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. 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. Therefore, this paper proposes a cloud control, privacy and access for the cloud user who are involved in the academic institution cloud system. This system intends to reduce the risk such as stealing and misuse of the private personal data. 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 and optimize the data usage.

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.

In this paper, the PAAC system is proposed to control privacy and access a private cloud which reduces the risk such as stealing and misuse of the private personal data, and also assists the cloud computing provider to conform to privacy law.

The rest of this paper is organized as follows. Section 2 describes the related work. Section 3 mentions issues of cloud computing. Section 4 discusses privacy of cloud computing. Section 5 describes benefits of private cloud. In section 6, the background theory is described. Section 7 discusses the analysing cloud privacy in Google and Facebook. Section 8 describes the proposed system. Finally section 9 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" which discusses the risks imposed by the adoption of cloud computing on data privacy and legal compliance, and "Privacy in the clouds" 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" and "Accountability as a Way Forward for Privacy Protection in the Cloud" 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. Issues of Cloud Computing

Here is a rundown on most of the current issues concerning cloud computing:

Security – While a leading edge cloud services provider will employ data storage and transmission encryption, user authentication, and authorization (data access) practices, many people worry about the vulnerability of remote data to such criminals as hackers, thieves, and disgruntled employees.

Reliability – Some people worry also about whether a cloud service provider is financially stable and whether their data storage system is trustworthy.

Ownership or Privacy– Once data has been relegated to the cloud; some people worry that they could lose some or all of their rights or are unable to protect the rights of their customers. Many cloud providers are addressing this issue with well-crafted user-sided agreements.

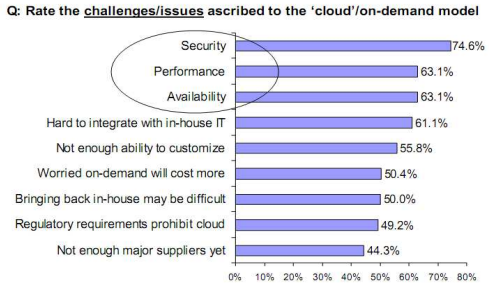
Data Backup – Cloud providers employ redundant servers and routine data backup processes, but some people worry about being able to control their own backups.

Data Portability and Conversion –As service competition grows and open standards become established, the data portability issue will ease, and conversion processes will become available supporting the more popular cloud providers. Worst case, a cloud subscriber will have to pay for some custom data conversion.

Multiplatform Support – More an issue for IT departments using managed services is how the cloud-based service integrates across different platforms and operating systems. Multiplatform support requirements will ease as more user interfaces become web-based.

Intellectual Property – A company invents something new and it uses cloud services as part of invention.

Customers Big Concerns About Cloud: Security, Performance, Availability



4. 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 (which may not be true all the time). The main problems associated with such a model are:

1) 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.

2) 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.

3) 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.

The properties of client-plus-cloud computing raise valid questions about security and privacy, such as:

- Are hosted data and applications within the cloud protected by suitably robust privacy policies?
- Are the cloud computing provider's technical infrastructure, applications, and processes secure?
- Are processes in place to support appropriate action in the event of an incident that affects privacy or security?

5. Benefits of Private Cloud

Private cloud (also called internal cloud or corporate cloud) is computing architecture that provides hosted services to a specific group of people behind a firewall. A private cloud has leverages in

terms of virtualization, automation, and distributed computing to provide on-demand computing capacity to internal users. The following list shows top ten benefits of using private cloud over public one.

- *Security Consideration:* If an organization has applications that require direct control and custody of data, private cloud is the better choice.
- *Resource Availability:* Private cloud can be considered for the applications that require certainly more than defined resources which cannot be guaranteed by shared resource environment.
- *Service Disruption:* When there is technology change, public cloud operator will pick time that is the most convenient and least costly to them. As a result of this, it can create serious problems if the upgrade goes badly or it is initiated during a time when you need to use their service heavily for the business demand.
- *Better Choice:* It is also the reduction of operational cost from a service-level agreement standpoint to those applications.
- *Virtualization:* A core private cloud service for SMBs is virtualization software for high availability and fast provisioning, easily upgradable components to handle scalability, and system monitoring and management. This solution could be deployed on-premise.
- *Resource Consumption:* As infrastructure clouds allow users to add and destroy resources as needed, companies are using private clouds to keep an account for resource consumption at a project or department level and use the resources back that are no longer in use.
- *Data Longevity:* As data ages within the public cloud, the cost continues to increase. Private clouds are licensed like enterprise. Longevity of data does not increase the cost of the solution.
- *Performance:* Public clouds are accessed over the Internet and it has the limitation of provider's bandwidth. Private clouds are deployed inside the firewall and accessed over the Ethernet LAN at wire speed. Adding nodes provides additional performance to the cloud.
- *Data Amount:* Private clouds can start in the few TB range and we can add more capacity by adding additional nodes or disks. Public clouds start even smaller. If you lease more capacity, cost scales linearly.
- *Confidentiality:* With private clouds we have better control and have knowledge of legal activities. When it comes time to destroy or delete the data, it is in our decision and can be confirmed by our own team.

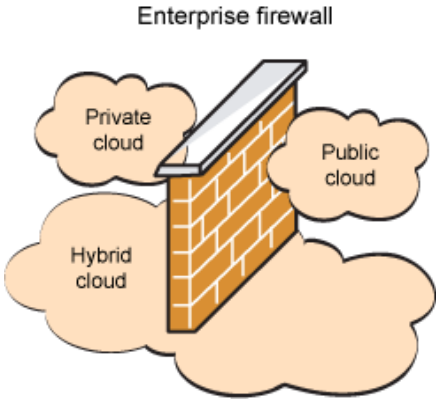


Figure 1. Public cloud, Hybrid cloud and Private cloud

6. Background

6.1. Access Control Models

Access control model is a framework that dictates access control using various access- control technologies. There are standard access control models which are highly domain and implementation independent. Each access control model has its own merits and demerits, and the specific business objectives they serve depend on the organization's need, culture, nature of business, etc. [8].

• Discretionary Access Control (DAC)
• Mandatory Access Control (MAC)
• Role Based Access Control (RBAC)

Discretionary Access Control (DAC)

Discretionary Access Control is based on ownership and delegation. In a DAC Model, access is governed by the access rights granted to the user or user groups. An organization/ administrator/ creator can identify a set of operations and assign them to an object and to a set of users (belonging to a user group). The DAC model is flexible but complex [8].

Mandatory Access Control (MAC)

In MAC, the data owner has limited freedom to decide on access control. Information is classified into different categories and each category is assigned a particular security level. This model is appropriate when securing confidentiality of data is critical [8].

Role Based Access Control (RBAC)

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].

7. Analyzing Cloud Privacy in Google and Facebook

Google and Facebook are good starting points for analyzing cloud privacy. In addition to search, Google offers, among a number of applications, e-mail, an application suite, a calendar, a blogging platform, website hosting services, and a web browser—all of which collect and/or store user-related data on Google's servers. Internet users in the United States spend an estimated 9% of their time online using some Google service. Google's industry dominance, coupled with its mission to organize the world's information and make it universally accessible and useful, raises significant privacy issues [9].

While Google has an overarching Privacy Policy, it also has privacy policies for more than forty specific applications and services. Google's Privacy Policy attempts to explain all of the ways in which users' personal identifying information may be collected, stored, used, and distributed to third parties. Google's Privacy Policy also allows it to share "aggregated, non-personal information" with advertisers, so long as the information does not individually identify users. However, it is possible to unveil the identity of a search engine user based on anonymized search results. More troubling, which exemplifies how many online privacy policies are implemented, Google reserves the right to change its privacy policies at anytime; and Google's terms of service state that use of a Google service constitutes an agreement to accept those terms, which include an agreement by users that Google can use their information according to its privacy policies. The result is that every time an individual uses a Google service, that person is accepting Google's Privacy Policy as it exists at that time [9].

Meanwhile, Facebook offers users substantial control over their privacy, with more than 100 settings. This array of privacy options is so confusing, many users typically choose poorly or not at all while, at the same time, Facebook is making publicly available more and more user information (Hoofnagle 2010). Even after changing privacy settings, certain information will still be shared across Facebook unless users take additional steps. For example, users must change certain "Account Settings" to prevent information from being shared with advertising networks and friends. The only way to prevent some personal data from being shared is to delete it. Facebook has recently been at the center of a privacy storm, with near-rebellions by users over Facebook's continually changing privacy policies, spurring even a call for a bill of privacy rights for social networks. Facebook's privacy policy has grown from just over 1,000 words in 2005 to nearly 6,000 words in 2010 [9]. Bowing to pressure from various constituencies, Facebook has recently attempted to simplify its privacy settings. And, as noted above, Google publishes over forty separate privacy policies. But recent court decisions have clearly signaled that privacy policies provide no real legal protection for users.

8. Proposed System

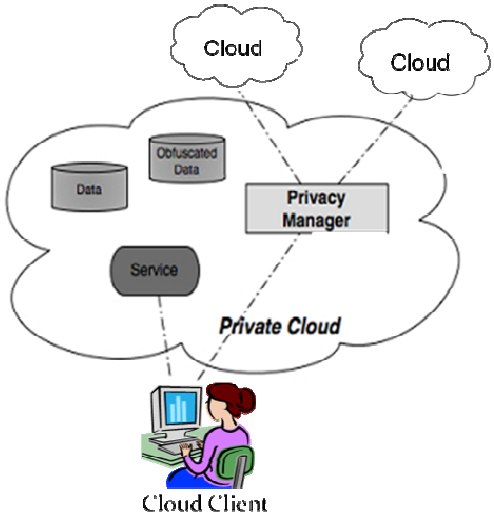


Figure 2. The proposed system architecture

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 access levels and data security levels and performs as a filter to the confidentiality of their sensitive information from the other unauthorized users.

In PAAC system, Client can access the private cloud via the privacy manager. 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 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
- To allow the users to control their data directly control as privacy settings (On-demand security control)
- To protect personal information in private cloud
- To specify and limit purpose of data usage

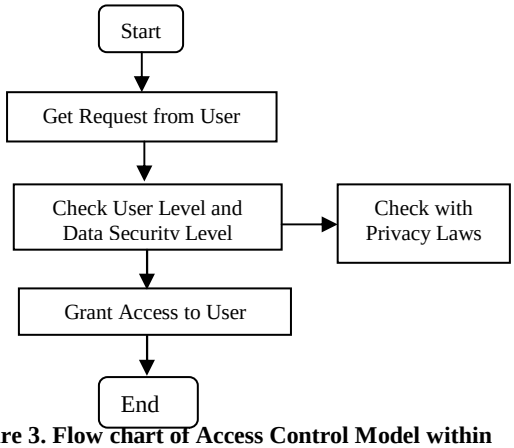


Figure 3. Flow chart of Access Control Model within Privacy Manager on Private Cloud

8.1. 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

8.2. The Proposed Access Control Model (Rule-based Access Control Model) to control access data

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, we denote 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., $(cond_1 \wedge \cdots \wedge cond_n) \vee (cond1_1 \wedge \cdots \wedge cond1_m)$.

8.3. 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

9. 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. This system can enhance the security of the cloud and protect access from the unauthorized users, provide transparency, scalability, vendor independency. 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] 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