International Journal of Advanced Culture Technology Vol.10 No.2 225-232 (2022)
DOI https://doi.org/10.17703/IJACT.2022.10.2.225

IJACT 22-6-30

Proxy based Access Privilige Management for Tracking of Moving Objects

[1]Hyun-Jong Cha, [2]Ho-Kyung Yang, [3]You-Jin Song*

[1]Dr., Dept. of Multimedia Science, Chungwoon Univ., Korea
[2]Prof., Dvision. of Information Technology Education, Sunmoon Univ., Korea
[3]Prof., Dept. of Information Management, Dongguk Univ., Korea
E-mail chj826@kw.ac.kr, porori0421@naver.com, song@dongguk.ac.kr

Abstract

When we drive a vehicle in an IoT environment, there is a problem in that information of car users is collected without permission. The security measures used in the existing wired network environment cannot solve the security problem of cars running in the Internet of Things environment. Information should only be shared with entities that have been given permission to use it.

In this paper, we intend to propose a method to prevent the illegal use of vehicle information. The method we propose is to use attribute-based encryption and dynamic threshold encryption. Real-time processing technology and cooperative technology are required to implement our proposed method. That's why we use fog computing's proxy servers to build smart gateways in cars. Proxy servers can collect information in real time and then process large amounts of computation. The performance of our proposed algorithm and system was verified by simulating it using NS2.

Keywords: *Proxy, Access Authorization, Attribute Transformation Key, Dynamic Threshold Cryptography*

1. INTRODUCTION

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[1-4].

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. 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 [5].

In this paper, in order to solve these problems, we proposed a accept access authority scheme using the CP-

Manuscript received: May 25, 2022 / revised: June 2, 2022 / accepted: June 7, 2022
Corresponding Author: song@dongguk.ac.kr
Tel: +82-54-770-2347, Fax: +82-54-770-2001
Professor, Dept. of Information Management, Dongguk Univ., Korea

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[6].

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.

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. 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[7].

2.2 CP-ABTD and Bilinear Mapping

User's private key in the CP-ABE (CP-ABE, Ciphertext Policy Attribute Based Encryption) 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[5].

CP-ABTD(Ciphertext Policy Attribute Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes) 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 [8].

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. PROPOSAL SCHEME

3.1 Dynamic Threshold Cryptography

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 1. Our proposal model is a computing environment that has a proxy node with calculation and routing functions based on SDN (Software Defined Network).

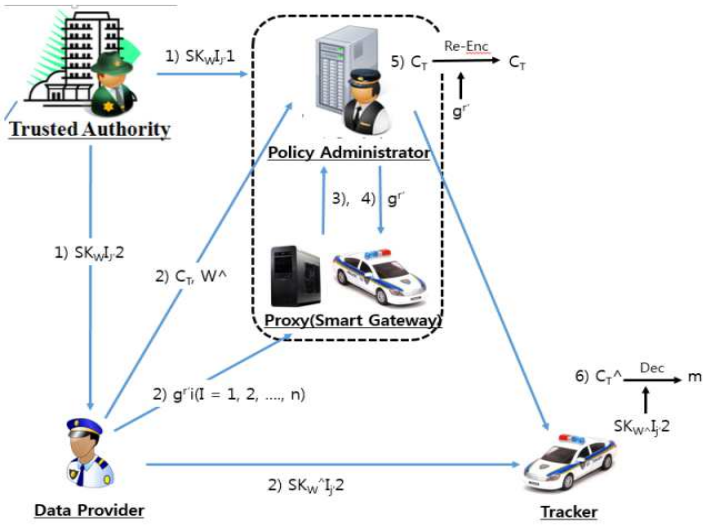

Figure 1. Our Proposal model

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 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 $\hat{e}: G_0 \times G_0 \rightarrow G_1$, a set of system properties is a $\Omega = (a_1, a_2, \cdots, a_n)$ (n is an integer), select $t_i \in Z_p^*$ that is any elements. In this procedure, we generate $y = \hat{e}(g,g)^o$, $\alpha \in {}_R Z_p^*$, $T_i = g^{t_1} (1 \leq j \leq n)$, public key($\hat{e}, g, y, T_i (1 \leq j \leq n)$), master key($mk = (\alpha, t_i (1 \leq j \leq n))$).

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$(m, \tau, pk)(m \in G_1)$: 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(∧), 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(∨), set leaf attribute to value of root node. And last attribute set $a_{j,i} \in \tau, c_{j,i} = T_i^{s_1}$. And delegator make cipher-text$(c_\tau = (\tau, c_0, c_1, \forall a_{j,i} \in \tau : c_{j,i}))$.

Fourth, Delegate$(sk_{w I_{u2}}, \hat{w}, I_j)$: 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 $ID_i (1 \leq i \leq n)$ of Proxys, to calculate the $f(ID_i) = p_i$ and $g^p = E$.
- Set the $g^{t_1 r'} = g^{r \hat{t}}$ by $a_i \in \hat{w}$. And set the attribute conversion key $sk_{w \rightarrow \overline{w}} = g^{r'}$ and calculate $f_1 x$ by $a_i \in \hat{w}$.
- Calculate a $\hat{d}_{i,2}$ given with expression (1).

$$\begin{aligned} \hat{d}_{i,2} &= g^{(u_n \quad u_1) t1 \quad 1 \quad r'} \\ &= g^{(u_n \quad u_1) t1 \quad 1 \quad r \hat{t} 1 \quad 1} \\ &= g^{(u_n \quad u_1) t1 \quad 1 \quad r'} \\ &= u_i + r_i'' \end{aligned} \tag{1}$$

- 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^{p_1} to proxy.

Fifth, Reconstruct $(g^{p_1} (1 \leq i \leq n))$: proxy received attribute conversion key share g^{p_1} over threshold value such as k, and it calculate k_i.

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

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

- (Q_k: To k or more of the proxy).
- Proxy calculate $E^{k_1} = (g^{p_1})^{k_1}$.
- Proxys calculate E^{k_1} and reconstruct $sk_{w\to\bar{w}} = g^{r'}$ by expression (3).

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

Sixth, m-Delegate $(sk_{wI_u1}, \hat{w}, sk_{w\to\bar{w}})$: 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).

$$\hat{d}_{i,1} = g^{ut_1{}^{-1}+r'} = g^{\bar{u}t_1{}^{-1}} \tag{4}$$

Seventh, m-Decrypt $(c_\tau, sk_{wI_u1}, I_j)$: checks attribute revocation list. If it is a don't attribute revocation target, calculate c_τ. but if he is revocation target, we don't any calculation. In this time, we use this expression (5).

$$\hat{c}_{j,i} = \prod_{a\in\bar{w}} \hat{e}(T_j^s, g^{\bar{u}t_1{}^{-1}}) = \hat{e}(g,g)^{\sum_{a\in\bar{w}}\bar{u}_1 s_1}$$

$$\hat{c}_\tau(\hat{\tau}, c_0, c_1, \forall a_{i,j} \in \hat{\tau}: \hat{c}_{i,j}) \tag{5}$$

Eighth, Decrypt $(\hat{c}_\tau, sk_{wI_u2})$:

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

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

- And calculate given with expression (7).

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

- Conversion of m by expression (8).

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

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.

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 Uid 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' ∈ 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 recombined.

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 $n = 5, k = 3$, $_gP_1$, $_gP_2$, $_gP_3$, $_gP_4$, ten thousand gr if unless gather three of the share of the $_gP_5"$ 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.

5. CONCLUSION

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.

REFERENCES

[1] Jang, Eun-Jin, and Seung-Jung Shin, "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*, Vol. 20, No. 4, pp.81-86, 2020.

[2] Park, Chulsu, and Jaesang Cha, "Analysis of Component Technology for Smart City Platform," *International Journal of Advanced Culture Technology*, Vol. 7, No.3, pp.143-148, 2019.

[3] Jung, Tae-Won, Jong-Yong Lee, and Kye-Dong Jung, "Traffic-based reinforcement learning with neural network algorithm in fog computing environment," *International Journal of Internet, Broadcasting and Communication*, Vol. 12, No. 1, pp.144-150, 2020.

[4] Moon, Seung Hyeog, "Big Data Platform Construction and Application for Smart City Development," *The Journal of the Convergence on Culture Technology*, Vol. 6, No. 2, pp.529-534, 2020.

[5] Ibraimi, L., Petkovic, M., Nikova, S., Hartel, P., & Jonker, W., "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," *IEEE Trans*. Image process, 2009.

[6] Song, You-Jin, "Data Access Privilege Management with a Revocation Period in a Cloud Environment," *International Journal of Software Engineering and Its Applications*, Vol. 10, No. 7, pp.127-134, 2016.

[7] Blaze, Matt, Gerrit Bleumer, and Martin Strauss, "Divertible protocols and atomic proxy cryptography," in *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, pp.127-144, 1998.

[8] Bethencourt, John, Amit Sahai, and Brent Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE symposium on security and privacy (SP'07)*, IEEE, pp.321-334, 2007.