Access Control of Cloud Service Based on UCON

Chen Danwei, Huang Xiuli, and Ren Xunyi

Nanjing University of posts & Telecommunications, New Model Street No.66, 210003, Nanjing, China
chendw@njupt.edu.cn, juliehxl@163.com, renxy@njupt.edu.cn

Abstract. Cloud computing is an emerging computing paradigm, and cloud service is also becoming increasingly relevant. Most research communities have recently embarked in the area, and research challenges in every aspect. This paper mainly discusses cloud service security. Cloud service is based on Web Services, and it will face all kinds of security problems including what Web Services face. The development of cloud service closely relates to its security, so the research of cloud service security is a very important theme. This paper introduces cloud computing and cloud service firstly, and then gives cloud services access control model based on UCON and negotiation technologies, and also designs the negotiation module.

Keyword: Cloud Service, Access Control, UCON, Negotiation.

1 Introduction

Cloud Computing is a large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet[1]. Cloud is the network which is constructed through cloud computing model, and cloud service is the service provided in cloud. Now, Cloud Computing has become the hottest technology in IT, and is also the research focus in academic.

The goal of cloud computing is to realize "the network is a high performance computer", that is to allow users to put all data and services into cloud and get all kinds of services from cloud only by their Internet terminal equipment. What users see is a virtual view when they use cloud service, and the data and services are actually distributed at different locations in cloud. The tendency that services and data will be transferred to web is inevitable, and more and more services and data will be in cloud.

Cloud service is based on Web Services [2], and Web Services are based on Internet. Internet has many its own inherent security flaws because of its openness, and it also has many other attacks and threats. Therefore, cloud services will face a wide range of security issues. At present, there are already many security specifications and technologies about Web Services, so it is of great significance for us to resolve security issues of cloud service using these existed security knowledge.

M.G. Jaatun, G. Zhao, and C. Rong (Eds.): CloudCom 2009, LNCS 5931, pp. 559–564, 2009.

Access control is one of the most important security mechanisms in cloud service, and Cloud service can not apply the traditional access control model to achieve access control because of its characteristics. But cloud services need to face the same security problems and Security requirements; and we also can't be divorced from the traditional access control model ideas.

For Unauthorized Access problems, it often built on fragile ID authentication and authorization. The mainly causes include: ①No authentication or fragile authentication; ②To send the password and authentication information in plaintext. The system should adopt a strong authentication system and make encryption transmission to prevent unauthorized access.

2 Cloud Services Access Control Based UCON

2.1 UCON Model

The usual traditional access control models include DAC, MAC and RBAC. New access control models have TBAC [3], ABAC [4], and UCON [5]. Cloud service usually has the following features: large amounts of resources, highly dynamic and flexible construction, lots of dynamic users, and so on. UCON can easily implement the security strategy of DAC, MAC and RBAC, and also includes security strategy of trust and DRM management covering security and privacy which are two important issues in the demand of Modern business information systems. As the next generation access control technology, besides taking ABC conception, UCON also inherits all the merits of traditional access control technologies, and can be established various access control model under every kinds of complex situation, and among them $UCON_{ABC}$ is the most integrated model.. UCON provides very superior decision-making ability, and will be a better choice to be used to establish cloud service access control model.

UCON is just a conceptual model, and no concrete realization specification, so there is still much work to do for establishing access control model based on UCON. UCON model is composed of six parts: Subjects, Rights, Objects, Authorization, oBligation, Conditions.

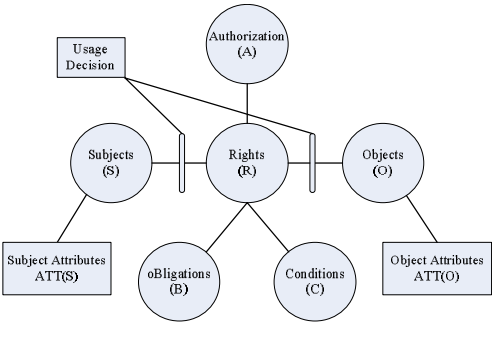

Fig. 1. UCON model

(l)Subject and Subject Attribute
Subject is an entity which has some rights of using object, marked as S. Subject means widely, it may be the user group, the user himself, or may also be a computer terminal, card machine, hand-held terminal (wireless), and even may be a program or process application.

Subject Attribute identifies the main capabilities and features of subject, and is the important parameter in the decision-making process, marked as ATT (S). The common subject attributes include: identity, user group, role, membership, and capacity list and security level.

(2)Object and Object Attribute
Object is an entity which accepts the visit of Subject, marked as O. Object also has a wide meanings, and it may be information, documents and records used in workflow system, or may be hardware on the network and wireless communication terminals.

Object Attribute identifies the important information of object, marked as ATT (O). Object attributes include security label, relations, type and access control lists and so on.

(3) Rights
Rights are a set of actions that subject visits object, marked as R. And the set also defines some conditions restriction that object request of subject. There are many types of rights.

(4) Authorization the principal,
Authorization is the only decision-making factor in the traditional access control model, and also is also an important part in UCON model, marked as A. Authorization is based on subject attributes, object attributes, as well as the right to request (for example: read or write privileges, etc.) and in accordance with the permission rules set to determine the operation of the authority. Implementation of authorization may lead to some changes to subject attribute or object attribute value, which will also impact on the decision-making process of this visit and the next.

(5) Obligation
Obligation is the function that must be implemented before visiting or during visiting, marked as B. What obligation should be fulfilled will be not statically set up by the system administrator in advance, and it is dynamically selected according to subject attributes and object attributes. The implementation of obligation may also update the variable attributes of the entities, which will also impact on the decision-making process of this visit and the next.

(6) Condition
Condition is the decision-making factor objected-condition and system, marked as C. Condition assesses the current hardware environment or relevant system limitations to decide whether or not to meet the user request. Conditions assessment doesn't change any subject attributes or object attributes.

2.2 Cloud Services Access Control Based UCON

2.2.1 Nego-UCON$_{ABC}$ Model

In UCON$_{ABC}$, authorization bases on attributes, obligations and conditions. Attributes are often provided in form of the digital certificate by which issuer declares the

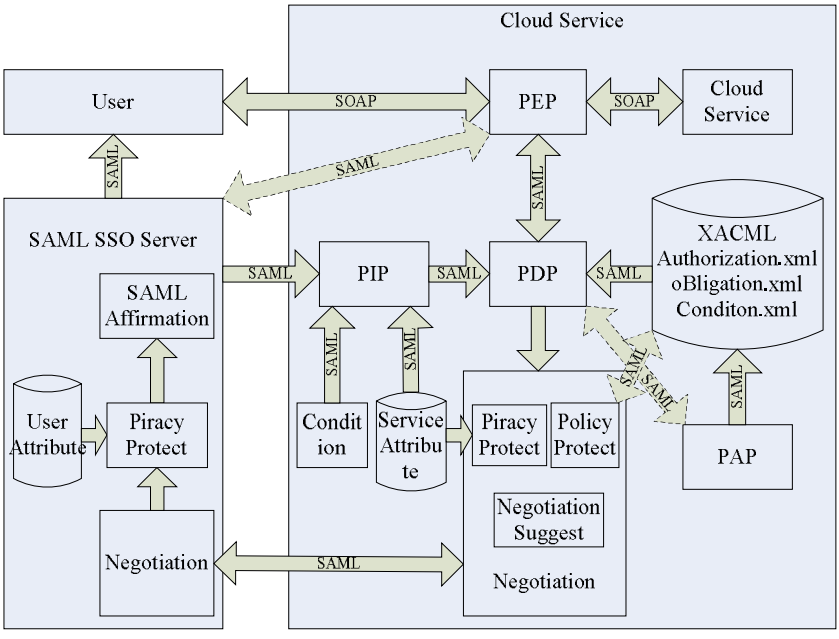

Fig. 2. Nego-UCON$_{ABC}$ model

attributes that an entity has. Obligations are storage in policy DB as rules in XACML [6]. Conditions will be obtained through the operating environment and be storied in policy DB as rules in XACML.

Besides, negotiation module is applied in model in order to enhance flexibility of cloud service access control. When access request mismatches with access rules, it allows user to get a second access choice through negotiation in certain circumstances, in stead of refusing access directly. That is, user can get chance to access through changing certain parameters and attributes in the negotiation process.

Authorization of UCON model bases on entity's attributes and access policies, but sometimes these attributes and policies are sensitive and need to be protected. And we need consider the protection of these sensitive attributes and policies in negotiation. Figure 2 is Nego-UCON$_{ABC}$ model bases on UCON$_{ABC}$ and negotiation.

Figure 2 includes three parts: Cloud user, SAML server and Cloud service. Cloud user is the initiator in service request. And SAML Server part includes three modules: SAML assertion module, sensitive attributes protection module and negotiation module. SAML assertion module mainly issues assertions and responses to assertions requests. Sensitive attributes protection module used to protect user's sensitive attributes and will be called when SAML issues assertion, and then attributes will be exposed according to the privacy polices. Negotiation module is used to negotiate with cloud server for attributes, obligations and conditions.

Cloud service part includes seven modules: Cloud service, PEP, PDP, PIP, PAP, XACML policy DB and negotiation module. Cloud service is the service provider. PEP is the policy enforcement point, and it accepts user's requests, and then executes decision of PDP. PDP is the policy decision point, it make authorization decision

based on ABC policies according to the entity attributes, obligations, conditions. PIP is the policy information point, it get entity attributes and conditions and provides them to PDP for making decision. PAP is policy administration point, and it makes and manages polices. XACML policy DB stores ABC polices, and polices are expressed in extensible access control markup Language in it. Negotiation module is used to negotiate with cloud user for attributes, obligations and conditions.

2.2.2 Nego Module

Nego module is added for enhancing flexibility of access control model. When user attributes are insufficient or condition parameters are inconsistent, the negotiation module will run. Nego module is shown in Figure 3. The whole module running process is divided into three negotiation levels: attributes query, attributes automatic negotiation [7] and artificial negotiation. Attribute query will start querying user's attribute when attributes are insufficient, and negotiation will end if getting the wanted attributes. Otherwise attribute automatic negotiation will run, this negotiation level will help get the wanted attributes according to attributes privacy polices of both sides, and negotiation will end if getting the wanted attributes. And if attribute automatic negotiation even has no result, cloud service will want user to participate in artificial negotiation, and cloud service will send negotiation suggestions to user firstly, then user will adjust his privacy policy for providing his attributes or change his conditions requests to meet demand of visit cloud service.

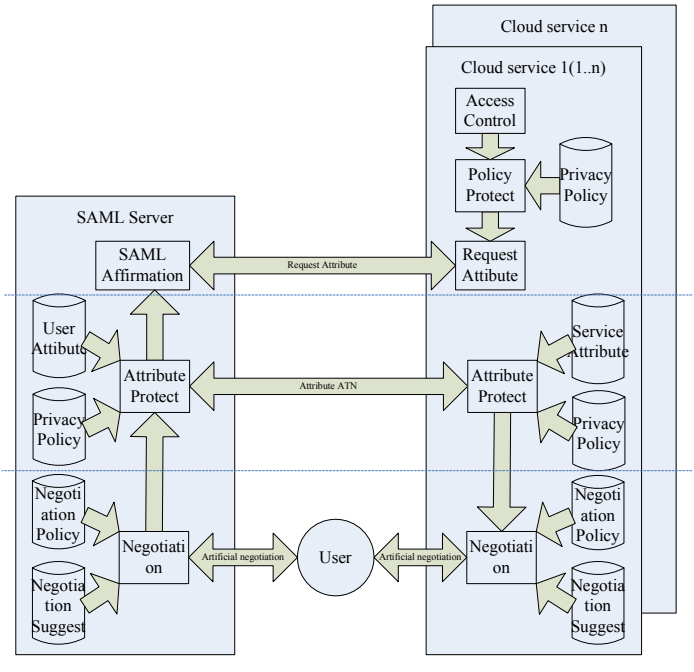

Fig. 3. Nego module

Nego module mainly includes two parts: SAML server and Cloud service.

SAML server part has three modules: SAML assertion, attribute protect and negotiation. SAML module response the requests of user attribute from cloud service, and attribute protect module protects privacy attribute during attributes automatic negotiation, and negotiation module provides the third way to visit cloud service by artificial negotiation.

Correspondingly, Cloud service part has three modules: Policy Protect, Attribute Protect and negotiation. Policy protect module protects privacy policy which decides the safe query sequence of attribute, and attribute protect module and negotiation modules have the same function to those of SAML server part.

3 Summary

This paper gives the cloud service security solution, and makes a research on cloud service access control model based UCON and negotiation. The next work that we will do is to realize the cloud service security prototype system.

References

1. Foster, I., Zhao, Y.: Cloud Computing and Grid Computing 360-Degree Compared. In: Grid Computing Environments Workshop (2008)
2. ning, G., jiamao, L., xiaolu, C.: Theory and Practice R & D of Web Services, January 2006, p. 10. Machinery Industry Press (2006)
3. Thomas, R.K., Sandhu, R.S.: Task-based Authorization Controls(TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management. In: Proceedings of the IFIP WG11.3 Workshop on Database Security, Lake Tahoe, California, August 11-13 (1997)
4. Yuan, E., Tong, J.: Attribute Based Access Control (ABAC) for Web Services. In: Proceedings of the IEEE Conference on Web Services (ICWS 2005). Orlando Florid (2005)
5. Sandhu, R., Park, J.: Usage Control: A Vision for Next Generation Access Control. In: Gorodetsky, V., Popyack, L.J., Skormin, V.A. (eds.) MMM-ACNS 2003. LNCS, vol. 2776, pp. 17–31. Springer, Heidelberg (2003)
6. OASIS Standard. eXtensible Access Control Markup Language(XACML) Version 2.0[OL], `http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf,2005-02`
7. Yu, T., Winslett, M., Seamons, K.E.: Interoperable Strategies in Automated Trust Negotiation. In: 8th ACM Conference on Computer and Communications Security (2001)