別表６
（３）

Keio University

# Thesis Abstract

| Registration Number | ■ "KOU"   □ "OTSU"<br>No.                    *Office use only | Name | BEN AYED SOUHEIL |
|---|---|---|---|

Thesis Title: A Study on Collaborative Access Control in a Multi-Domain Cloud Computing Environment

Thesis Summary

The Internet infrastructure is evolving with various approaches, such as grid computing, peer to peer and cloud computing, on the way to remove barriers between clients and providers. Interest in cloud computing is growing with the rise of new generation applications and services to access on-demand information technology resources at lower cost, particularly in business community. The cloud approach is expanding to a distributed multi-domain environment, called multi-domain cloud computing environment, where users have the ability to access securely IT resources across multiple domains. For delivering services securely, cloud computing providers are facing several security issues, including controlling access to services and ensuring privacy. Most of access control approaches tend to centralization of policy administration and decision by introducing a central third party mediator. However, with the growth of the Internet and the increase of cloud computing providers, a centralized administration is no longer supported. This dissertation studies the authentication and the authorization functionalities of access control in a distributed multi-domain cloud computing environment and defines a collaborative access control approach for multi-domain cloud computing environment by proposing a delegation-based access control across multiple cooperative domains. The proposed approach enables authenticating and checking user's authorizations for accessing a cloud resource in a visited domain that does not establish a direct cooperative relationship with the user's home cloud computing provider by establishing a path of cooperative delegations. In particular, the dissertation defines the infrastructure of the proposed multi-domain access control, including the authentication and authorization phases, and proposes access control framework for collaborative access control across multiple-cooperative domains. For enabling authentication across multiple domains, we implemented the first Diameter EAP server with a new state machine that defines the interaction with other layers and can support any EAP authentication mechanism as a plug-in. EAP plug-ins are implemented separately and are dynamically pluggable. The collaborative access control defined in this dissertation extends the XACML model by introducing a new entity called Delegation Validation Point (DVP) for supporting multi-delegation across multiple cooperative domains. In addition, four new SAML messages are added to the SAML profile for XACML in order to handle the XACML multi-delegations data between two successive cooperative domains. Two Diameter applications are defined for transporting securely multiple delegation requests and answers and for building a trusted path of cooperation to acquire the chain of delegations. The evaluation of a prototype of the proposed solution shows that the system leads to significant access control response across distributed cooperative domains.