International Journal of Multimedia and Ubiquitous Engineering
Vol.8, No.6 (2013), pp.97-104
http://dx.doi.org/10.14257/ijmue.2013.8.6.10

# Context-Aware Information-Based Access Restriction Scheme for Cloud Data

Seul-Ki Choi[1] and Jin Kwak[2*]

[1]*ISAA Lab, Department of Information Security Engineering, Soonchunhyang University, Korea*
[2]*Department of Information Security Engineering, Soonchunhyang University, Korea*

*skchoi@sch.ac.kr, jkwak@sch.ac.kr*

***Abstract***

*To provide secure and efficient access control methods in cloud computing environments, many system models have been proposed that employ attribute-based encryption and proxy re-encryption schemes. Most of these access control schemes are based on the user's authentication information and access privileges. However, when users request access privileges through non-secure environments such as mobile devices and wireless networks, we need to be able to restrict access requests, depending on the user's context-aware information. To achieve this, in this paper we propose an access restriction scheme for access to cloud data that is based on context-aware information.*

***Keywords:*** *Cloud Computing, Context-Aware, Attribute-Based Encryption*

## 1. Introduction

Cloud computing that provides computing resources through the Internet is a new computing paradigm that has attracted considerable attention in both academia and industry [1]. Cloud data centers have become increasingly popular due to their adoption of these cloud computing concepts. A cloud data center provides efficient management capability for large amounts of data, and offers easy accessibility through the network at any time and from any place. However, due to these very features of management capability and easy accessibility, a cloud data center can be vulnerable to new and existing security threats. Therefore, to prevent breaches in the security of cloud data, many studies are now being conducted regarding the control of data access control. The existing scheme controls access by making use of the user's role and privileges, but without considering the larger context of the user's information. Therefore, existing access control schemes are still vulnerable to security threats, because when a user accesses the cloud data center via a non-secure channel or a mobile device whose computational power is insufficient to perform encryption, the data owner cannot block the user's access request. Therefore, in this paper, we propose a context-aware information-based data restriction scheme for cloud data.

The remainder of this paper is organized as follows. In Section 2, we review the related research presented in Yu's scheme. In Section 3, we analyze security threats in Yu's scheme. In Section 4, we present our proposed scheme, and in Section 5, we analyze its security features. Section 6 presents our conclusions.

*Corresponding Author : Jin Kwak (jkwak@sch.ac.kr)

ISSN: 1975-0080 IJMUE

## 2. Related work

### 2.1. Yu's scheme

In Yu's scheme, data is composed of a header and body [2]. The header is configured to encrypt the data encryption key (DEK) based on a set of attributes. The body is the data that is encrypted using the secret key DEK. The data owner creates a data file by combining the header with the body, and sends the data file to the cloud service provider. The user can obtain the DEK when the user's secret key satisfies a set of attributes of the header, and the user decrypts the body using the DEK.

Yu's scheme performs updates using proxy re-encryption in order to efficiently revoke user access. With this method, it is impossible for the user to perform the operation if the user does not possess the attribute of the same version. To perform this operation, the data owner must create an access structure that includes a dummy attributes, as shown in Figure 1.

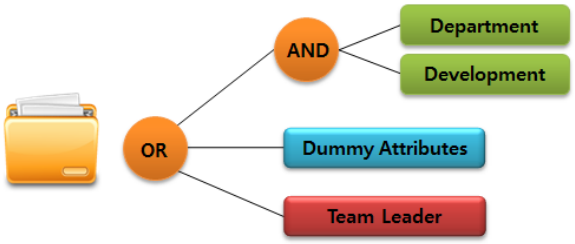


**Figure 1. Example of access structure in Yu's scheme**

Figure 2 shows the system configuration of the existing scheme. In this scheme, the data owner transmits encrypted data (body) and the encrypted DEK to the cloud service provider using attribute-based encryption. The cloud service provider then transmits the data file when the user requires the data.

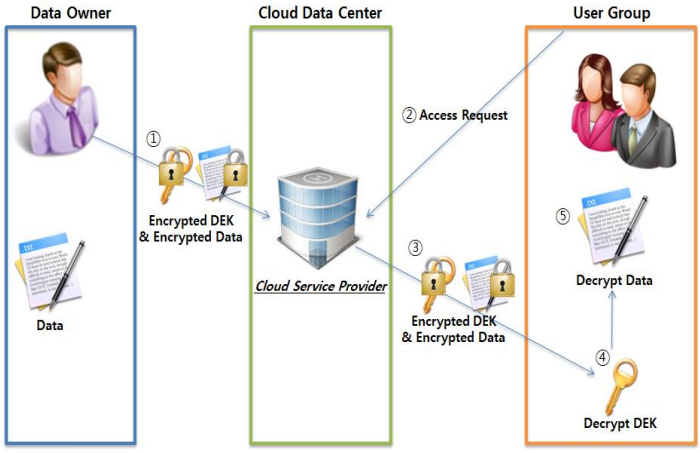


**Figure 2. System configuration of the existing scheme [1]**

## 3. Security Threat in Yu's Scheme

There are a variety of methods to access a cloud data center, because users use varying devices and network environments. Therefore, when various users access a cloud data center, their context information is always different. Yu's scheme controls access to the cloud data center, but it does so without considering the user's context information. As a result, existing access control schemes are vulnerable to the threat of data leakage.

For example, when there is a data access structure as shown as Figure 1, the team leader can access the data. However, the team leader is able access the cloud data center through a non-secure channel, or can also use a mobile device whose computational power is insufficient to perform the required encryption. In this case, if a cloud data center grants an access request by verifying the project manager's role and privileges, but does so without context information, the requested data is transmitted through a non-secure channel. This is why, in granting access requests, a cloud data center needs to consider the context information.

## 4. Our Proposed Scheme

Our proposed scheme uses an access structure that includes context-aware information, as shown in Figure 3.

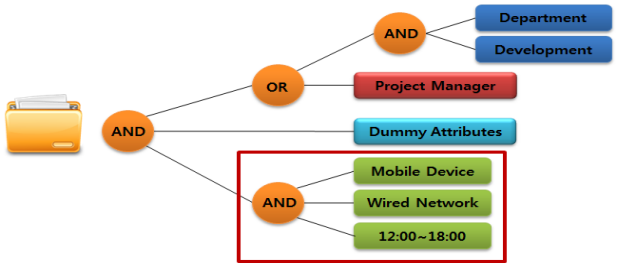


**Figure 3. Access structure of the proposed scheme**

The data owner obtains the user's context-aware information via a user/device authentication server that is located in the cloud data center. The data owner then assigns a set of attributes to each user and generates the corresponding secret key. Table 1 shows the system parameters that explain the details of the process of the proposed scheme.

**Table 1. System parameters**

| Notation | Description | Notation | Description |
|---|---|---|---|
| PK | System public key | DEK | Symmetric data encryption key |
| MK | System master key | L | A set of attributes for the user |
| AS | Access structure for the data | SK | User's secret key |
| $Data_{ID}$ | Unique ID for the data | UL | User list |

### 4.1. System setup

At this level, the data owner selects a security parameter k, and inputs this parameter into the A Setup(k) algorithm, which outputs a public key PK and master key MK.

### 4.2. New data upload

The data owner encrypts his data before transmitting it to the cloud data center. The details of the process are as follows.

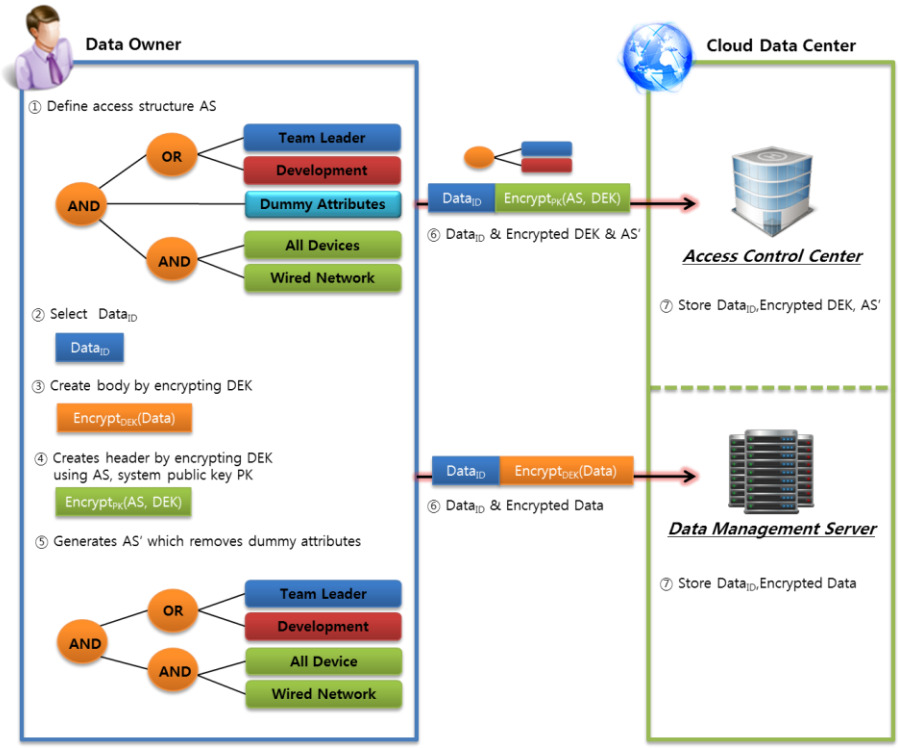


**Figure 4. New data upload process**

① The data owner defines the access structure AS, including the dummy attributes and the context-aware information.

② The data owner selects a unique ID for the data.

③ The data owner randomly selects a symmetric data encryption key DEK from the key space, and creates the body by encrypting the data file using DEK.

④ The data owner creates a header by encrypting DEK using AS, a system public key PK.

⑤ The data owner generates AS′, which removes the dummy attributes.

⑥ The data owner transmits DataID, the header (encrypted DEK), and AS′ to the access control center, and sends DataID and the body (encrypted data) to the data management server.

⑦ The access control center and data management server receive DataID, the header, the body, and AS′ from the data owner, and stores them.

### 4.3. Granting access to a new user

For a new user to be granted access to the system, the data owner assigns an access structure and a corresponding secret key to this user, as follows.

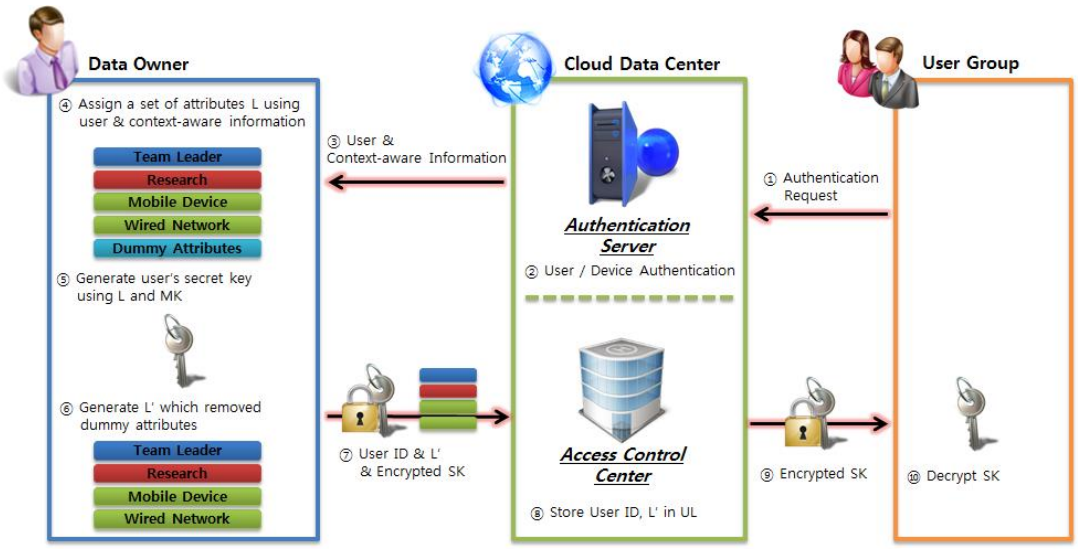


**Figure 5. Process for granting access to a new user**

① The user sends an authentication request message to the user/device authentication server.

② The authentication server receives the request message from the user and obtains user's information, including roles, privileges, and context-aware information.

③ The authentication server sends the user and the context-aware information to the data owner.

④ The data owner assigns a set of attributes L to the user using the user's basic information and context-aware information.

⑤ The data owner generates the secret key SK for the user using the AKeyGen(L, MK) algorithm, and encrypts the user's secret key SK using the user's public key.

⑥ The data owner generates L′, which removes the dummy attributes.

⑦ The data owner transmits the user ID, the encrypted SK, and L′ to the access control center.

⑧ The access control center stores the user ID and L′ in the user list UL.

⑨ The access control center sends the user's secret key to the user.

⑩ The user decrypts the secret key using his private key and obtains his secret key SK.

### 4.4. Data access

When the user sends a request message to the cloud data center, the access control center determines the user's access privilege and transmits the cloud data via the data management server.

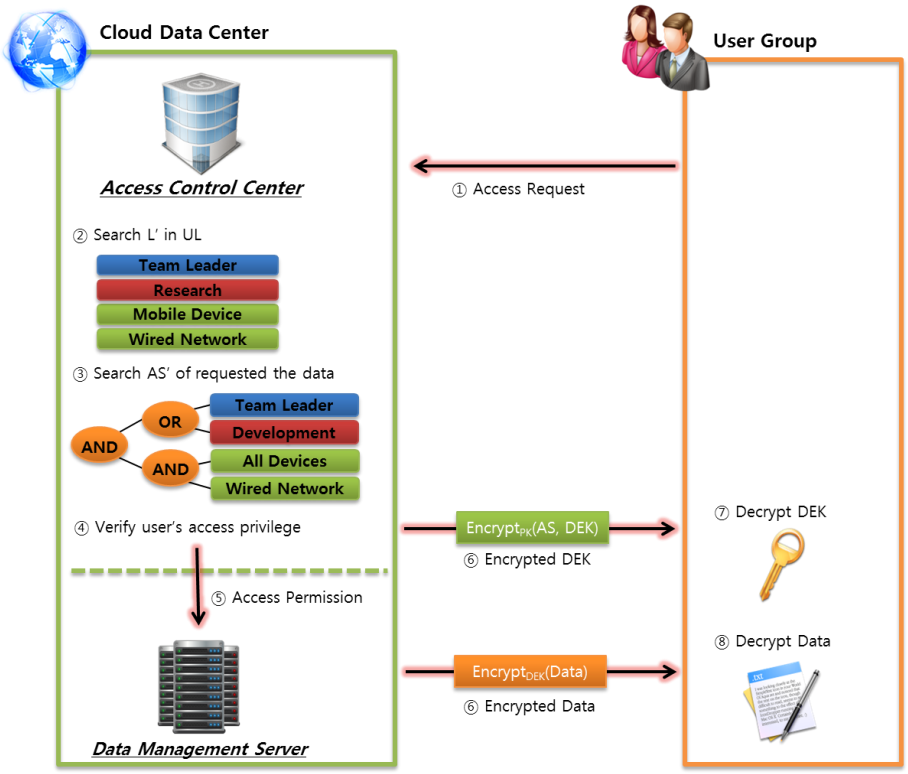


**Figure 6. Data access process**

① The user sends an access request message to the cloud data center in order to access cloud data.

② On receiving an access request message, the access control center searches for L′ in UL.

③ The access control center searches for the AS′ of requested data.

④ The access control center verifies the user's access privileges using L′ AS′.

⑤ If the user's access privilege is verified, the access control center sends an access permission message to the data management server.

⑥ The access control center and data management server send the header and the body to the user.

⑦ The user obtains the DEK by decrypting the header using his secret key SK.

⑧ The user obtains the data by decrypting the body using DEK.

### 4.5. Data deletion

This operation is performed only when the data owner's request is received. To delete data, the data owner sends a data deletion request along with his signature to the access control center and the data management server. If the data owner's signature is verified, the data is deleted.

## 5. Security Analysis of Our Proposed Scheme

In our proposed scheme, the data owner can obtain the context information of users who access the cloud data center through the user/device authentication server. Accordingly, the data owner is able to assign a suitable and flexible access structure depending on the access environment of each user. Therefore, when a user accesses the cloud data center through a non-secure channel or via a mobile device whose computational power is insufficient to perform encryption, the data owner can block the user's access request. Thus, the access control offered by our proposed scheme is superior to that offered by the existing scheme.

## 6. Conclusions

Cloud computing is an innovative computing paradigm that provides computer resources as a service. A cloud data center also offers many advantages due to its adoption of cloud computing concepts. A cloud data center can manage large amounts of data, and it provides easy accessibility as a service. Such centers, however, are quite vulnerable to security threats due to the features of cloud services. In response to this situation, many studies regarding data access control are currently being conducted. Existing schemes control access without considering the context information of the user. Therefore, we proposed in this paper a data access control scheme that takes the user's context information into consideration. As a result, our proposed scheme assigns access in a manner that is both suitable and flexible. The one shortcoming of our scheme that needs to be addressed, though, is the probable overload that will occur due to the frequent generation of secret keys.

## Acknowledgements

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2012-010886).

## References

[1] Y. -J. Song and J. -M. Do, "Secure Data Management based on Proxy Re-Encryption in Mobile Cloud Environment", The Journal of Korea Information and Communications Society, vol. 37B, no. 04, **(2012)**, pp. 288-299.
[2] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE INFOCOM, **(2010)** March, pp. 1-9.
[3] G. Kulkarni, J. Gambhir and T. Patil, "Security Aspects in Cloud Computing", Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd Internal Conference, **(2012)**, pp. 547-550.
[4] D. Jamil and H. Zaki, "Cloud Computing Security", International Journal of Engineering Science and Technology (IJEST) **(2011)**, pp. 3478-3483.

# Authors

**Seul-Ki Choi**

He received his B.S. degree in Information Security from Soonchunhyang University (SCH), South Korea, in 2013. Currently, he is an M.S. candidate at the Information Security Application and Assurance Lab, SCH. His research interests include cloud data security, smartwork security, and cryptology.

**Jin Kwak**

He received his B.S. (2000), M.S. (2003), and Ph.D. (2006) degrees from Sungkyunkwan University (SKKU), Korea. Before joining the faculty at Soonchunhyang University (SCH) in 2007, he was a visiting scholar at Kyushu University, Japan. Subsequently, he served at the Ministry of Information and Communication (MIC), Korea, as Deputy Director. Furthermore, he served as Dean of the Department of Information Security Engineering (DISE) at SCH (2009–2010) and Vice-Dean of the College of Engineering (2009) at SCH. He is now Professor at DISE. In addition, he is Director of the SCH BIT Business Incubation Center and of the Industry-University & Institute Partnership Division Center at SCH. His main research areas are cryptology, information security applications, and information assurance.