Research Article

A Study on Moving Object Tracking Using Proxy-Based Access Privilege in Fog Computing

Dr.Hyun-Jong Cha [a], Dr.Ho-Kyung Yang [b] , Dr.You-Jin Song [c*]

[a] Department of Multimedia Science, Chungwoon University, KOREA
[b] Division of Information Technology Education, Sunmoon University, KOREA
[c] Department of Information Management, Dongguk University, KOREA
Corresponding Author: You-Jin Song, **email:** song@dongguk.ac.kr

Abstract: The vehicles operating in IoT environment is a tool for conveniently human life. However, the information of the car user has a problem that may be illegally collected. With accept the security solutions used in existing wired Internet environment, it is impossible to solve the problem of security that may occur in the automobile operating in IoT environment. Approach that we have proposed is, to use an attribute-based decoding schemes and dynamic threshold cryptography. So, it provides a method capable of delegate authority to delegate so that can prevent tracking information of the car. In order to implement the research method we have proposed, there is a need for real-time processing technology and co-operation technology. So, we use the proposed proxy in the fog computing, to install the smart gateway in a car, after you collect the information in real time, to use as a proxy for processing a large amount of calculation. And I will simulate our proposed algorithm and system using usim(cloud service simulator) or NS2.

Keywords: Proxy, Access authorization, Attribute transformation key, Dynamic threshold cryptography, Modification attack

1. Introduction

Internet of Things means to the technology to connect to the Internet incorporates a sensor and communication capabilities for a variety of things. Here, things may contain a variety of embedded system such as electronics product, mobile devices and wearable computers. Moreover, things that are connected to the internet of things has a unique IP (Internet Protocol) which can distinguish themselves, it must be connected to the internet. Then, it is possible to build a sensor in order to collect data from an external environment. These Internet of things is activated, network traffic has increased explosively. These increases in traffic can be network performance is directly linked to lower. In addition, as more cases of using cloud computing service for big data analysis of the increased traffic, it may increase the movement path of the data and which can result in overloading of the entire network. Therefore, it becomes necessary to provide service to be able to prioritize more than a certain proportion of the data in the vicinity of network Edge. Then, it is distributed intelligence computing that was developed to solve this problem. For example, a fog computing.

Thus, fog computing is a paradigm which extends the cloud computing services to the network edge stage. The concept such as data, computing, storage and application services to users is similar to cloud computing. But, Proximity to the user, geographic distribution of high-density, such as motility support, etc. can have large discrimination compared to the cloud computing **(Jung, 2020)**.

Internet of Things and practical application of Machine-to-Machine communication compared to the existing of communications infrastructure. Even data flow is reduced against of existence general communication infrastructure. Sensor data is smaller in normal size. However, in order to always process the data generated, the sensor must be pass data codes collected in the vicinity of Edge and process it. In this case, the sensor perform only simple pretreatment and smart-gateway (edge) process a real-time processing. It is important to design to perform complex processing such as QoS control. In this way, system architecture designer have idea of a simple processing and complex calculations such as simple device process a simple job and smart-gateway process a higher job. They must have a idea of depended on the role and power with device **(Nakao, 2013)**.

Our lives in the future is going to be more convenient. Because the Internet of things technology is developed. But, we must be sure to solve the security problem. Then we can support the IoT technology such as smart home, smart car, and smart grid is to provide safely.

If we don't occur the security problems in IoT environment, we have a large damage to occur even more convenient due to the service of the IoT. For example, a company very quickly developed and to provide to the user a variety of services that can be used in the IoT environment. But, they have a very low measure on the might encounter security problems or not. Because they don't aware of the importance for the security of IoT service problems by the companies and the government. Furthermore, we don't know that what kind of security problems

on the IoT environments and how can solve this problem to easy on this environment with fog computing scheme. So this is very critical problems.

In addition to the importance of safety in the future of urban transportation system, it will demand of technology to avoid sensing the danger of each mobile increases (Park, 2019). For this reason, such as a camera image and the driver of the trend work of the vehicle, and immediately analyzed a variety of data amount, to calculate the risk of risk, to support or automate the avoidance behavior. The result of processing the collected information to the central server, such as a current mobile communication system, in the structure to be transmitted to each mobile, network latency or delay problems due to lack of altitude determination times there (Moon, 2020). Further, the mobile level requires individual real-time processing, the neighborhood of the accident information by exchanging information of the moving bodies that was in a similar situation geographically mobile or past close to each other, congestion information collection of information that is appropriate to the environment, such as is required.

However, collected current of the data over the past many of the moving body to the central server, Summary and index in a searchable form, as in the example of a surveillance camera, it is very difficult. In such a case, by treatment with important information only data extracted and the network edge (Edge), reduce the amount of data on the network, it is necessary to introduce a mechanism for transmitting only the important meta information **(Hwang, Kim, Lee and Jung, 2017; Maruyama, 2014)**.

Smart Car related hacking is clear that bring serious damage. Related smart car, in Texas in 2010, hacking the navigation of vehicle, there was incident that paralyzed of 100 cars engine and horn. And June 2013 in California, there is incident that hacking the smart car and open the car door and stolen the thing. In addition, in August 2013 hacker conference, it demonstrated that was hacked type vehicle in 2010 “Toyota Prius" and "Ford Escape" by Nintendo's portable game consoles. If introduced to the commercialization of unmanned vehicle systems it can receive as much direct damage are on the driver's life. All modern vehicles has been mounted Micro controller and CAN (Controller Area Network) that the internal bus for the device to communicate with each other. If the CAN to obtain access right a wireless connection, it can also be obtained access to the major systems such as brake and handle potentially. Most of the security risks of such smart cards, vehicle manufacturers occurred began to allow access to the vehicle functions developers. Thus, it must precede privacy protection that personal location can be compromised through unauthorized access of mobile such as a vehicle or ID.

The ABE (Attribute based encryption) have been proposed to prevent the invasion of privacy of personal information, and extend this, CP-ABTD (Ciphertext Policy Attribute Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes) has been proposal (Ibraimi, Petkovic, Nikova, Hartel and Jonker, 2009). However, CP-ABTD is necessary to check the access rights again even though the user has been delegated rights to the data. In this regard, It is required a procedure for authorization to determine the access right to the fog computing environment in which the access of non-purpose the vehicle information is trying to use **(Robinson, Vogt and Wagealla, 2005)**.

In this paper, in order to solve these problems, we proposed a accept access authority scheme using the CP-ABTD and dynamic threshold cryptography. Proposed system collecting the sensor (device) and in the near place (Edge), and process data through a pre-processing or real time processing or smart gateway handles only the sensor data **(Song, 2016)**.

To solve the authorization problem of access rights, in this paper, the user of the service (secondary users) may browse the vehicle information provides a method for managing access service user. The proposed scheme, with the ability Proxys is to determine the access rights of the service user. In other words, by using a dynamic threshold password, what consent each Proxys that authority has been granted by the threshold, it is determined external users of authority is given the right to browse. Since only the existing CP-ABTD attribute conversion key, lost or, if it is modulated, it is impossible to re-encryption is performed. The proposed scheme, by dividing the attribute conversion key to the dynamic threshold password, is secure against attack modulation.

In this paper, related research describe in Chapter 2. And our proposed system describe in Chapter 3. And Analysis of our proposed system with existence system such as CP-ABE, CP-ABTD in Chapter 4. Lastly, Chapter 5 is conclusion.

Now that you are writing your paper, you will need to use the tab button to indent each new paragraph that you write. The standard number of spaces indented are five, you should have your tab button set to automatically indent these number of spaces without having to change anything.

Remember to write clearly and do not use personal pronouns. Include your in-text citations to show your reader where and when you got information from other sources **(Carlson, 2010)**. Your APA paper should be double spaced throughout.

2. Related Works

2.1. Smart-Traffic Network Model base on SDN

SDN is a technique that can provide a flexible network through the network virtualization and network functions virtualization. It is composed of the data and control planes. Users can program the control plane in accordance with

the situation can be controlled as required objects present on the data plane. OpenFlow is the lower part of the SDN. In this paper, we configured the structure of smart-traffic model using SDN that have three stages. That have Edge area, Smart Gateway or Proxy area, and Core area. As shown in Figure 1, Edge region are configured cars, smart phones, laptops, and cameras. Proxy layer of the intermediate layer is composed of a Smart Gateway, which is a small computer which is mounted on another server or automobile. Servers that exist in the Core region is a server for a large volume, real-time processing **(Blaze, Bleumer and Strauss, 1998; Mambo and Okamoto, 1997)**.

Special purpose computing device called a processing node to configure the computing infrastructure required by smart transportation network needs to be placed on the network. For example, a special router, not only transmission of packets, the computing common applications can be dealt. Further, by using the fog computing arrangement, the same management on demand computing instances and IaaS cloud including the management, such as creating a computing resources of a particular level network layers for a particular geographic area. It must provide a program interface that allows **(Hong, Lillethun, Ramachandran, Ottenwalder and Koldehofe, 2013)**.

Figure.1. Smart-Traffic Network base on SDN

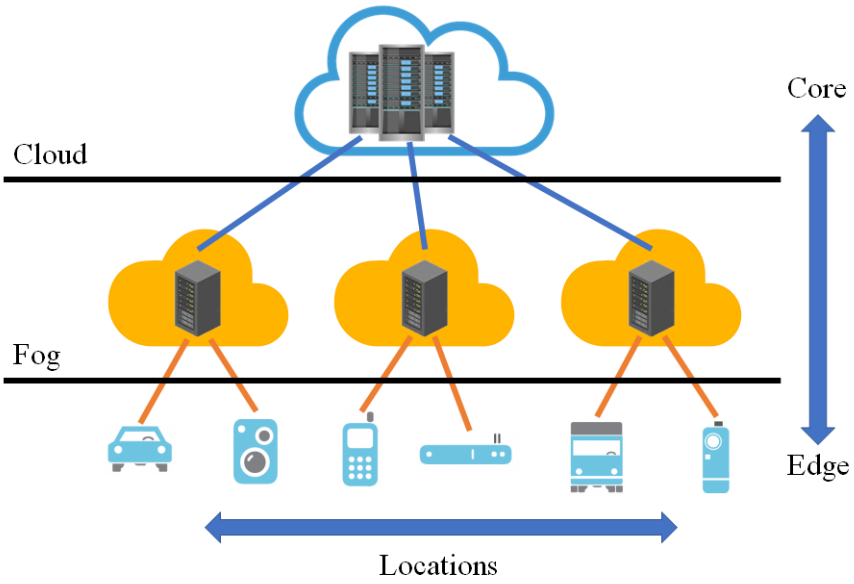


Figure 1 shows the structure of Smart-Traffic Network base on a fog computing environment such as SDN/NFV **(Roy, Bose and Sarddar, 2015)**. Mobile node have each compute instance. it will be executed until its own computing power and routing functions. At this time, the instance means the capacity of the specific system resources such as CPU speed, number of cores, memory size and storage capacity with in nodes. In other words, each node using a separate instance for running the application code in the environment of smart transportation network **(Hong, Lillethun, Ranachandran, Ottenwalder and Koldehofe, 2013)**.

2.2. CP-ABTD and Bilinear Mapping

The Bilinear Mapping $\hat{e}:G_1\times G_2\rightarrow G_2,G_1$ is the output space of the bilinear mapping) for the Cyclic Group, G_1,G_2 is following properties.

- Bilinear : The $e(u^a,v^b)=e(u,v)^{ab}$ is established for all $u\in G_1,v\in G_2$ and all $a,b\in Z$.
- Non-degenerate : $G_X(X=1,2)$ is a generator $g\in G_X$ for the $e(g,g)\neq 1$.
- Computable : There is efficient algorithms for calculating the $e(g,g)$ for all $u\in G_1,v\in G_2$.

User's private key in the CP-ABE (CP-ABE, Ciphertext Policy Attribute Based Encryption) **(Bethencourt, sahai and Waters, 2007)** is associated with the attribute set and the ciphertext is associated with the attributes access structure. When satisfy the attributes sets of user's private key for a specific decoding policy in the ciphertext, ciphertext is decrypted. CP-ABE system have not explained by practical aspects of the problem of Revocation and Delegation.

CP-ABTD(Ciphertext Policy Attribute Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes) **(Ibraimi, Petkovic, Nikova, Hartel and Jonker, 2009)** may perform a delegation of flexible attributes and revocation function at the same time, as an extension of the attribute-based proxy re-encryption. CP-

ABTD has the three features. First, the delegate with the private key associated set of attributes may delegate his rights to others. Second, the Delegator may decide to delegate his authority to others. In other words, it is possible that the delegate who has been delegated the authority to re-delegate authority to other users. Third, it is possible to attribute revocation to take the decryption authority delegate.

2.3. Dynamic Threshold Cryptography

The secret sharing scheme is two way. There are ways in which all share the restored gather to create a plain text. And if there is a possible way to restore the share only as much as the threshold number. method is not restored because the problem of the modulation and revocation of share, proposed method is not affected by the modulation and revocation of share method **(Jakobsson, 1999)**.

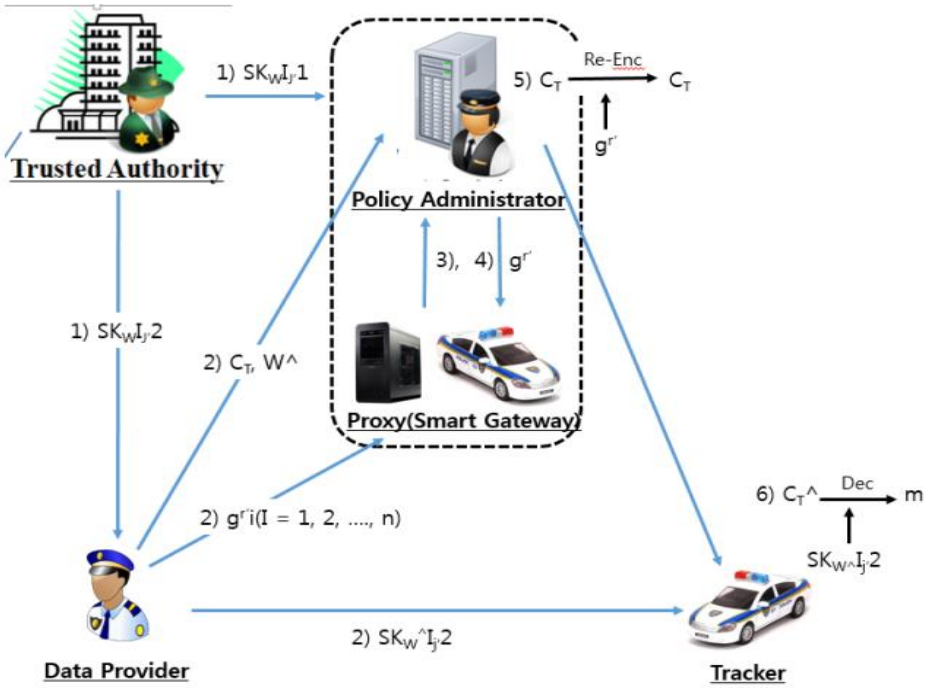
Dynamic threshold cryptography is distributed to n users by distributing plaintext into n share. And Dynamic threshold cryptography is to distribute the plaintext to n users by n share. Then if the plaintext k share has gathered restore utilizing a Lagrange Interpolation. In proposed system, such a feature will be used when delegate split the attribute conversion key to shares. And will be used when proxies restore the attribute conversion key from the shares.

3. Our Proposal Scheme

3.1. Structure

In this section, in the IoT-based smart transportation network, it presents a model for a method of tracking a particular vehicle such as Figure 2. Our proposal model is a computing environment that has a proxy node with calculation and routing functions based on SDN (Software Defined Network).

Figure.2. Our Proposal model



It assumed that access to the vehicle information through the approval of the Administrative Review Board (Proxys). Participants, it compose of delegator (Data Provider), the delegate (Tracker: Service User), the certification authority (TA, Trusted Authority) and policy manager (PA, Policy Administrator).

Sensing data generated from the vehicle is received data via a smart traffic signal of smart transportation network. At this time, data is encrypted to ensure confidentiality of sensitive data such as personal information. Data collected from the environment of the vehicle smart transportation network are the vast and unstructured data, in a typical cloud computing environment, real-time processing is difficult, it is possible to delay time of the network becomes a problem. Accordingly, the smart signal machine running proxy functions, not only the collection of the sensing data, processing, will have the function of saving.

3.2. Algorithm

In this paper, a procedure that is reviewing the access rights of the management committee and approved construct in the next scenario. we process re-encrypted in order to it can perform tracking and decoding of the law enforcement agencies to encrypted data of the moving object to track. In the case of a particular vehicle tracking necessary to real-time processing, treated with a proxy, only the secondary user(For example, police vehicles, etc.) to provide a re-encryption to be able to recover the data. In other words, police etc. that a secondary user decryption authority of the particular vehicle to track in the institution which manages vehicle information can be delegated and decoded. Constructors of vehicle data is encrypted with the public key of the vehicle. This can only be decrypted by private key of the management Review Board. It is to allow decryption key of the police has been delegated decryption authority.

First, Trusted Authority (TA) defines system parameter, and generates public key pk and master key mk using Setup(k) algorithm. And generates two secret key share sk_{wI_u1} and sk_{wI_u2} associated with vehicle attribute *w* and identifier I_u using KeyGen (mk, w, I_u) algorithm, and then sk_{wI_u1} is distribute to the user side PA and is distribute to the vehicle.

Second, Vehicle transfers Ciphertext c_τ (setting the data m, access structure) to the database of user side PA using Encrypt(m, τ, pk) algorithm. Also, we generate and transfer secret key share sk_{wI_u2} for Mandator using attribute set $\hat{w}$ and mandator(for example, an insurance company employee) consisted on the bases of vehicle attribute set w in Delegate($sk_{wI_u2}, \hat{w}, I_j$) algorithm. To send the attribute conversion key share $g^{p_1}(1 \le i \le n)$ obtained by dividing the attribute conversion key $g^{r'}$ to the management committee. Also, to send an attribute set $\hat{w}$ to PA.

Third, the delegate is request admits to the management committee of the user side in order to view the data m of the vehicle. Management committee approve or reject after determining the validity of the mandator's access (In this scenario to be admits almost).

Fourth, When the management committee approves the documents viewing request of the delegate, we original constitute attribute conversion key $g^{r'}$ that attribute conversion key share $g^{p_1}(1 \le i \le n)$ of about k using Reconstruct ($g^{p_1}(1 \le i \le n)$) algorithm, and then it transfer to the PA.

Fifth, PA generates a secret key share sk_{wI_u1} from m-Delegate ($sk_{wI_u1}, \hat{w}, sk_{w\to\bar{u}}$) algorithm their own secret key share sk_{wI_u1}, attribute conversion key $g^{r'}$, attributes set $\hat{w}$ that car was defined. Finally, $\hat{c}_\tau$ that the ciphertext c_τ was re-encrypted to the secret key share sk_{wI_u1} and identifier I_i in m-Decrypt (c_τ, sk_{wI_u1}, I_i) algorithm, and then it transfer to the mandator.

Sixth, Delegator is get the data m by key sk_{wI_u2} received from vehicle or the PA and decrypted ciphertext c_τ.

3.3. Detailed Procedure of our model

The proposed scheme is composed of eight algorithm such as Setup, KeyGen, Encrypt, Delegate, Reconstruct, m-Delegate, m-Decrypt and Decrypt. Setup and KeyGen for each algorithm TA, Encrypt and Delegate is delegate, Reconstruct is Proxys, m-Delegate and m-Decrypt is PA, Decrypt is performed by the delegate.

First, Setup(*k*) : Security parameter *k* input receiving constructor g, to produce a *G0* of decimal places the number *p*. bilinear map is $\hat{e}: G_0 \times G_0 \to G_1$, a set of system properties is a $\Omega = (a_1, a_2, \cdots, a_n)$ (n is an integer), $a_i \in \Omega$ select $t_i \in Z_p^*$ that is any elements. In this procedure, we generate $y = \hat{e}(g,g)^o$, $\alpha \in_R Z_p^*$, $T_i = g^{t_1}(1 \le j \le n)$, public key($\hat{e}, g, y, T_i(1 \le j \le n)$), master key($mk = (\alpha, t_i(1 \le j \le n))$).

Second, KeyGen (mk, w, I_u) : This procedure generates a secret key in the set w and the delegation's identifier I_u of property. In the second process, system transmitted the first of the secret key share *x* to the PA, and it send a second secret key share *y* to delegate in the following procedure.

- Calculate the base component of the private key : Calculate the $d_0 = g^{\alpha\ u_W}$ and $u_{id} \in_R Z_p^*$.
- Calculate the attributes component of the secret key : Select the attributes $a_i \in w, u_i \in_R Z_p$. And calculate the $d_{i,1} = g^{u, t_1\ 1}$ and $d_{i,2} = g^{(u_n\ u_1)t_1\ 1}$.

Third, Encrypt(m, τ, pk)($m \in G_1$) : We select $s \in Z_p^*$ randomly. And generate cipher-text $c_0 = g^s, c_1 = m \bullet y^s = m \bullet \hat{e}(g,g)^{\alpha s}$. And we compose access structure τ. In this time we set root node is s. When

we make access structure, if we have AND gate($\wedge$), set leaf attribute to $s_i \in_R Z_p^*$. And last attribute is $s_n = s - \sum_{i=1}^{n-1} s_1$. And if we have OR gate($\vee$), set leaf attribute to value of root node. And last attribute set $a_{j,i} \in \tau, c_{j,i} = T_i^{s1}$. And delegator make cipher-text($c_\tau = (\tau, c_0, c_1, \forall\ a_{j,i} \in \tau : c_{j,i})$).

Fourth, Delegate($sk_{wI_{u2}}, \hat{w}, I_j$) : Select $r' \in_R Z_p$, generate k-1 order of any polynomial of $f(0) = r'$.

- Generate : $f(x) = r' + f_1 x + f_1 x^2 + \cdots + f_{k-1} x^{k-1}$
- Using each identifier $ID_i (1 \le i \le n)$ of Proxys, to calculate the $f(ID_i) = p_i$ and $g^p = E$.
- Set the $g^{t_1 r'} = g^{r\hat{i}}$ by $a_i \in \hat{w}$. And set the attribute conversion key $sk_{w \to \overline{w}} = g^{r'}$ and calculate $\hat{d}_{i,2}$ by $a_i \in \hat{w}$.
- - Calculate a $\hat{d}_{i,2}$ given with expression (1).

$$\begin{aligned} \hat{d}_{i,2} &= g^{(u_n - u_1)t1^{-1} r'} \\ &= g^{(u_n - u_1)t1^{-1} r_1' t1^{-1}} \\ &= g^{(u_n - u_1)t1^{-1} r'} \\ &= u_i + r_i'' \end{aligned} \tag{1}$$

- System transmits secret key share $sk_{\hat{w}I_{u2}} = (d_0, \forall\ a_j \in \hat{w} : \hat{d}_{j,2})$ to delegate and attribute set $\hat{w}$ to PA. And it send *n* size attribute conversion key share g^{p1} to proxy.

Fifth, Reconstruct ($g^{p1} (1 \le i \le n)$) : proxy received attribute conversion key share g^{p1} over threshold value such as k, and it calculate k_i .

- In this time, proxy calculate by expression (2).

$$k_i = \prod_{\substack{i \ne j \\ i \in Q_k}} \frac{ID}{ID_i - ID_j} \tag{2}$$

(Q_k : To *k* or more of the proxy).

- Proxy calculate $E^{k1} = (g^{p1})^{k1}$.
- Proxys calculate E^{k1} and reconstruct $sk_{w \to \overline{w}} = g^{r'}$ by expression (3).

$$\prod_{i \in Q_k} E^{k1} = g^{\sum_{i \in Q_k} (p_1 \cdot k_1)} = g^{\sum_{i \in Q_k} (\prod_{i \in Q_k} \frac{ID}{ID_i - ID_j})} = g^{r'} \tag{3}$$

Sixth, m-Delegate ($sk_{wI_{u1}}, \hat{w}, sk_{w \to \overline{w}}$) : checks an attribute delegation list. If it is attribute delegate target, calculate $sk_{wI_{u1}}$ by $a_i \in \hat{w}$. But if not, don't any calculation. When we use this expression (4).

$$\hat{d}_{i,1} = g^{ut1^{-1} + r'} = g^{\overline{u}t1^{-1}} \tag{4}$$

Seventh, m-Decrypt ($c_\tau, sk_{wI_{u1}}, I_j$) : checks attribute revocation list. If it is a don't attribute revocation target, calculate . but if he is revocation target, we don't any calculation. In this time, we use this expression (5).

$$\begin{aligned} &\hat{c}_{j,i} = \prod_{a \in \overline{w}} \hat{e}(T_j^s, g^{\overline{u}t1^{-1}}) = \hat{e}(g,g)^{\sum_{a \in \overline{w}} \overline{u}_1 s_1} \\ &\hat{c}_\tau(\hat{\tau}, c_0, c_1, \forall\ a_{i,j} \in \hat{\tau} : \hat{c}_{i,j}) \end{aligned} \tag{5}$$

Eighth, Decrypt ($\hat{c}_\tau, sk_{wI_{u2}}$) :

- Calculated with all the attributes using expression (6).

$$c_\tau'' = \prod_{a \in \overline{w}} \hat{e}(T_j^{s_i}, g^{(u_k \quad \bar{u}_1)t_1 \quad 1}) = \prod_{a \in \overline{w}} \hat{e}(g^{t_i s_i}, g^{(u_k \quad \bar{u}_1)t_1 \quad 1}) = \hat{e}(g,g)^{\sum_{a \in \overline{w}} (u_k \quad \bar{u}_1)s_i} \tag{6}$$

- And calculate given with expression (7).

$$\hat{e}(c_0, d_0) \bullet \hat{c}_{j,i} \bullet c_\tau'' = \hat{e}(g^s, g^{a \quad u_i}) \bullet \hat{e}(g,g)^{\sum_{a \in \overline{w}} \bar{u}_i s_i} \bullet \hat{e}(g,g)^{\sum_{a \in \overline{w}} (u_i \quad \bar{u}_1)s} = \hat{e}(g^s, g^{a \quad u_i}) \bullet \hat{e}(g,g)^{u_i s} = \hat{e}(g^s, g^a) \tag{7}$$

- Conversion of m by expression (8).

$$m = \frac{c_1}{\hat{e}(g^s, g^a)} = \frac{m \bullet \hat{e}(g,g)^{as}}{\hat{e}(g^s, g^a)} \tag{8}$$

4. Analysis

4.1. Analysis between CP-ABE, CP-ABTD and Proposed Scheme

Attributes based encryption (CP-ABE) is safer than a conventional encryption method (a public key based encryption, an ID-based encryption). So Encryption scheme of attribute-based, rather than traditional encryption method, with which is a safety feature to the malicious user's public attack. However, in comparison with the recently proposed attribute withdrawal is possible attribute-based encryption (CP-ABTD), property-based encryption (CP-ABE) is, withdraw the delegation of the delegation features and user attribute of the user's attributes function is not. CP-ABTD as compared to conventional CP-ABE, either delegate property may provide the ability to withdraw. However, although CP-ABTD also possible processing authority delegation, we are not able to present a clear model that can solve this. Not only, it is not safe for the loss or alteration of attribute conversion key. Therefore, CP-ABTD is possible to malicious attackers attribute conversion key modulation attack.

Therefore, we proposed a secure system for delegation modulation attack the privileges of the CP-ABTD to base. Delegate In the proposed system to provide shared information for access to the delegate, the proxy is designed to be able to prove that you have legitimately accessed the contrary. Here, the sense of determining the validity for the delegate access in each granted the share of conversion key attribute that is divided into dynamic threshold password Proxys has grasped the identity of the delegate using the share of only the threshold at the time of approving access after, and generates an original of attribute conversion key.

Dynamic threshold password used to delegate the viewing authority of the encrypted data can solve the problem for modulation attacks was noted with CP-ABTD. In other words, if more of the share threshold is maintained, but you can restore the attribute conversion key, it is impossible to attribute conversion key restoration when it comes to the threshold or less of the share exists. From this point of view, the safety of this method is the possibility to be restored in accordance with the share amount of information needed to restore the attribute conversion key is determined. Example, information theoretical safety (information-theoretic based on secure).

Table 1 shown to compare with CP-ABE, CP-ABTD and our proposed scheme about security properties.

Table.1. Compare with CP-ABE, CP_ABTD and Proposed scheme

(◯ : Good, △ : General, X : None)

	CP-ABE	CP-ABTD	Proposed Scheme
Attribute withdrawal	×	○	○
Delegation of authority	×	×	○
Safety against of a collusion attack	○	○	○
Safety against of a tampering attack	×	×	△

4.2. Analysis of Safety

Safety against of a collusion attack.

The most important security features in the attribute-based encryption scheme is a safety for the collusion attack. It is to combine the set of properties to the two or more users to extend their decryption authority.

For example, there is a cipher text that has been configured in the access structure $r = (a1 \wedge a2)$. User A's private key is composed of a set of properties $WA = (a1, a3)$, and User B's private key is composed of a set of properties $WB = (a2, a4)$. Collusion attack generates a private key associated with the $WA \cup WB = (a1, a2, a3, a4)$ by combining the secret key of the user A and user B, and browsing the configured encryption by access structure $r = (a1 \wedge a2)$.

However, the proposed system is safe for collusion attack with CP-ABTD. Because our system have a novel Keygen algorithm. It have the unique identifier for each user that is generated using any of random included in the private key.

TA cannot know U_{id} such as each user determined in any random number. It is impossible to combine the private key for the collusion attack. Therefore, the proposed scheme is secure against collusion attacks that combine the secret key between users A and B. And, it is impossible even collusion attack between the proxy and the user. For example, User B, in collusion with the malicious proxy, it tries to convert the passphrase for the user A to your passphrase. At this time, in order to convert the passphrase, it is necessary to user A generates a delegate attribute conversion key $gr'(r' \in R\ Z\ P)$ access to a user B.

At this time, if the attribute conversion key is not generated, re-encryption is not performed. Therefore, the proposed scheme is secure against collusion attack between the proxy and the user.

Modulation attack of attribute conversion key.

Attribute conversion key share of modulation attacks and attribute conversion key share ${}_gP_i\ (1 \le i \le n)$ is lost, or through the modulation, meaning an attack that original attribute conversion key *gr"* and so can't be recombinant to. However, CP-ABTD because with only attribute conversion key, or the value is lost, it is impossible to perform the re-encrypted if modulation. This is a very serious problem. Therefore, the proposed system, the attribute conversion key *gr"* the attribute conversion key share ${}_gP_i\ (1 \le i \le n)$ in minutes only recombinant k or higher share the original attribute if unless gather at the time of the dynamic threshold encryption it is possible to construct a conversion key gr". For example, for ${}_gP_i\ (1 \le i \le n)$, assuming that $n = 5, k = 3, gP1, gP2, gP3, gP4$, ten thousand gr if unless gather three of the share of the *gP5"* possible to find the can. In other words, it is not possible to restore the conversion key if you do not know all the k number of share, for on a general communication is very difficult to collect a share, the proposed scheme is a safety.

8.Conclusion

In everyday life, IoT and M2M communication is a computing paradigm to process the information based on the sensor. Data is saved by concentrated data, such as cloud computing, the availability of information to process is not satisfied.

The number of information of the moving object that is collected in future smart transportation network is enormous. In such a simple traffic forecast uses a centralized data, but there is a need for real-time like at present radio waves of the accident etc. Further, when tracking a particular vehicle, must provide information such as IDs, positions of the corresponding and driving record. But In the case of a general vehicle is concerned infringement of privacy such as information leakage.

To solve these problems, in this paper, the data processed and stored in cloud server, it process and transmit information by a proxy. The encrypted data is transmitted in consideration of the information leakage, Here,

investigative agencies of a secondary user was performed re-encryption can be restored only information about the specific vehicle. In this paper, we proposed the approval system of proxy-based data access rights that are suitable for fog computing environment using the CP-ABTD and dynamic threshold cryptography.

CP-ABTD have a safety against malicious users of public attack. But it could not be proven safety against the falsification of the conversion key share of the attributes. Therefore, we proposed a proposed system that it is possible to prevent the modulation attack of attribute conversion share. System is using a dynamic threshold encryption technology. And it is necessary to generate a re-encryption key each time the attribute withdrawal occurs has a problem. For this reason, the proposed up to now the system has the drawback of load on the calculation occurs. So we has plans to run additional future research, on how to solve this problem.

Acknowledgments

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2019R1F1A1056507).

References

A. Nakao, A. (2013). Objectives of SDN in future network. Electronics. Information and Communication Journal, 96(12), 902-905.
B. Jang, E. J., & Shin, S. J. (2020). Proposal of New Data Processing Function to Improve the Security of Self-driving Cars' Systems. The Journal of The Institute of Internet, Broadcasting and Communication, 20(4), 81-86.
C. Park, C., & Cha, J. (2019). Analysis of Component Technology for Smart City Platform. International Journal of Advanced Culture Technology, 7(3), 143-148.
D. Maruyama, H. (2014). Edge-heavy data and architecture in the big data era. Journal of Information Processing and Management, 56(5).
E. Hwang, C., Kim, H. S., Lee, J. Y., & Jung, K. (2017). A study on BSN data collection technique through mobile devices in a cloud environment. International journal of advanced smart convergence, 6(2), 82-88.
F. Ibraimi, L., Petkovic, M., Nikova, S., Hartel, P., & Jonker, W. (2009). Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes.
G. P. Robinson, H. Vogt and W. Wagealla, Privacy, Security, and Trust within the Context of Pervasive Computing, Springer-Verlag, 2005.
H. Song, Y. J. (2016). Data Access Privilege Management with a Revocation Period in a Cloud Environment. International Journal of Software Engineering and Its Applications, 10(7), 127-134.
I. Blaze, M., Bleumer, G., & Strauss, M. (1998, May). Divertible protocols and atomic proxy cryptography. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 127-144). Springer, Berlin, Heidelberg.
J. Mambo, M., & Okamoto, E. (1997). Proxy cryptosystems: Delegation of the power to decrypt ciphertexts. IEICE transactions on fundamentals of electronics, Communications and computer sciences, 80(1), 54-63.
K. Hong, K., Lillethun, D., Ramachandran, U., Ottenwälder, B., & Koldehofe, B. (2013, August). Mobile fog: A programming model for large-scale applications on the internet of things. In Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing (pp. 15-20).
L. Roy, S., Bose, R., & Sarddar, D. (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.
M. Bethencourt, J., Sahai, A., & Waters, B. (2007, May). Ciphertext-policy attribute-based encryption. In 2007 IEEE symposium on security and privacy (SP'07) (pp. 321-334). IEEE.
N. Jakobsson, M. (1999, March). On quorum controlled asymmetric proxy re-encryption. In International Workshop on Public Key Cryptography (pp. 112-121). Springer, Berlin, Heidelberg.
O. Jung, T. W., Lee, J. Y., & Jung, K. D. (2020). Traffic-based reinforcement learning with neural network algorithm in fog computing environment. International Journal of Internet, Broadcasting and Communication, 12(1), 144-150.
P. Moon, S. H. (2020). Big Data Platform Construction and Application for Smart City Development. The Journal of the Convergence on Culture Technology, 6(2), 529-534.