in daily life.
- A vehicle connected with a user's wearable device via Bluetooth recognizes a rider using his/her state and prepares a customized control service for a rider while driving.
- A user keeps sending his/her encrypted sensing information while driving.

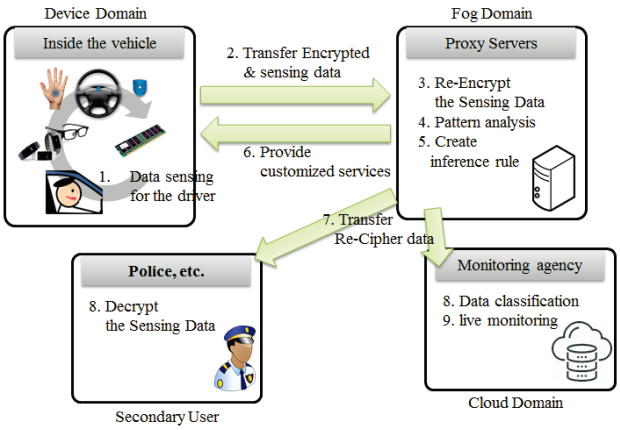


**Figure 3** The structure of the proposed system model

### 3.3 Makeup of the ABPRE-Based System Model

The proposed system uses the ABPRE algorithm, based on the structure shown in Fig. 4. The model used is made up of a total of six stages, as shown in Fig. 5.

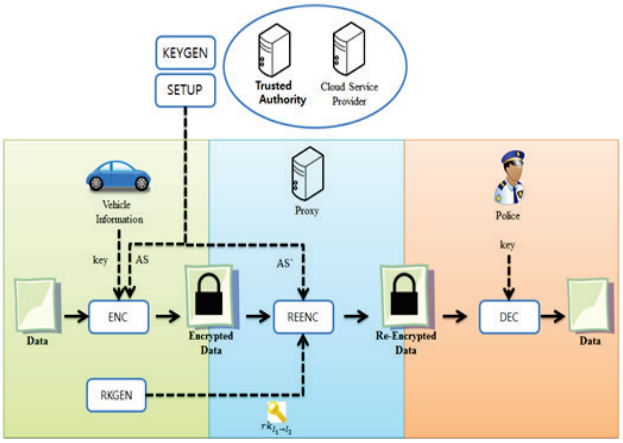


**Figure 4** The structure of the proposed system model

First, Setup: The administrative institution enters a security parameter for each vehicle to generate a public parameter and master key.

Second, Key generation: The administrative institution generates a private key after an attribute index aggregate and master key for each vehicle are entered.

Third, Encryption: An access structure for the generated data and a generated message are entered at each vehicle to generate a ciphertext.

Fourth, Re-encryption key generation: The administrative institution needs access control for the data so that only those entities that should have access to the data should do so, with respect to each vehicle. The private key and access structure are entered for each vehicle to generate a re-encryption key.

Fifth, Re-encryption: A re-encryption key and ciphertext are entered at the proxy to generate a re-encrypted ciphertext. If the index aggregate satisfies the access structure of the original ciphertext, a new ciphertext is generated; otherwise it is not generated.

Sixth, Decryption: If the access structure of the ciphertext is satisfied for the index aggregate after entering the private key and the ciphertext, a message is generated; otherwise it is not generated.

The setup and key generation stages are performed by the institution managing keys and access privileges; the re-encryption stage by the administrative institution that owns the data; the encryption stage by the data generator; the re-encryption stage by the proxy; finally, the decryption stage is performed by a secondary user.

### 3.4 Detailed Process of Model

The proposed system uses the ABPRE algorithm, based on the structure shown in Fig. 4. The model used is made up of a total of six stages, namely Setup, KeyGen, Encrypt, RKExtract, Re-encryption, and Decrypt. Setup and KeyGen are performed by a Trusted Authority, while Encrypt and RKExtract are performed by a vehicle. Furthermore, Re-encryption is performed by a proxy, while Decrypt is performed by the police.

First, Setup ($1^k$): This algorithm is processed in the Cloud server in Fig. 4. Processing for data sharing in Fig. 5 is started after this algorithm has been executed. In this algorithm, a security parameter $k$ is inputted to generate a public parameter *pp* and a master key *mk*. Select $y,\ t_i$ given with Eq. (1).

$$y, t_i \in Z_p (1 \le i \le 3n) \tag{1}$$

A generation source $g,h \in G$ is randomly selected. Define the $Y, T_i, T_i'$ given with Eq. (2).

$$Y = e(g, h)^y,\ T_i = g^{t_i},\ T_i' = h^{\frac{1}{t_i}} (1 \le i \le 3n) \tag{2}$$

The public parameter *pp* is Eq. (3).

$$\left\langle e, g, h, Y, T_i, T'_{i\,1 \le i \le 3n} \right\rangle \tag{3}$$

The master key *mk* is Eq. (4).

$$\left\langle y, t_{i\,1 \le i \le 3n} \right\rangle \tag{4}$$

Second, KeyGen(*S*, *mk*): This algorithm is processed in the Cloud server in Fig. 4. Processing for data sharing in Fig. 5 is started after this algorithm has been executed. In this algorithm, the index aggregate *S* and master key *mk* are entered to generate the private key *usk*.

The attribute index aggregate is defined as $S$. $r_1,\ldots,$ $r_n \in Z_p$ is randomly selected. $r = r_1 + r_2 + \cdots + r_n$ and $\hat{D} = h^{y\,r}$ are calculated.

If $i \in S$, $D_{i,1}$ and $D_{i,2}$ given with Eq. (5); otherwise $D_{i,1}$ and $D_{i,2}$ given with Eq. (6).

$$D_{i,1} = h^{\frac{r_i}{t_i}},\ D_{i,2} = h^{\frac{r_i}{t_{2n+i}}} \tag{5}$$

$$D_{i,1} = h^{\frac{r_i}{t_{n+i}}},\ D_{i,2} = h^{\frac{r_i}{t_{2n+i}}} \tag{6}$$

The private key *usk* is $\left\langle S, (D_{i,1}, D_{i,2})_{i \in N}, \hat{D} \right\rangle$.

Third, Encrypt (*AS*, *m*): This algorithm is processed in the Vehicle in Fig. 4. In this step, encrypt the processing for data of vehicle information in ENC of Fig. 5. In this algorithm, the access structure *AS* and message *m* are entered to generate a ciphertext *C*.

The access structure *AS* and plaintext $m \in G_T$ are defined. A random value $s \in Z_p^*$ is selected. $\widetilde{C} = m \cdot Y^S, \widehat{C} = g^S, \breve{C} = h^S$ is calculated. And $W_i, C_i$ is calculated given with Eq. (7).

$$(W_i = 0,\ C_i = \hat{A}_l^r),\ (W_i = *,\ C_i = A_i^{*r})(1 \le i \le n) \tag{7}$$

If $AS$ is $+d_i, C_i = T_i^S$; otherwise $AS$ is $-d_i, C_i$ is Eq. (8).

$$C_i = T_{n+i}^S, C_i = T_{2n+i}^S \tag{8}$$

The ciphertext is $C = \left\langle AS, \widetilde{C}, \widehat{C}, \breve{C}, (C_i)_{i \in N} \right\rangle$.

Fourth, RKExtract (*usk*, *AS*): This algorithm is processed in the Vehicle in Fig. 4. This step is done during the process of Fig. 5. Processing for RKGEN in Fig. 5 is started after this algorithm has been executed. In this algorithm, the private key *usk* and access structure *AS* are entered to generate a re-encryption key *rk*.

$d \in Z_p$ is randomly selected. $v \in g^d, \hat{D}' = \hat{D}$; $\xi$ is defined, and $\xi$ is the ciphertext of *ASv*.

If $i \in S$, $D'_{i,1}$ and $D'_{i,2}$ given with Eq. (9); otherwise $D'_{i,1}$ and $D'_{i,2}$ given with Eq. (10).

$$D'_{i,1} = D_{i,1} \cdot (T_i')^d,\ D'_{i,2} = D_{i,2} \cdot (T_{2n+i})^d \tag{9}$$

$$D'_{i,1} = D_{i,1} \cdot (T'_{n+i})^d,\ D'_{i,2} = D_{i,2} \cdot (T'_{2n+i})^d \tag{10}$$

The re-encryption key is Eq. (11).

$$C = \left\langle S, AS, (D'_{i,1}, D'_{i,2})_{i \in N}, \hat{D}, \xi \right\rangle \tag{11}$$

Fifth, Re-encryption: This algorithm is processed in the Proxy in Fig. 4. In this step, re-encrypt the processing

for data of vehicle data in REENC of Fig. 5. A re-encryption key *rk* and ciphertext *C* are entered to generate a re-encrypted *rk*. If the index aggregate *C* satisfies the access structure, re-encrypted ciphertext *C′* is generated; otherwise it is rejected.

If *AS* is $+d_i, E_i$ given with Eq. (12); otherwise *AS* is $-d_i, E_i$ given with Eq. (13).

$$E_i = e(C_i, D'_{i,1}) = e(g^{t_i,s}, h^{\frac{r_i+d}{t_i}}) = e(g,h)^{s(r_i+d)} \tag{12}$$

$$\begin{aligned} E_i &= e(C_i, D'_{i,1}) = e(g^{tn+is}, h^{\frac{r_i+d}{tn+i}}) = e(g,h)^{s(r_i+d)}, \\ e(C_i, D'_{i,2}) &= e(g^{t2n+is}, h^{\frac{r_i+d}{t2n+i}}) = e(g,h)^{s(r_i+d)} \end{aligned} \tag{13}$$

$\hat{C}$, $\hat{D}'$ are generated using $\overline{C}$ given with Eq. (14).

$$\overline{C} = e(\hat{C}, \hat{D}') \prod_{i \in N} E_i = e(g,h)^{ys+nds} \tag{14}$$

The ciphertexts are $C' = \langle AS', \widetilde{C}, \overline{C}, \breve{C}, \zeta \rangle$ and $C_{re} = \langle AS', \widetilde{C}, \overline{C}, \breve{C}, \zeta' \rangle$.

Sixth, Decrypt (*usk*, *C*): This algorithm is processed in the Second User or the Cloud Server in Fig. 4. In this step, decrypt the processing for data of Vehicle data in DEC of Fig. 5. The private key *usk* and ciphertext *C* are entered and if the index aggregate satisfies the access structure of ciphertext *C*, message *m* is generated; otherwise it is rejected.

If *AS* is $+d_i, E_i$ given with Eq. (15); otherwise *AS* is $-d_i, E_i$ given with Eq. (16).

$$E_i = e(C_i, D'_{i,1}) = e(T^s, h^{\frac{r_i}{t_i}}) = e(g,h)^{sri} \tag{15}$$

$$\begin{aligned} E_i &= e(C_i, D_{i,1}) = e(T^s_{n+i}, h^{\frac{r_i}{tn+i}}) = e(g,h)^{sri}, \\ e(C_i, D_{i,2}) &= e(T^s_{2n+i}, h^{\frac{r_i}{t2n+i}}) = e(g,h)^{sri} \end{aligned} \tag{16}$$

The ciphertext $C' = \langle AS', \widetilde{C}, \overline{C}, \breve{C}, \zeta \rangle$ and the private key $usk = \langle S, (D_{i,1}, D_{i,2})_{i \square N}, \hat{D} \rangle$ are used to decrypt given with Eq. (17).

$$\frac{\widetilde{C} e(v, \breve{C})^n}{\overline{C}} = \frac{m \cdot e(g,h)^{ys} \cdot e(g^d, h^s)^n}{e(g,h)^{ys+nds}} = m \tag{17}$$

## 4 COMPARATIVE ANALYSIS

In this paper, comparative analysis is performed on the proposed method based on Sandip's DSS Model in terms of efficiency and security.

### 4.1 Efficiency Analysis

With the two methods, data are processed by a fog server or proxy in order to reduce overheads that would otherwise result for the cloud server. However, with the DSS model, synchronization is performed at the cloud server with the data received, in addition to performing final decision making.

With the proposed method, the cloud server only stores ciphertexts sent from the lower layer, and as a result there is only a small amount of processing done by the cloud server. Also, with the DSS model, the middle layer identifies law-violating vehicles at the fog server based on traffic rules using an identification algorithm, but with the proposed method, identification is done based on attributes, so that the processing stage is made simple.

### 4.2 Security Analysis

An ideal standard for attribute-based re-encryption is proposed for the cloud [11]. It includes unidirectionality, data confidentiality, non-interaction, and non-performance [12]. With unidirectionality, re-encryption cannot be done in reverse.

With data confidentiality, non-approved entities with respect to the ciphertext cannot obtain the information. With non-interaction, entities other than the owner are not needed for generating a re-encryption key. With non-performance, a re-encrypted ciphertext cannot be obtained by combining two re-encryptions.

With multiplex use, re-encrypted data can be re-encrypted again and distributed. With re-encryption control, whether or not re-encryption is performed can be controlled by the data owner. With master key security, a user cannot obtain the master key of the owner by colluding with another entity. With collusion attack prevention, a revoked user should not be able to use encrypted data by colluding with the cloud.

The proposed model meets the requirements of unidirectionality, data confidentiality, non-interaction, non-performance, master key security, and collusion attack prevention. However, it does not meet the requirements of multiplex use and re-encryption control. In the proposed model with regard to multiplex use, when data generated at a vehicle are sent encrypted, the proxy performs the re-encryption. This is used by an investigative institution such as the police, because there will not be a case in which the used data are re-encrypted to be used for a secondary purpose. Although re-encryption control stores the ciphertext generated at a vehicle with the administrative institution, because the administrative institution must be able to use it given that specific attributes are satisified, re-encryption control is not considered since there will not be a case in which re-encryption is not performed.

In addition, analysis is done to determine whether it is secure against collusion attack, user/attribute abolition, and man-in-the-middle attack. While a single user without privileges cannot decrypt the contents by himself, in a collusion attack, multiple users collude with each other and combine their attributes to decrypt the ciphertext.

With the proposed method, even if multiple entities in a single domain collude with each other, create a single set of false attributes and use it, since only previously authorized users will be able to decrypt, collusion attack can be prevented. In addition, ciphertexts are kept at the CSP, while keys and attributes are kept at the TA, thereby dispersing privileges and preventing collusion attack.

User/attribute abolition is an important matter of consideration when attribute-based encryption is used. With the proposed method, there are no changes made with respect to the private key. Instead, the access structure is immediately updated to reflect changes in user privileges and sent down to the proxy server. After decryption, if the access structure is not satisfied, the ciphertext cannot be viewed. User abolition problem is addressed in this manner.

Man-in-the-middle attack is when an attacker gets between the two communicating entities, eavesdrops and picks up information to forge a message, thereby obtaining information valuable to it. With the proposed method, messages that are re-encrypted at the proxy are secure even if the attacker finds out the private key as long as the access structure, which serves as the material for the re-encryption key, is not satisfied. However, if the attacker disguises himself as a proxy, obtains the ciphertext generated at a vehicle and disguises himself as a legitimate vehicle to a proxy, and given the private key and the access structure all have proper values, the man-in-the-middle attack may temporarily pose a danger.

### 4.3 Comparative Analysis

Comparing with the previously proposed DSS model, it did not take into account the matter of privacy for drivers at all. Therefore, personal information of drivers could be obtained by all entities in the network. With the method proposed in this paper, because data are sent encrypted from vehicles, confidentiality is ensured primarily. Furthermore, access control is done with an access structure so that entities without viewing privileges cannot obtain personal information. Tab. 2 compares the DSS model with the proposed method. Because DSS does not have any considerations of security as mentioned previously for collusion attack, user/attribute abolition, and man-in-the-middle attack, there is no security support with DSS.

**Table 2** Compare with existing DSS

| | DSS | Proposed Scheme |
|---|---|---|
| Prevention of collusion attack | × | ○ |
| User / attribute abolition | × | ○ |
| Man-in-the-middle attack | × | △ |

However, the proposed method supports security with respect to collusion attack and user/attribute abolition, with a partial support with respect to man-in-the-middle attack. Furthermore, the proposed model supports security in terms of unidirectionality, data confidentiality, non-interaction, non-performance, and master key security.

## 5 CONCLUSIONS

Introduction of IoT has become active, and fog computing is the system that is attracting attention. The Internet of things is that things like peripheral appliances, automobiles and other devices transmit and receive various information via the network. Sensors are attached to eyeglasses, watches, shoes and clothes, and physical information is exchanged with the server. Analyse these data and provide information. However, there is a problem when saving all of these data to the cloud server. Although there are physical things like storage capacity, there are time restrictions to send and receive many data. Therefore, the availability of information decreases. The number of mobile information collected also in the future smart transport network is very large. For simple traffic forecasts, etc., we use centralized data as it is now. However, real-time information such as information on accidents must be included. Also, when tracking a specific vehicle, we must provide the information of the mobile to the investigation agency. When unconditional information is provided to an investigation agency, privacy infringement such as general information leakage of vehicles is concerned.

In order to solve these problems, this paper proposed a fog computing based model. The data processed by the cloud server can be processed immediately by processing with the proxy of the edge of the network. Also, in order to prevent information leakage of general vehicles, encrypted data is transmitted. Secondary users, such as investigative agencies, used re-encryption technology to be able to decrypt only information on specific vehicles. Secondary users have access rights based on their attributes. Therefore, in our thesis, we constructed a safety DSS model using the method. Moreover, we confirmed the safety of the proposed method compared with DSS model proposed based on conventional fog.

In this paper, the proposed model can be applied to the environment of companies dealing with confidential data of customers and the medical environment dealing with patient information. In the future, we will study the problem of delegating authority to withdraw the user's access authority. In addition, authentication problems of each user and proxy should also be studied.

### Acknowledgements

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2016R1D1A1B03931689). This work was also supported by the Dongguk University Research Fund of 2017.

## 6 REFERENCES

[1] Nakao, A. (2013). Objectives of SDN in Future Network. Electronics. *Information and Communication Journal, 96*(12), 902-905.

[2] Hiroshi, M. (2013). Edge-Heavy Data and architecture in the big data era. *Journal of Information Processing and Management, 56*(5), 269-275. https://doi.org/10.1241/johokanri.56.269

[3] Liang, X., Cao, Z., Lin, H., & Shao, J. (2009). Attribute Based Proxy Re-encryption with Delegating Capabilities. *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security / ACM*, 276-286. https://doi.org/10.1145/1533057.1533094

[4] Shanqing, G., Yingpei, Z., Juan, W., & Qiuliang, X. (2008). Attribute-Based Re- Encryption Scheme in the Standard Model. *Wuhan University Journal of Natural Sciences, 13*(5), 621-625. https://doi.org/10.1007/s11859-008-0522-5

[5] Mambo, M. & Okamoto, E. (1997). Proxy cryptosystems: Delegation of the power to decrypt cipertext. *IEICE Trans. Fund Electronics Communications and Computer Science, 80*(1), 54-63.

[6] Hong, K., Lillethun, D., Ramachandran, U., Ottenwälder, B., & Koldehofe, B. (2013). Mobile fog: A programming model for large-scale applications on the internet of things. *Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing / ACM*, 15-20. https://doi.org/10.1145/2491266.2491270

[7] Baek, J., Vu, Q. H., Liu, J. K., Huang, X., & Xiang, Y. (2015). A secure cloud computing based framework for big data information management of smart grid. *IEEE transactions on cloud computing, 3*(2), 233-244. https://doi.org/10.1109/TCC.2014.2359460

[8] Sandip, R., Rajesh, B., & Debabrata, S. (2015). A Fog-Based DSS Model for Driving Rule Violation Monitoring Framework on the Internet of Things. *International Journal of Advanced Science and Technology*, 82, 23-32. https://doi.org/10.14257/ijast.2015.82.03

[9] Chang Soo Heo. *DRM Cloud Using CP-ABPRE*. Pukyong National University of Korea, 2015.

[10] Kaitai, L., Au, M. H., Liu, J. K., Susilo, W., Wong, D. S., Yang, G., Yu, Y., & Yang, A. (2015). A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. *Future Generation Computer Systems*, 52, 95-108. https://doi.org/10.1016/j.future.2014.11.016

[11] Luo, S., Hu, J., & Chen, Z. (2010). Ciphertext Policy Attribute-Based Proxy Re-encryption. *International Conference on Information and Communications Security* / Springer, 6476, 401-415. https://doi.org/10.1007/978-3-642-17650-0_28

[12] C-ICT. (2016). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility. European Commission, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX :52016DC0766

[13] Cha, H. J., Yang, H. K., Kim, J. M., & Song, Y. J. (2016). Design of Monitoring system of rule violation using ABPRE in the Fog Computing Environment. *Asia-pacific Journal of Applied Science and Engineering for Better Human Life*, 6, 29-31. https://doi.org/10.21742/asehl.2016.6.08

**Contact information:**

**Hyun-Jong CHA**
Department of Defense Acquisition Program,
Kwangwoon University, 20 Kwangwoon-ro, Nowon-gu,
Seoul, 01897, Korea
E-mail: chj826@kw.ac.kr

**Ho-Kyung YANG**
Division of Information Technology Education,
Sunmoon University,
70 Sunmoon-ro 211 beong-gil, Tangjeong-myeon, Asan-si,
Chungcheongnam-do, 31460, Korea
E-mail: porori2000@kw.ac.kr

**Jin-Mook KIM**
Division of Information Technology Education,
Sunmoon University,
70 Sunmoon-ro 211 beong-gil, Tangjeong-myeon,
Asan-si, Chungcheongnam-do, 31460, Korea
E-mail: calf0425@sunmoon.ac.kr

**You-Jin SONG**
(Corresponding Author)
Department of Management,
Dongguk University,
707 Seokjang-dong, Gyeongju,
Gyeongsangbuk-do, 38066, Korea
E-mail: song@dongguk.ac.kr