The Security Enhancement for Privacy-Aware Access Control System on Private Cloud (PAAC)

Ei Ei Mon, Thinn Thu Naing
University of Computer Studies, Yangon
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. Companies such as RedHat, Microsoft, Amazon, Google, and IBM are increasingly funding cloud computing infrastructure and research, making it important for students to gain the necessary skills to work with cloud-based resources. This paper presents a free, educational private cloud using an existing infrastructure. However, security is a huge issue for cloud users especially access control, user profile management and accessing services offered by the private cloud environment. Therefore, this paper proposes a private cloud control, privacy and access for the cloud user who are involved in the academic institution private cloud system. This system intends to reduce the risk such as stealing and misuse of the private personal data. This system uses Eucalyptus Cloud Infrastructure as a testbed. The main ideas of this system (in term of security and privacy) are to minimize the confidential information of cloud users, to maximize the access control and to specify the data usage.

Keywords: private cloud, privacy, eucalyptus, role-based access control, rule-based access control

1. Introduction

Cloud computing has brought up major advancements to the IT industry. Building on its predecessors, namely, grid and utility computing, this new evolutionary model is witnessing a rapid expansion and proliferation. 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 [6]. This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**.

In spite of all the advantages delivered by cloud computing, several challenges are hindering the migration of customer software and data into the cloud. On top of the list is the security and privacy concerns arising from the storage and processing of sensitive data on remote machines that are not owned, or even managed by the customers themselves. With cloud computing, all the customer can see is a virtual infrastructure built on top of possibly non-trusted physical hardware or operating environments.

As promising as it is, cloud computing is also facing many challenges that, if not well resolved, may impede its fast growth. Data security, as it exists in many other applications, is among these challenges that would raise great concerns from users when they store sensitive information on cloud servers. These concerns originate from the fact that cloud servers are usually operated by commercial providers which are very likely to be outside of the trusted domain of the users. Data confidential against cloud servers is hence

frequently desired when users outsource data for storage in the cloud. In some practical application systems, data confidentiality is not only a security issue, but also of privacy concerns. In a typical university scenario, PC labs and servers are under-utilized during the night and semester breaks. In addition, these resources are on high demands mainly towards the end of the semester. The target users of this system are academic students, research students, researchers, staffs, running the applications and services.

The rest of this paper is organized as follows. Section 2 describes the related work. Section 3 mentions privacy of cloud computing. Section 4 discusses models and assumption of the proposed system. Section 5 describes technique preliminaries. In section 6, the proposed system is described. Finally section 7 concludes the paper.

2. Related Work

Research on data privacy in cloud computing is still in its early stages. Good reports on the topic are presented in "WPF REPORT: Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing" [1] which discusses the risks imposed by the adoption of cloud computing on data privacy and legal compliance, and "Privacy in the clouds" [2] which emphasizes on the need to develop a sound digital identity infrastructure to support tackling privacy and security concerns in computing clouds. "Taking Account of Privacy when Designing Cloud Computing Services" [3] and "Accountability as a Way Forward for Privacy Protection in the Cloud" [4] present a comprehensive set of guidelines on designing privacy-aware cloud services. [3] summarizes the privacy patterns in 6 recommended practices: "(1) minimizing customer personal information sent to and stored in the computing cloud; (2) protecting sensitive customer information in the cloud; (3) Maximizing user control; (4) Allowing user choice; (5) Specifying and limiting the purpose of data usage; (6) providing the customer with privacy feedback". Note that tips 2 to 6 are addressed in this paper.

3. Privacy of Cloud computing

Privacy in cloud computing is the ability of a user or a business to control what information they reveal about them-selves over the cloud or to a cloud service provider, and the ability to control who can access that information. Numerous existing privacy laws impose the standards for the collection, maintenance, use, and disclosure of personal information that must be satisfied by cloud providers. The nature of cloud computing has significant implications for the privacy of personal, business and governmental information. Cloud 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 [1]. A cloud SP is a third party that maintains information about, or on behalf of, another entity. Whenever an individual, a business, a government agency, or other entity shares information in the cloud, privacy or confidentiality questions may arise [1]. Trusting a third party requires taking the risk of assuming that the trusted third party will act as it is expected. The main problems associated with such a model are:

- Loss of control: Data, applications, and resources are located with SP. The cloud handles IDM as well as user access control rules, security policies and enforcement. The user has to rely on the provider to ensure data security and privacy, resource availability, monitoring of services and resources.
- Lack of trust: Trusting a third party requires taking risks. Basically trust and risk are opposite sides of the same coin. Some monitoring or auditing capabilities would be required to increase the level of trust.
- Multi-tenancy: Tenants share resources and may have opposing goals which could be conflicting. There is a need to provide a degree of separation between tenants.

4. Models and Assumption

Assume that the system is composed of the following parties:

- the Data Owner,
- the Data Users,
- the Data Provider,
- a Privacy Manager.

To access data files shared by the data owner, Data users for brevity, download data files of their interest from Cloud Servers. For simplicity, assume that the only access privilege for users is data file reading. Cloud Servers are always operated by the Cloud Service Provider (CSP). They are assumed to have abundant storage capacity and computation power. The Privacy Manager is also a party which is used for auditing every file access event. In addition, assume that the data owner can not only store data files but also run his own programs on Cloud Servers to manage his data files.

In the proposed system, the system uses role-based access control model and rule-based access control model in order to enhance the security of the private cloud.

5. Technique preliminaries

5.1. Role Based Access Control (RBAC)

Access control model is a framework that dictates access control using various access control technologies. RBAC is a widely used - and dominant - access control model, and most access control security products available in the market today are based on this model because its objectives are architectural. The model allows access to a resource, based on the role the user holds in the organization [8]. The basic principles of role-based access control (RBAC) are very simple. The proposed 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. The indirection between users and authorized actions provided by the set of roles means that the management of access control policies is greatly simplified. More formally, this system assumes the existence of set of users U in which the other sub-set user groups are included such as (for example, in the academic private cloud system) U= {Faculty, Staff, Teacher, Students, Researchers, Research Students}, a set of roles R and a set of permissions P (where permission is an object-action pair). According to each user sub-sets, it needs to define the corresponding access role set R and a set of permission P (where permission is an object-action pair) [10].Then in core RBAC an access control policy is specified by a user-role assignment relation $UA \subseteq U \times R$ and a permission-role assignment relation $PA \subseteq P \times R$. A user u is authorized for permission p if there exists a role $r \in R$ such that $(u, r) \in UA$ and $(p, r) \in PA$. In this case, a user u is authorized for permission p if there exist roles r and r′ such that $(u, r) \in UA$, $r > r'$ and $(p, r') \in PA$.

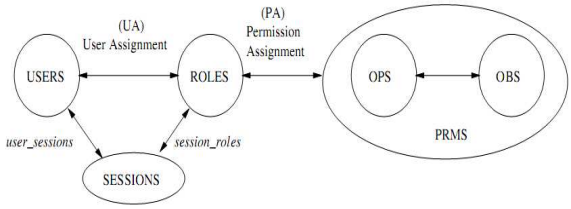

Figure 1. Core RBAC Model

5.2. Access Control Lists (ACLs)

Each object may be associated with an access control list (ACL), which corresponds to one column of the access matrix, and is represented as a list of subject-rights pairs. When a subject tries to access an object, the set of rights associated with that subject is used to determine whether access should be granted. This comparison of the accessing subject's identity with the subjects mentioned in the ACL requires prior authentication of the subject. ACL-based systems usually support a concept of group rights. When a large number of objects provide the same rights to a set of subjects, these subjects may be combined into a group, thus reducing the size of the ACL.

5.3. Authentication and Authorization of the testbed cloud infrastructure (Eucalyptus)

Two types of "actors" need to be authenticated and authorized on UEC (Ubuntu Enterprise Cloud).

- The users or administrators of the system which have specific rights to modify the system and start and stop instances;
- The components of the system (node controller NC, cloud controller CLC, cluster controller CC) which need to trust each other when transmitting requests.

On a general level, the authentication is performed using locally generated X509 certificates, as cryptographic keys to authenticate and secure communications between all actors with communication based on the WS-Security policy framework. This is true for all internal communication within the cloud. Users authenticate either with an X509 certificate or a Query type key. The initial user account authentication process is shown in Figure 2.

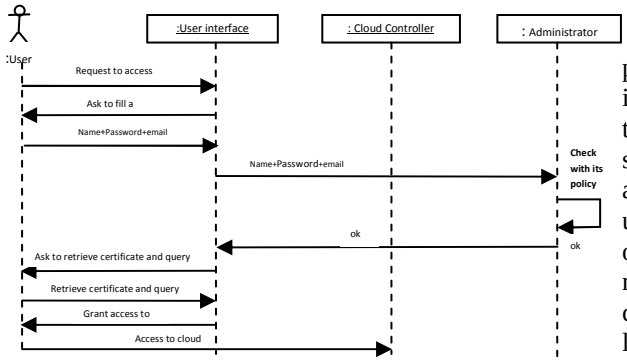

Figure 2. Sequence diagram of initial user account on UEC

6. Proposed System

6.1 System Architecture

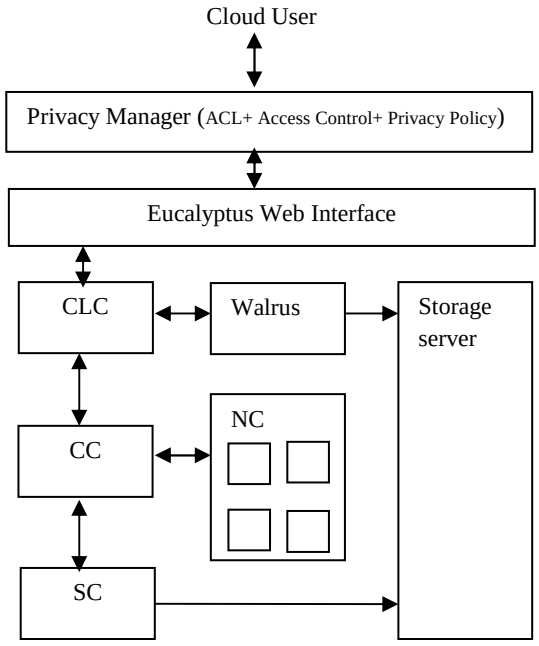

Figure 3. The proposed system architecture with privacy manager

In PAAC system, Cloud User can access the private cloud via the privacy manager described in Figure 3. 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 classifies data on degree of sensitivity. The Privacy Manager is responsible to handle the privacy laws, to classify user levels, classify the data security levels, control single sign-on and control data access in the private cloud to enhance the security of the cloud. The privacy manager defines access control list (ACL), access control policies and privacy policies as shown in figure 3.

6.2 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
CS	set of conditions
C	constraint
S	subject in policy
O	data object or data type
R	set of roles of user

6.3. Authorization Policy

The system defines an authorization policy as a triple, AP = (S, P, C) where:
S: is the subject in this policy, which could be a user or a role.
P: is the target permission in this policy, which 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.
C: is a constraint in this policy. If C is empty then this policy reverts to simple RBAC that is described the following:

Privileges:
roles ⊆ user × role
subroles ⊆ role × role
privs ⊆ role × privilege
Permissions:
groups ⊆ user × group
subgroups ⊆ group × group
gperms ⊆ group × permission
uperms ⊆ user × permission

6.4. 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.

Using ACL makes the system enhance the confidentiality due to the limited access of the ACL.

Data Access:
DA= (U,P,R)
CS= $\{c_1,c_2,\ldots\ldots,c_n\}$
A data access DA (U,P,R) is granted only if there exists an authorization policy AP(S,P',CS) such that U ∈ S, P =P′ and CS maps to true under PS.

```
Algorithm: 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
```

PAAC's central design goal is to maximize users' control in managing the various aspects related to the privacy of sensitive data. This is achieved by placing user access levels, data

security levels and data privacy mechanisms. Moreover, PAAC 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 and performs as a filter to the confidentiality of their sensitive information from the other unauthorized users using the above DataAccess algorithm.

The data security level is classified as Full trust, Compliance-based trust and No trust. Before uploading the data to be stored and processed in the private cloud, the cloud client classifies this data, based on significance and sensitivity, into three privacy categories: No Privacy (NP), Privacy with Trusted Provider (PTP) and Privacy with Non-Trusted Provider (PTNP).The main processes of privacy manager are as follows:

- To handles the data privacy standards/laws
- To allow access the data in private cloud according to the user's level or role
- To allow the users to control their data directly control as privacy settings (On-demand security control)
- To protect personal information in private cloud with access control lists(ACL) and role-based access model
- To specify and limit purpose of data usage with the access control policy or privacy policy using the rule-based access control mechanism

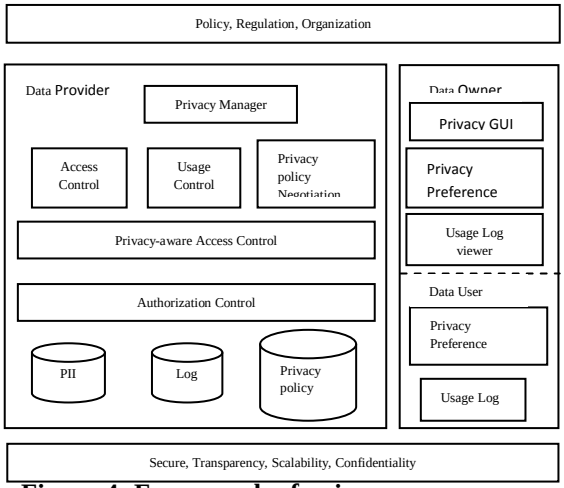

Figure 4. Framework of privacy-aware access control

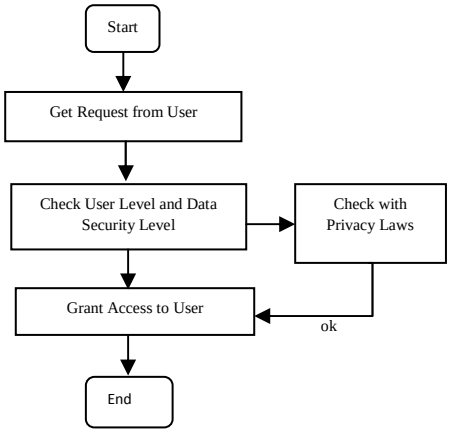

Figure 5. Flow chart of Access Control Model within Privacy Manager on Private Cloud

In PAAC system, to perform the main processes of access control model the system uses the processes of the flowchart of Access Control Model within Privacy Manager on Private Cloud (figure 5). In this figure, when the cloud user request the resources in the private cloud system, the privacy manager checks this user level and data security level according to the role-based access control model. Then, the privacy manager also checks with the privacy policies defined by the cloud providers. If the privacy manager grants access to this user, the user can access the corresponding requested resources or services in the private cloud system.

6.5. Minimize confidential information sent to and stored in the cloud

If the cloud user wants to upload the personal data into the cloud, the privacy manager uses the following procedure:

- Analyze the minimal amount of information from user
- Decide to store only data in which cloud applications need to used immediately
- Allow control to users about their information generates trust
- Store data by data storing mechanisms with the privacy standards/ laws

6.6. The Proposed Access Control Model (Rule-based Access Control Model) to control access PII

In order to enforce access control in private cloud, this paper proposes a rule-based access control model where policies are specified by resource owners, and they denote implicitly the 'profile' of authorized users by means of one or more access conditions, i.e. constraints on the user level, and data security level of the relationships they have with other users in the cloud. In what follows, the system denotes by V_{PC}, E_{PC}, UL_{PC}, SL_{PC} the sets of nodes, edges, user levels, and data security levels, respectively, of a private cloud PC. The notion of access condition is formally defined as follows:

Definition 1 (Access Condition)

Given a private cloud, an access condition cond against PC is a tuple (v, ul, sl), where $v \in V_{PC} \cup \{*\}$ is the node with which the requestor must have a user level, $ul \in UL_{PC} \cup \{*\}$ is a user level, $sl \in SL_{PC} \cup \{*\}$ is a data security level that the user level must have. If $v = *$ and/or $ul = *$, v corresponds to any user in V_{PC} and/or ul corresponds to any user level in UL_{PC}, whereas if $sl = *$, there is no constraint concerning the data security or trust level. Access control requirements of a given object can then be expressed by a set of conditions. More precisely, given an object obj owned by v_0, the set of access conditions applying to obj are expressed by an access rule specified by v_0. Such notion is formally defined as follows.

Definition 2 (Access Rule)

An access rule rul is a tuple (oid,cset), where oid is the identifier of object obj, whereas cset is a set of conditions $\{cond1,...,cond_n\}$, expressing the requirements a node must satisfy in order to be allowed to access object obj. It is important to note that the conditions in cset do not denote a set of alternative requirements, but all the requirements to be satisfied. In other words, the semantics of a set of conditions $\{cond1,...,cond_n\}$ can be expressed as $cond1 \wedge \cdots \wedge cond_n$. It may be also the cases that more than one rule are specified for a given object. For instance, let us suppose that object obj is associated with two rules rul, rul1. In such a case, we consider the corresponding two sets of conditions $\{cond_1,...,cond_n\}$ and $\{cond1_1,..., cond1_m\}$ assets of alternative access control requirements—i.e., $(cond_1 \wedge \cdots \wedge cond_n) \vee (cond1_1 \wedge \cdots \wedge cond1_m)$.

6.7. Specify and limit the purpose of data usage

When the information is loaded into the cloud, it must be limited to the preferences and conditions set by a user or organization. The privacy manager specifies the data usage according to the following steps:

- Limit data usage by user level and data security level
- Allow to use data only to the user's specified purpose
- Validate the cloud application designs against the allowed usage intentions
-

7. Conclusion and Future Work

The proposed system is intended to minimize personal information in the cloud, to protect personal information in the cloud, to maximize user control, to allow user choice, to specify and limit purpose of data usage. As this system uses role-based access control model and rule-based access control to limit access, this system provides confidentiality and integrity of the private cloud system. 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] R.Gellman, “WPF REPORT: Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing”, February 23, 2009.

[2] A. Cavoukian, “Privacy in the clouds”, *in Springer* Identity in the Information Society, Published online: 18 December 2008.

[3] S. Pearson, “Taking Account of Privacy when Designing Cloud Computing Services”, *in Proceedings of ICSE-Cloud’09*, Vancouver, 2009.

[4] 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)

[5] S. Pearson, y. Shen and M. Mowbray, “A Privacy Manager for Cloud Computing”, HP Labs, Long Down Avenue, Stoke Fifford, Bristol B34 8QZ, UK

[6] 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 2009 Eighth IEEE International conference on Dependable, Autonomic and Secure Computing

[7] B. Carminati, E. Ferrari, and A. Perego, “Rule-Based Access Control for Social Networks “, DICOM, Universit` a degli Studi dell’Insubria, Varese, Italy

[8] V. Purohit, “Authentication and Access Control”, the Cornerstone of Information Security, September 2007

[9] National Telecommunications Administration, “Cloud Privacy: Normative Standards Needed to Foster Innovation”, U.S. Department of Commerce, Washington, DC 20230, June 1, 2010

[10] A. Syalim, “Controlling Access to Encrypted Databases Using Multipolicy Access Control System”, February 2006