Access Control Framework Design for Personal Cloud

1 Jun-young Park, 2Young-rok Shin, 3Kyoung-hun Kim, 4Eui-nam Huh,
1, First author, 2Kyung Hee University, {parkhans, shinyr}@khu.ac.kr
3 Gang Dong College, iioii.net@gmail.com
4, Corresponding Author Kyung Hee University, johnhuh@khu.ac.kr

Abstract Collaboration service has been receiving much attention to a personal user in cloud computing. But it has a lot of problems in privacy. While a user access cloud computing service, the cloud service provider can collect information of her without user agreement. To solve this problem, we define requirements of personal cloud Access Control (AC) and propose AC framework based on personal cloud service reference model.

Keywords: Personal Cloud, Cloud Access Control

1. Introduction

Nowadays many personal cloud services are provided by global IT companies. Also, Cloud computing service has been receiving much attention to personal user. Due to a personal user increasing, the problems of user privacy have been also increased. Cloud service providers serve comfortable service to individual user but they can collect personal information without user agreement.

Therefore we need privacy protection in Cloud computing service and security framework to conceal user information to cloud service providers.

In this paper, section 2 describes the personal cloud and reference model. Section 3 gives an overview of related existing AC methods. Section 4 defines requirements and proposes personal cloud AC framework. Section 5 gives the conclusions.

2. Personal Cloud

The personal cloud is a popular concept in these days. It describes a user-centric service model of cloud computing that a user is able to access her personal contents and services in anytime, at anywhere and with any devices [1, 2, 5].

2.1 Personal Cloud Reference Model

This model consists of user, 3rd party for user authentication, Collaboration Service Provider (CoSP) for managing the personal cloud service and Cloud Service Provider (CSP) as shown in figure 1 [2].

3. Related Access Control Method

Personal Cloud AC employs XACML and RBAC based on Personal Cloud reference model.

3.1 XACML

XACML (eXtensible Access Control Markup Language) defines the syntax for a policy language and the semantics for processing those policies. There is also a request and response format to query the policy system, and semantics for determining applicability of policies to requests [4].

3.2 Role-Based Access Control (RBAC) [3]

The roles are created by the system administrator to represent specific task competencies which determine resources types and each role can access. Individual users are assigned to certain roles according to their job functions. Each role is associated with a set of permissions. A many-to-many mapping exists between users to roles and roles to permissions.

4. Personal Cloud Access Control

4.1 Requirements of Personal Cloud AC

We defined several requirements of Personal Cloud access control that a generic AC model for collaborative environments should be supported.

Compatibility with Previous Security Policy: access control of personal cloud services need to provide compatibility with security
policy, which belongs to existing service, of web-service or cloud service rather than make each services-based security policy.

**Establish an Individual Security Policy:** personal cloud service is managed independently by CSPs. In this sense, each CSP should establish individual security policy to manage them.

**Cloud Service Collaboration and Inter-Cloud:** A user and service should be certified automatically in corresponding services for cloud service collaboration and inter-cloud by the AC model.

**User Privacy Guarantee:** The access control model should be able to protect clearly against violation of privacy in personal cloud. A CSP manager can violate user privacy so the model should support the user privacy protection from CSP using temporary ID.

**3rd-Party Auditor:** The access control model needs a trusted 3rd-party auditor for verifying and compliance regarding collaboration service.

**Access Control based SLA:** All of service providers should ensure SLA for QoS based on established access control policies.

### 4.2 Personal Cloud AC Framework

This framework employs well-known access control scheme such as RBAC, XACML and etc. In this sense, our proposed framework is able to apply to the other existing access control systems.

**3rd-Party Service Provider (SP)**

It is in charge of user authentication and audit concerning all service providers.

#### 5. Conclusion

In this paper, we defined requirements and proposed the access control framework for personal cloud service. Even though privacy must be considered and ensured, especially, it is often noted but rarely studied in this area. In the future, we will study on various AC techniques to improve the AC framework.

#### 6. Acknowledgement

This work was supported by the IT R&D program of MKE/KEIT. [10035321, Terminal Independent Personal Cloud System] Corresponding Author is Eui-Nam Huh.

#### 7. References


---

**Figure 2. Personal Cloud AC Framework**

**User** (Client) requests service access to **CoSP** using user’s device with personal information.

**Collaboration Service Provider (CoSP)** provides user authentication by the 3rd party SP.

**Policy Enforcement Point (PEP):** With service access request, the PEP verifies credential from 3rd party SP regarding user authentication in accordance with user’s service information. Then the credential-verification publish access token based on service information and authority.

**Cloud Service Provider (CSP)** is composed of PDP, PIP, and PAP and is able to generate, determine, store and delete security policy.

**Policy Decision Point (PDP)** requests access policy and user role information in order to verify authority. The permission check module compares access control list, user role and access policy and then decides permission.

**Policy Information Point (PIP)** stores security policy related cloud service and user permission in each service.

**Policy Administration Point (PAP)** manages security policy and policy list.