THE PRIVACY-AWARE ACCESS CONTROL SYSTEM USING ATTRIBUTE-AND ROLE-BASED ACCESS CONTROL IN PRIVATE CLOUD

Ei Ei Mon, Thinn Thu Naing

University of Computer Studies, Yangon, Myanmar
eemucsy@gmail.com, ucsy21@most.gov.mm

Abstract

Cloud is a relatively new concept and so it is unsurprising that the information assurance, data protection, network security and privacy concerns have yet to be fully addressed. The cloud allows users to avoid upfront hardware and software investments, gain flexibility, collaborate with others, and take advantage of the sophisticated services. However, security is a huge issue for cloud users especially access control, user profile management and accessing services offered by the private cloud environment. A privacy enhancement system on Academic-based private cloud system using Eucalyptus open source cloud infrastructure has been proposed in this paper. This system provides the cloud users to improve the privacy and security of the private personal data. Two approaches (Role-based Access Control and Attribute-based Access Control model) are combined as a new approach (ARBAC). This means that they are applied to improve the privacy which supports both mandatory and discretionary access control needs on the target private cloud system.

Keywords: Private cloud, Privacy, Eucalyptus, Role-based access control, Attribute-based access control

1 Introduction

Cloud computing has brought up major advancements to the IT industry. Today, clients are capable of running their software applications in remote computing clouds where data storage and processing resources could be acquired and released, almost, instantaneously. The virtualization layer on top of the commodity hardware in computing clouds is the driving force that allows cloud providers to "elastically" and promptly respond to client resource demands and requirements [8].

In spite of all the advantages delivered by cloud computing, the security and privacy concerns are significant challenges from the storage and processing of sensitive data on remote servers that can even not be managed by the cloud users themselves.

The rest of this paper is organized as follows: Section 2 describes the related work. Section 3 mentions Privacy-aware access control system. Section 4 describes technique preliminaries. In Section 5, the proposed system is described. Finally Section 6 concludes the paper.

2 Related work

Researches on data privacy in cloud computing are still in its early stages. Good reports are presented in [5] , discuss the risks imposed by the adoption of cloud computing on data privacy and legal compliance, and A. [1] which emphasizes on the need to develop a sound digital identity infrastructure to support tackling privacy and security concerns in computing clouds. and [7] and [6] present a comprehensive set of guidelines on designing privacy-aware cloud services. [7] summarizes the privacy patterns in 6 recommended practices: "minimizing customer personal information sent to and stored in the computing cloud; protecting sensitive customer information in the cloud; Maximizing user control; Allowing user choice; Specifying and limiting the purpose of data usage; providing the customer with privacy feedback". [3] proposed attribute based access control model with its authorization architecture and policy formulation to impose attribute conditions for authorizing a user.

3 Privacy-Aware access control system

Privacy in cloud computing is the ability of a user or a business to control what information they reveal about themselves over the cloud, and the ability to control who can access that information. Cloud Service Providers (SPs) can store information at multiple locations or outsource it, then it is very difficult to determine, how secure it is and who has access to it [5]. The privacy policy rules on personal identifiable information (PII) can be defined to restrict access of applications to

978-1-61284-159-5/11/$26.00 ©2011IEEE

collected data and considered by the following requirements: such as operations, purposes, data users, user access roles, privacy policies, conditions and data.

3.1 Definitions and model assumption

In this section, the following definitions and their responsibilities will be defined:

Data Owners

The cloud users can create their own VM services, and application services and data services. All of those services are stored into the private data region on the cloud storage according to their permissions in the organization.

Data Users

The cloud users can access some pre-defined services, and data which are created by other Data Owners according to their appropriate permission in the cloud system.

Cloud Service Providers

The cloud administrators can operate the cloud servers and components of the cloud system and the cloud services according to the predefined rules to the cloud users.

Privacy Manager

It performs as a filter to the confidentiality of users' sensitive information from the other unauthorized users according to the predefined privacy policies and the user levels and data security levels.

Attribute and Role Based Access Control Model (ARBAC)

This system applies an attribute and role based access control model (ARBAC) for cloud services. In ARBAC model, Service providers publish well-defined access control requirements in policy statements. Before invoking services, requestors must provide their attribute information and all parameters of method it will access to service providers. When service providers receive requests, they retrieve the attribute information from requests, and determine whether to permit or to deny these requests according to their access control policies.

3.2 Scenarios of the system

This paper mentions some scenarios defined to provide the privacy policies for the system.

Scenario-1: User Provisioning

- A new user decides to self register via a user interface;
- The self-registration process requires the user to provide data, including personal data. In this step the user can also specify their privacy preferences;
- The self-registration module triggers the provisioning of the user (creation of user accounts, setting of access control rights and storage of personal information) to the various involved the system;
- During the user provisioning process, privacy policies are generated from user's privacy preferences and user's personal data.

Scenario-2: Authentication and Authorization of users

Initial user account creation involves two step operations:

1) Any user with access to Cloud Controller user interface can fill a form to request an account.
2) When a request is received, it is up to the administrator to grant access to the user according to its own policy.

Scenario-3: Proper Data Acquisition

If the cloud users (The Researchers or Faculties) want to upload the own data (created VM instances or Developed Services) into the cloud, the privacy manager defines data collection policy. The information is collected by authorized appointed user only and the own data must be adequate, relevant and not excessive as well as the purpose must be mentioned.

Scenario-4: Privacy-aware Management of Personal Data

The system needs to control access personal identifiable information (PII) and each PII has an access control list. Groups and roles may be used instead of individual names. Personal and confidential data can be stored in a variety of data repositories, log files, audit systems, etc. Privacy manager specifically defines and pushes privacy policies to the privacy-aware system.

Scenario-5: Notification about the purpose of usage

The system needs to know for which purpose the user access to PII control privacy. In particular, the data users must receive special notification if any person whom it is proposed to add to their access control list already has access to personal identifiable information on a large number of people.

Scenario-6: Permissible Data Processing

The data processing should be granted by the data or resource owner on his personal identifiable information. The data owner may open the PII with herself and the data user has been referred, the data user and referring data owner on the access control list.

Scenario-7: Permissible Data Transfer

The data owner may be responsible to transfer her PII to her friends or members. The data owner may grant which user for which data.

Scenario-8: Permissible Data Deletion

No-one shall have the ability to delete PII information until the appropriate time period has expired.

Scenario-9: Privacy-aware Relationships

This scenario is considered by the following facts: If Faculty X trusts Faculty Y and Faculty Y trusts Student Z that does not mean Faculty X trusts Student Z. Faculty X needs to trust that Faculty Y will not pass on any information about Faculty X to Student Z. If X breaks his trust relation with Faculty Y then Faculty X would like to forget all the information Faculty Y had about Faculty X.

4 Technique preliminaries

4.1 Role Based Access Control (RBAC)

Access control is a core requirement for any information system. Some typical access control models for services have been presented, such as Attributed-based Access Control (ABAC) Model for services [2], Role-based Access Control (RBAC) Model for services and so on. This system assumes that there is a set of roles that are authorized to perform certain actions and that users are authorized to play certain roles. More formally, this system assumes the existence of set of users U in which the other sub-set user groups are included such as a set of roles R and a set of permissions P (where permission is an object-action pair).

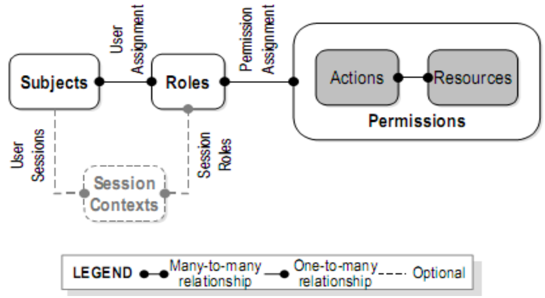

Figure 1 The Core RBAC model

4.2 Attribute Based Access Control (ABAC)

The Attribute Based Access Control (ABAC) model consists of two aspects: the policy model which defines the ABAC policies and the architecture model which applies the policies to data access control [3].

4.2.1 Attributes defined

Unlike RBAC, the ABAC model can define permissions based on just about any security-relevant characteristics, known as attributes. For access control purposes, this paper is concerned with three types of attributes:

Subject Attributes. A subject is an entity (a user) that takes action on a resource. Each subject has associated attributes which define the identity and characteristics of the subject. Such attributes may include the subject's identifier, name, organization, job title, and so on.
Resource Attributes. A resource is an entity that is acted upon by a subject. As with subjects, resources have attributes that can be leveraged to make access control decisions.
Environment Attributes. These attributes describe the operational, technical, and even situational environment or context in which the information access occurs. For example, attributes such as current date and time, the current services, and the data's security level, are not associated with a Particular subject or a resource. Policy representation can be more fine-grained within ABAC because it can be based on any combination of subject, resource, and environment attributes.

4.2.2 ABAC Policy Formulation

Here this paper formally defines the (basic) ABAC policy model: U, R, and E are the set of users, resources, and environments are as follows:

U	A set of users U employed in the cloud. UG - General Cloud Users US - Special Cloud Users UG= {Students, Staffs, Faculty, Teachers, Others} US= {Cloud Providers, Researchers, Research Students} U={{UG_1,UG_2,…UG_k},{US_1,US_2,…US_k}}, k is total users defined in the cloud.
R	A set of resources R allowed to access in the cloud R={(R_{Iaas1}, R_{SaaS1}, R_{DaaS1}), (R_{Iaas2}, R_{SaaS2}, R_{DaaS2}), ….(R_{IaasM}, R_{SaaSM}, R_{DaaSM})} R_{IaaS}={cpu $type_i$, $memory_i$, disk space $type_i$) R_{SaaS}={$service_1$, $service_2$, ….$service_n$) R_{DaaS}={($data_1$, $storge_1$), ($data_2$, $storge_2$)….) , m is total vector sets of resources defined in the cloud.
E	A set of environmental region E in the cloud E={(e_{time1},$e_{location1}$), (e_{time2},$e_{location2}$),…., (e_{timeN},$e_{locationN}$), n is total environmental regions defined in the cloud.

ATTR(u), ATTR(r), and ATTR(e) are attribute assignment relations for user u, resource r, and environmental regions e, respectively:

$ATTR(u) \subseteq UG_1 \times US_1 \times \ldots UG_K \times US_K$

$ATTR(r) \subseteq R_{IaaS1} \times R_{SaaS1} \times R_{DaaS1} \ldots \times R_{IaaSM} \times R_{SaaSM} \times R_{DaaSM}$

$ATTR(e) \subseteq e_{time1} \times e_{location1} \times \ldots \times e_{timeN} \times e_{locationN}$

This paper also uses the function notation for the value assignment of individual attributes. For example:
Role(u) = "Student"
ServiceOwner(r) = "UCSY"
CurrentDate(e) = "01-23-2011"
In the most general form, a Policy Rule that decides on whether a user UG_1 can access a resource R_{IaaS1} , R_{SaaS1} and R_{DaaS1} in a particular environment e_{time1},$e_{location1}$, is a Boolean function of s, r, and e's attributes:

Rule: can_access (u, r, e) ←f (ATTR(u), ATTR(r), ATTR(e))

Given all the attribute assignments of u, r, and e, if the function’s evaluation is true, then the access to the resource is granted; otherwise the access is denied. A Policy rule base may consist of a number of policy rules, covering many subjects and resources within a security domain. The access control decision process in essence amounts to the evaluation of applicable policy rules in the policy store. For example, a rule that dictates “Users with role ‘Researcher’ may access the ‘Research’ special cloud service” can be written as:

R1:can_access (US_1, R_{IaaS1}, e_{time1} ,$e_{location1}$) ←(Role(US) = ‘Researcher’) ∧(Name(r) = ‘Server1’) ∧ (Time(e) = ’24 hours’)

This example also shows that conventional RBAC rules can be accommodated by the ABAC model just as easily. For example, to enforce that a resource may only be accessed by its owners, this paper can have a rule as follows:

R2: can_access (u, r, e) ← (UserID(u) = ResourceOwner(r))

5 System architecture

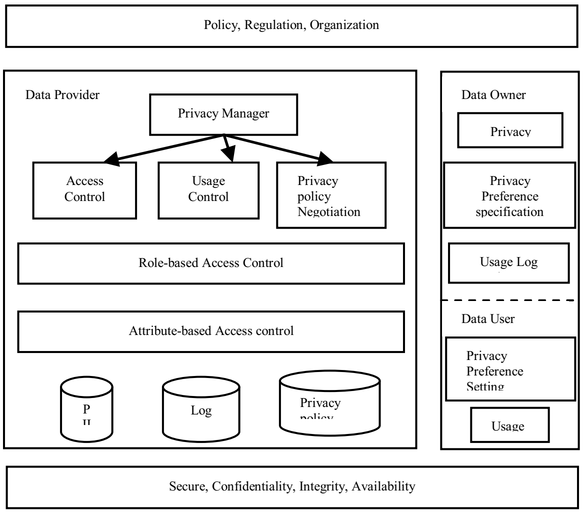
Policy, Regulation, Organization
Data Provider
Privacy Manager
Access Control
Usage Control
Privacy policy Negotiation
Role-based Access Control
Attribute-based Access control
P
Log
Privacy
Data Owner
Privacy
Privacy Preference specification
Usage Log
Data User
Privacy Preference Setting
Usage
Secure, Confidentiality, Integrity, Availability

Figure 2 The proposed system framework

In this system, the cloud client is allowed to store their data in the cloud according to the privacy standards or laws before upload data and to access the data in the cloud according to their user levels. The Privacy Manager is responsible to define the privacy policies, handle the privacy laws, to classify user levels, classify the data security levels, control data access in the private cloud to enhance the security of the cloud. This system uses an Attribute Based Access Control (ABAC) model with Role Based Access Control (RBAC) as a new approach (ARBAC), which is based on subject, object, and environment attributes and supports both mandatory and discretionary access control needs. In addition, it is assumed that the data owner can not only store data files but also run his own programs on Cloud Servers to manage his data files.

5.1 Access control list

To determine the read, write, and execute access, the access check is performed on the ACL entries in the following algorithm:

1) If the user requesting access is the object owner, and the requested permission is granted by the ACL entry, then access is granted.

2) If the user requesting access is a named user in the ACL, and the requested permission is granted by the ACL entry, then access is granted.

3) If the user requesting access is in the owning group of the file, or is a member of any named groups, and the requested access permission is granted by the ACL entry of the owning group or the ACL entry of any of these named groups, then access is granted.

4) If the user requesting access is a member of any of the named groups, and the requested access permission is granted by the ACL entry of any of these named groups, then access is granted.

5) If the requested access permission is granted by the “other” entry, then access is granted, otherwise access is denied.

5.2 Classification of data security levels

The data security level is classified (described in Table 1) based on significance and sensitivity

Table 1 Classification of data security levels

Data Security Level	**Type of Privacy**	**Properties**
Full trust(LL)	No Privacy (NP)	This data is not sensitive and can be disclosed in public.
Compliance-based trust (AL)	Privacy with trusted provider (PTP)	This level of data is sensitive. They should not be disclosed because users can access according to their roles with RBAC.
No trust (HL)	Privacy with non-trusted provider (NPTP)	This level of data is very sensitive and can be accessed only by privileged users.

5.3 Definition and Notation

U	set of users
P	set of permission the user wants to acquire
SL	security level
UL	user level
AP	authorization policy
PS	set of policies
DA	data access
C	set of constraint
S	subject in policy
O	data object or data type
R	set of roles of user

5.4 Authorization Policy

The system defines an authorization policy as a triple, AP = (S, P, C). S: could be a user or a role. P: is defined as a pair <M,O>, where M is an operation mode defined in {READ, APPEND, DELETE, UPDATE} and O is a data object or data type. If C is empty then this policy reverts to simple RBAC that is described the following:

Privileges:
roles $\subseteq$ user × role
subroles $\subseteq$ role × role
privs $\subseteq$ role × privilege

Permissions:
groups $\subseteq$ user × group
subgroups $\subseteq$ group × group
gperms $\subseteq$ group × permission
uperms $\subseteq$ user × permission

Data Access:
DA= (U,P,R)
C= $\{c_1,c_2,\ldots\ldots,c_n\}$

A data access DA (U,P,R) is granted only if there exists an authorization policy AP(S,P',C) such that U ∈ S, P =P′ and C maps to true under PS.

```
Algorithm1: RequestPermission (DataAccess da,U)
  initialize candidate policy set PS = {}
  for every AP in policy set of the application or service
       if (U in da ∈ S in AP) and (P in da = P in AP)
           put AP into PS
       end if
  end for
  result = "Reject"
  for every AP in PS
        if (Check CS in PS) and (Check UL and SL)
            result = "Accept"
break
        else
            result = "Reject"
        end if
  end for
 return result
```

This paper's central design goal is to control access the various PII related to the privacy of sensitive data. This is achieved by placing user access levels, data security levels and data privacy mechanisms. Moreover, this system provides a privacy manager which allows users the different privacy operations applied on their data according to their user group or access levels and data security levels. It also performs as a filter to the confidentiality of their sensitive information from the other unauthorized users using the above Algorithm1.

6 Conclusions and future work

The aims of the proposed system are to protect personal information in the cloud; to specify privacy policies for the private cloud; to reduce the risk such as stealing and misuse of the private personal data; to enforce user's security policy to decide only which attributes should be disclosed so that users can reveal their attributes to service providers according to their need. This system uses role-based access control model and attributed-based access control to limit access. The users of the private cloud system can access their resources against interference. Therefore, this system can enhance the security of the cloud and protect access from the unauthorized users, provide confidentiality, integrity and availability. Future work includes two main research directions, namely, the support for topical trust and the usage of access rules also for certificate protection.

References

[1] A. Cavoukian, "Privacy in the clouds", in Springer Identity in the Information Society, Published online: 18 December 2008.

[2] A. Syalim, "Controlling Access to Encrypted Databases Using Multipolicy Access Control System", February 2006

[3] E. Yuan and J. Tong, "Attributed Based Access Control (ABAC) for Web Services," Proc. IEEE International Conference on Web Services, IEEE Computer Society, Jul. 2005, pp.561-569, doi: 10.1109/ICWS.2005.25.

[4] J. Park, R. S. Sandhu and G. Ahn, "Role-Based Access Control on the Web," ACM Transactions on Information and Systems Security, Vol. 4, pp.37-71, Feb. 2001.

[5] R.Gellman, "WPF REPORT: Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing", February 23, 2009.

[6] S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud", HP Labs Technical Report,HPL2009178,http://www.hpl.hp.com/techreports/2009/HPL-2009-178.pdf , 2009.

[7] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services", in Proceedings of ICSE-Cloud'09, Vancouver, 2009.

[8] W. Itani, A. Kayssi and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures, Department of Electrical and Computer Engineering, in Eighth IEEE International conference on Dependable, Autonomic and Secure Computing, 2009.