View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Queensland University of Technology ePrints Archive

QUT Digital Repository:
http://eprints.qut.edu.au/

This is the published version of this conference paper:

Albeshri, Aiiad Ahmad and Caelli, William (2010) *Mutual protection in a cloud computing environment.* In: IEEE 12th International Conference on High Performance Computing and Communications (HPCC 2010), 1-3 September 2010, Melbourne.

© Copyright 2010 IEEE

Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

Mutual Protection in a Cloud Computing Environment

Aiiad Albeshri[1] and William Caelli[2]

Information Security Institute
Queensland University of Technology
Brisbane, Australia.
Email: [1] a.albeshri@student.qut.edu.au [2] w.caelli@qut.edu.au

***Abstract*—The term “cloud computing” has emerged as a major ICT trend and has been acknowledged by respected industry survey organizations as a key technology and market development theme for the industry and ICT users in 2010. However, one of the major challenges that faces the cloud computing concept and its global acceptance is how to secure and protect the data and processes that are the property of the user. The security of the cloud computing environment is a new research area requiring further development by both the academic and industrial research communities. Today, there are many diverse and uncoordinated efforts underway to address security issues in cloud computing and, especially, the identity management issues. This paper introduces an architecture for a new approach to necessary “mutual protection” in the cloud computing environment, based upon a concept of mutual trust and the specification of definable profiles in vector matrix form. The architecture aims to achieve better, more generic and flexible authentication, authorization and control, based on a concept of mutuality, within that cloud computing environment.*

Keywords: Cloud Computing, Access Control, Reverse Access Control, Profile, Security:

I. Introduction

“Cloud computing” is essentially composed of a large-scale distributed and virtual machine computing infrastructure. This new paradigm delivers a large pool of virtual and dynamically scalable resources including computational power, storage, hardware platforms and applications to users via Internet technologies. Private and public organizations alike can make use of such cloud systems and services while many advantages may be derived when migrating all or some information services to the cloud computing environment. Examples of these benefits include increases in flexibility and budgetary savings through minimization of hardware and software investments. According to Salesforce.com, the market for cloud computing as a whole is predicted to grow to $160B by 2011 [1, 2]. In addition, a study entitled *Leaders in the Cloud* provided by the Sand Hill Group [3], suggests that use and reliance on this new environment for computing is arriving sooner than expected. It states:"*People are asking the same questions about the cloud today that they did about Internet back in 1997*".

Cloud computing could be categorized into two distinct philosophies: *internal cloud* and *external cloud* structures. Internal cloud exists when the cloud structure is only owned and operated by a single enterprise, for example, the United States government. Within this enterprise the data center is shared and the enterprise can run and optimize its requirements. Most importantly, the data center which implements the cloud is owned and operated by the agreed group of departments in the name of the government of the USA. On the other hand, an external cloud is a general and open market offering, such as the “Amazon S3” concept which offers cloud services to anybody. The underlying principle in both here is basically a business model, not a specific technical structure. That is, internal and external clouds usually deploy exactly the same technology. However, with the external cloud the individual company relinquishes control of its information system to the cloud provider, thus requiring extensive legal analysis.

In fact, the migration process into the cloud is very simple. It starts by identifying what an organization needs to move to the cloud, finding the provider, negotiating on some requirements, and finally, signing of the contract. So, overall security may be considered to be based on trust and “keeping fingers crossed (hope)” alone. There is no guarantee that a cloud provider will always follow and meet contract terms and conditions.

Moreover, as the cloud computing environment is based on interaction with all information systems via the Internet, this factor increases risk and security vulnerabilities. One of major challenges that faces the cloud computing concept and its global acceptance is how to secure and protect the data and processes that are the property of the user. According to an IDC Asia/Pacific Cloud Survey (2009) [4], the major concern within the cloud environment was the issue of security. Although the majority of the cloud providers claim that their systems are secure and robust, it has been argued that all these strong security systems can be breached. The Cloud Security Alliance’s initial reports [5, 6, 1] give examples of such violations. These examples include SQL-injection at cloud platform level, phishing of the cloud provider, and third party data control. Also, some recent incidents regarding cloud downtime, such as Gmail (October 2008, for one day), increase the concerns about data being available all the time. And crucially, moving sensitive data (e.g. personal and medical) into the cloud raises critical questions regarding privacy and confidentiality of such data as well as possible legal considerations regarding transborder data flows and the like.

There is a further question: by the end of the contract, how to assure that all data will be totally deleted in a safe

978-0-7695-4214-0/10 $26.00 © 2010 IEEE
DOI 10.1109/HPCC.2010.87

way? Also, certain regulations require data and operations to remain in certain geographic locations. In addition, the auditing process is another problem in the cloud environment, as the owner of the data lacks control in the cloud. Information Security Magazine asks [7]: "*How do you perform an on-site audit when you have a distributed and dynamic multi-tenant computing environment spread all over the globe? It may be very difficult to satisfy auditors that your data is properly isolated and cannot be viewed by other customers.*"

In this paper, we introduce an architecture for a new approach to the problem identified as "*Mutual Protection for Cloud Computing (MPCC)*". The main concept underlying MPCC is based on a philosophy of *Reverse Access Control*, where customers control and attempt to enforce the means by which the cloud providers control authorization and authentication within this dynamic environment, and the cloud provider ensures that the customer organization does not violate the security of the overall cloud structure itself. The scheme involves the matching of the cloud provider security "profile" with that of the client, so as to attain mutual acceptance of the overall security environment. This framework will help to control and monitor the requirement that a cloud provider always meets an organization's security requirements, and that the user cannot readily violate the security stance of the cloud provider, for example by obtaining access to the data and processes of another cloud user.

The rest of this paper is organized as follows: the second section discusses related work; the third section explains the proposed MPCC framework and identifies some key functions; the fourth section discusses a potential implementation for some of the MPCC functions; finally in the fifth section, the paper draws some conclusions.

II. Related Work and Background

According to the literature, most security architectures used within the cloud environment are seen from a "web-services" perspective. This uses the traditional methods of access control, where authentication and authorization decisions are made based on subject attributes, object attributes, and requested rights. Mandatory Access Control (MAC), Role-Based Access Control (RBAC) and the Discretionary Access Control are examples of such traditional methods. For instance, Dawani et al. (2009) introduced (Nego-UCONABC), an access control framework for cloud services based UCONABC (Usage Control) [8]. In this framework, they extended the traditional access control to include recent access control and digital rights management. The authorization process here is based on attributes, obligations and conditions. Attributes are often provided in the form of the digital certificate by which an issuer declares the attributes that an entity has. Obligations are stored in a policy database as a set of rules in XACML.

Dawani et al. argue that Nego-UCONABC provides superior decision-making ability, and would be a better choice to establish a realistic cloud service access control model [8]. However, it is clear that this solution is based on a web-services perspective and does not cover many of the security issues within this new environment, such as:

- How to enforce and guarantee that there will be no shift of data and processes to other locations (as may be required by law and regulations);
- Upon the end of the contract, how to delete the data and processes;
- Resilience and continuity of service;
- Consistent and integral naming services;
- Guarantee of lack of interference across the domains of the cloud, either accidentally or deliberately; etc.

Moreover, this solution still outsources the client's data as well as control into the cloud, and there is no enforcement for the cloud provider to always fulfill the contractual agreement. Such architectures may be regarded as extensions of conventional access control schemes into a service environment. There is, in principle, no scheme to match the access control requirements so defined against those provided by the cloud system or cloud provider. Today, when organizations want to move to the cloud environment they migrate all their data and computations into the cloud. As a result, they have no more control over their data. Even though they have a contract with the cloud provider, there is still no guarantee or means of enforcement that the cloud provider will always meet the enterprise's requirements.

In the MPCC system we expect the cloud system not only to offer the services specified by the client, which are the normal subject/object security and access control definitions, but also, as a first step, the cloud provider must provide evidence that these services are reliably enabled. For example: how do we know that the cloud service provider does indeed offer true subject/object security enforcement? Going one step further: we need to be assured that the access control that we must have enforced by the cloud system is constant, and may be defined and controlled in a dynamic fashion, in line with the flexibility offered by the cloud services themselves. Simply put, the access control parameters required by the cloud client must be "imposed" upon the cloud service while, in the sense of mutuality, the protection specification of the cloud provider must be known and acknowledged by the client. This leads to the overall "mutuality" requirement, whereby access control profiles of the cloud provider and customer need to be defined and aligned. From the client's viewpoint, this may be considered as a "reverse access control (REVACC)" profile.

We now expect the cloud operator and owner to inform each and every client of the access control services it offers, and their level of guaranteed enforcement. Those access control services must, in turn, meet the client's requirements. The client's security requirements may be expressed through the use of RBAC, for example. Thus the client requires the cloud provider to implement RBAC, as the client is no longer in control of the relevant computer systems, now virtualized.

III. Mutual Protection for Cloud Computing (MPCC) Framework

It is important, therefore, for any organization which wants to move all or some of its services to the cloud to define

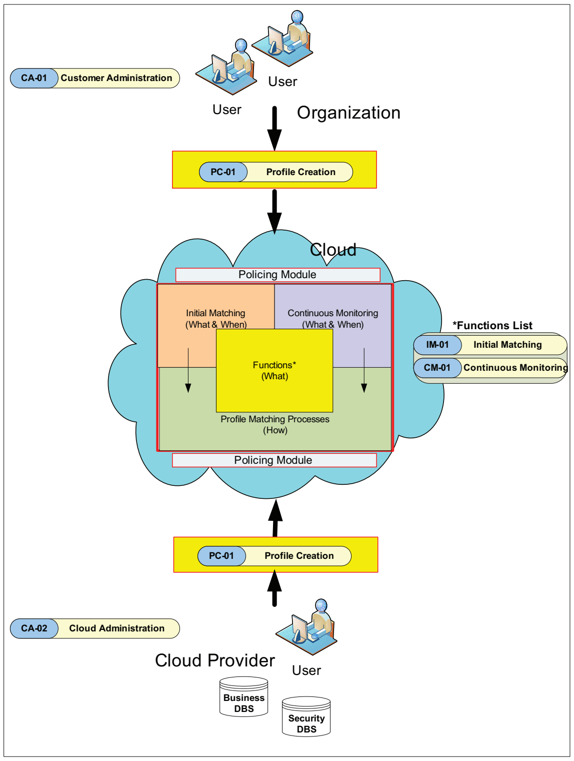

Figure 1. Mutual Protection for Cloud Computing (MPCC) Framework

its requirements and to match up those requirements with the services offered by cloud providers. For instance, an organizations need to be sure that the file level and process access control requirements for their services are met by the cloud provider. One of the main goals of the MPCC approach is to provide a secure outsourcing of computational processes without outsourcing control. Some examples of access control needs include:

- Authorization of an organization's employees to access the systems now operating in the cloud;
- Data protection (Confidentiality, integrity and availability) in such shared and open environments;
- Encryption of an organization's data for confidentiality assurance, when specified;
- Location data for an organization's data;

In this proposed framework, each side (i.e. the client organization and the cloud provider) has to create its appropriate profile. The proposed "PC-01 Profile Creation" function, for example, is responsible for such a profile creation process. After the creation of a profile by both sides, a cloud provider may advertise its profile as may the proposed client, seeking proposals. The main problem, and again a major subject of this research project, is the "mating" of the two profile sets to produce a measure of compatibility.

Importantly, within the MPCC framework both organization and cloud provider need to apply IS management standards such as ISO/IEC 27001 [9] and ISO/IEC 27002 [10] as evidence of management commitment to and responsibility for IS.

A. MPCC Functions:

In the MPCC framework we introduce an architecture for mutual protection in the cloud computing environment. In this architecture, each side (organization and provider) has to create its own profile using the profile creation function. The associated "policing module" consists of two functions: an "Initial Matching Function", and a "Continuous Monitoring Function" (Figure 1).

1) PC-01: Profile Creation Function: The term "profile" in our terminology consists of set of access control vectors and is derived from the accepted terminology used elsewhere, e.g. in the creation of "profile" statements in a mandatory access control environment such as under SELinux, "B2" Multics, etc. In our approach, both the cloud provider and the organization have their own profile. This profile consists of a set of vectors. An example of such a profile is as follows:

- **Organization's Profile:**

This profile contains the following parameters (we tell the cloud what system we want to run and what access control we will require):

Organization's profile categorizes each of organization's applications, and says what access control we want you, the cloud provider, to implement for us.

Organization's profile consists of a set of vectors for each application or service wanted by the organization.

$$profile_{org} = \{vector_1, vector_2, ..., vector_n\}$$

where n = number of applications needed to be in cloud.

There is a vector for each application within the organization. This vector includes some parameters regarding this application. These parameters may include application name, access control requirements for this application, geographic and location requirements, security requirements (Confidentiality, Integrity and Availability), etc.

$$vector_{app} = \{parameter_1, parameter_2, ..., parameter_n\}$$

where, n = number of vector parameters for this service.

For example, vector (payroll) = {Payroll, RBAC, Brisbane, Confidentiality, Integrity, Availability, IS15408}.

This vector is for the payroll service, the access control provided is RBAC or DAC, Data location will be in Australia (Sydney or Brisbane), confidentiality, integrity and availability should be guaranteed, also this service should be certified by IS15408 common criteria.

Organization passes its profile to the cloud and expects the cloud to return the matching profile.

- **Cloud provider's Profile:**

This profile contains the following parameters (cloud tells organization what it is offering, so enterprise can make a decision). Cloud provider has a vector for each service it provides. Cloud provider should advertise its full profile in the cloud.

Table I
PROFILE OF ORGANIZATION

	Application	AC Requirements	Geographic Requirements	Security Requirements			Cert.
				Confidentiality	Integrity	Availability	
Vector 1	Payroll	RBAC	Brisbane	Yes	Yes	Yes	IS15408
Vector 2	Inventory	DAC	Australia	Yes	Yes	No	IS15408
...	...	...	...	...	...	...	...

Table II
PROFILE OF CLOUD PROVIDER

	Service	AC Requirements	Geographic Location	Security Requirements			Cert.
				Confidentiality	Integrity	Availability	
Vector 1	Payroll	RBAC, DAC	Australia, China, USA	Yes	Yes	Yes	IS15408
Vector 2	Inventory	All	India	Yes	Yes	No	IS15408
...	...	...	...	...	...	...	...

$$profile_{cloud} = \{vector_1, vector_2, ..., vector_n\}$$

where n = number of services offered by the cloud provider.

This profile consists of a set of vectors for each service provided by the cloud.

$$vector_{service} = \{parameter_1, parameter_2, ..., parameter_n\}$$

where, n = number of vector parameters for this service.

For each application within the cloud there is a vector which includes some parameters regarding this service. These parameters may include service name, access control requirements provided for this service, geographic and location requirements, security requirements (Confidentiality, Integrity and Availability) provided by the cloud provider. For example:

vector (payroll) = {Payroll, {RBAC, DAC}, {Australia (SYD, BNE), China, USA (NY) }, Confidentiality, Integrity, Availability, IS15408}.

This vector is for the payroll service, the access control provided is RBAC or DAC, data location will be in Australia, China or USA , and the confidentiality, integrity and availability are guaranteed, and this service is certified by IS15408 common criteria.

Cloud provider should advertise its full profile in the cloud.

One of the steps in the matching profile process is to verify that all claimed profiles from cloud provider's side are true. For example, if cloud provider claims it will provide RBAC, then by analyzing the previous audits (logs file), the matching process can verify this claim. Another possible solution may be that within each vector there is a certificate (something like a digital certificate) issued from a certificate authority.

2) IM-01: Initial Matching Function: An organization creates its own profile (set of vectors) and passes it into the cloud. This function will find and compare this profile with all available profiles for cloud providers and match it with these profiles. In addition, the organization's profile should be a subset of the profile of cloud provider.

$$profile_{requested} \subseteq profile_{cloud}$$

Based on the result from this matching, a decision will be made to accept the deal and make the contract between organization and cloud provider.

3) CM-01: Continuous Monitoring Function: By definition, the cloud is dynamic, so its vectors (profile) are dynamic and may be changed. For example, the geographic location of the data might be changed from one place to another. Thus, we need a policing function which can audit and watch the agreements and access control requirements. The contract should define how to police and who does the policing. The policing function might be a service provided by a third party or deployed within the organization. If an organization has chosen a cloud provider, they will have to agree on the procedure of the policing function, which will monitor that the cloud provider meets, and continues to meet, the access control and security requirements for the organization. Continuous Monitoring Function will keep an eye on the profile of the cloud provider, and conduct ongoing assessment and regular checking to make sure there are no changes in the profile. If any change is detected (e.g. the location of the data storage is changed which means a breach for the location agreement), the organization must be notified and all activities should be stopped. This function has to monitor the actions of the organization's employees and the cloud provider's employees. A regular report should be generated and sent to the organization for audit and review purposes.

4) CA-01: Customer Administration Function: The main purpose of this function is to control and manage all administration activities related to the information system within the organization. Organization need to manage the access control policies and procedures. Thus, organizations should develop, broadcast, and periodically update and review the access control policy. Organizations need to address the scope, purpose, responsibilities, and procedures that help in the implementation process of the access control policies. Some guidance is available for such security policies and procedures, such as NIST Special Publication 800-12 [11]. Moreover, access control policy and procedures should be consistent with applicable laws, regulations, and standards.

In addition, organizations need to control and manage the accounts of their information systems. This includes the process of creating, activating, modifying and deleting accounts. In addition to the identification of authorized users, this function is responsible for assigning authorized users their access rights and privileges. Furthermore, this function will monitor the anonymous accounts and also remove and terminate any expired account.

Moreover, the employees within the organization need to be aware of the security issues related to the information system. In MPCC architecture, this function is responsible for providing the organization with the knowledge and awareness training to all users of the information systems. The main goal of the awareness process is to make the users familiar with IT security concerns and with how to respond to them. So, the main audience of this function are the IT users. NIST Special Publication 800-50 [12] provides guidance on how the organizations may build their security awareness process.

Also, the organization frequently reviews and analyses information system audit records that have been provided by the continuous matching function. These reports will help to detect any inappropriate or unusual activity, and to investigate suspicious activity or suspected violations. All findings must be reported to the people in charge within the organization to take the necessary actions.

Finally, any organization needs to assess and review the level of security within itself, especially when using the cloud environment. This function will help the organization assess the security level, based on the regular reports resulted from the audit and analysis process. NIST Special Publication 800-53A [13] offers guidance for such assessment. As well, legal regulations must be considered when assessing these security levels.

5) CA-02: Cloud Administration Function : The cloud provider needs to administer the operations and control of the actual cloud structure itself. In addition, cloud provider should manage the users' identity and assigns users to the roles, provides users with approved accounts and privileges, and facilitates change requests and approvals over time.

In addition, cloud providers should do training for their users who are dealing with the data. This function focuses on teaching skills which allow a user to act professionally in response to an incident which may breach the security of the organization. NIST Special Publication 800-50 [12] provides guidance on how the cloud providers may achieve the appropriate security training for their users based on the specific requirements of the organization and the information systems.

Moreover, cloud provider should enforces assigned access authorizations to their users based on an appropriate policy. Based on the agreement or contract, cloud provider should employ the required access control policies and associated access enforcement mechanisms. Encryption of stored information could be an example of such an access enforcement mechanism.

IV. Potential Implementation

In this section we briefly explain how to build or simulate the cloud environment, and how some of the proposed functions from the previous section for MPCC architecture could be implemented using existing technologies.

A. Cloud implementation/simulation

The cloud could be implemented either with the use of a virtual infrastructure provisioning method such as Amazon's Elastic Compute Cloud (EC2), an application development and delivery such as Google's App Engine (GAE), or by building your own cloud from scratch, using your own storage, processing, and networking resources [14]. For implementation and testing purposes, the third option is preferred. It involves building and managing your own cloud using open source software and tools. However, this requires some knowledge and professional skills to optimize all resources.

Furthermore, there is some open source software that could be used in cloud computing. For instance, Apache , which is a cloud-based tool that could be used in the implementation of the web server. Also, virtualized application in the cloud needs to use a database and a database relies on DBMS/RDBMS to organise, store, and retrieve data. According to MySQL web site, it has become the most popular open source database. It is used by the world's largest companies, such as Yahoo, Google and YouTube. Moreover, there are some open source platforms that can be used to run dynamic web sites and servers, such as LAMP (Linux, Apache, MySQL, and PHP).

For the communication process, HTTP (Hypertext Transfer Protocol) is recommended. It is a famous application level protocol for distributed and collaborative information systems. The main idea of this protocol is based on a client/server (or request/response) approach, where the client initiates a request while the server is listening, waiting for the requests. Moreover, these communications need to be secure. Thus, some security standards have to be used such as SAML (Security Assertion Mark-up Language). SAML is an XML-based standard for a secure authentication and authorization processes. SAML relies on HTTP as its communications protocol.

B. PC-01: Profile Creation Function

For creating the profile we might use the relational database (e.g. MySQL), by creating a table for each profile, where each row in this table represents a vector for a specific application/service.

For expressing and evaluating access control policies, the eXtensible Access Control Markup Language (XACML), a well-established OASIS standard, can be used [15].

The exchanged "profile" messages in the cloud could be based on the protocols that are presented in the Security Assertion Markup Language (SAML) [15]. The SAML standard defines a framework for exchanging security information between online business partners.

Statements and certificates made by the cloud provider may be verified or checked by either a consumer association, or preferably by a quality assurance group of the Government. The profile claimed by the cloud provider should be verified and enforced and may be use the law in here . In this conception, cloud computing is like a utility (i.e. water, power, etc), and utilities should be regulated. Therefore, the profile made by the cloud provider should be checked and validated.

For the “Profile Matching Process” we will create a program (using Java Programming language) which compares the profile of both sides (the organization and the cloud provider), and produces an index which shows how much these profiles are matched. Based on this index the organization will decide whether or not to sign the contract.

“Continuous Monitoring Function” will do the policing functions in order to make sure no changes have been made by the cloud provider. It utilizes the “Profile Matching process”. As mentioned earlier in this paper, this might be done by a third party nominated at contract time. We might use the idea of distance bounding protocols [16] (cryptographic protocols) to check if there is any geographical/location changes to the data. Their main idea is to calculate the time delay for a round trip message, and then based on this time delay the physical distance is calculated.

V. Conclusions and future work

The security of cloud computing is a new research area requiring more input from both the academic and industrial communities. Although recent research has addressed the problems of protecting cloud systems, usually via security processes offered under “web services” structures, several issues still remain to be investigated. This paper introduces a new approach for *Mutual Protection for Cloud Computing (MPCC)*. The main concept underlying MPCC is based on a philosophy of *Reverse Access Control*, where customers control and attempt to enforce the means by which the cloud providers control authorization and authentication within this dynamic environment, and the cloud provider ensures that the customer organization does not violate the security of the overall cloud structure itself. The future work for the MPCC project will be in how to implement this framework. Moreover, evaluation of success of the proposed architecture will concentrate on assessment of the likely impact upon time and cost of system development processes, compared to those without the proposed structures. In addition, vector and profile standardization will be more easily and more quickly accomplished if there is an international standard to agree on notations used for vectors and profiles.

VI. Acknowledgment

Albeshri gratefully acknowledges King Abdulaziz University (KAU) in Saudi Arabia for sponsoring his PhD studies.

References

[1] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, “Controlling data in the cloud: outsourcing computation without outsourcing control,” in *Proceedings of the 2009 ACM workshop on Cloud computing security*, pp. 85–90, ACM, 2009.

[2] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility,” *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599–616, 2009.

[3] K. Pemmaraju, “Leaders in the cloud: Identifying the business value of cloud computing for customers and vendors,” Mar 2010. available at: http://www.sandhill.com/opinion/editorial.php?id=296.

[4] A. D. Ho, “Cloud strikes all the right chords but security concerns keep it from hitting the perfect pitch,” Nov 2009. Available at: www.idc.com.sg.

[5] “Cloud security alliance: Security guidance for critical areas of focus in cloud computing v2.1,” Dec 2009. Available at: www.cloudsecurityalliance.org.

[6] “Cloud security alliance: Top threats to cloud computing v1.0,” Mar 2010. Available at: www.cloudsecurityalliance.org.

[7] N. Roiter, “How to secure cloud computing,” Mar 2009. Available at: http://searchsecurity.techtarget.com.

[8] C. Danwei, H. Xiuli, and R. Xunyi, “Access control of cloud service based on ucon,” in *Cloud Computing*, pp. 559–564, Springer Berlin / Heidelberg, 2009.

[9] Standards Australia, “AS/NZS ISO/IEC 27001: 2006 Information technology - Security techniques - Information security management systems - Requirements,” June 2006.

[10] Standards Australia, “AS/NZS ISO/IEC 27002: 2006 Information Technology - Security Techniques - Code of practice for information security management,” July 2006.

[11] NIST, “Nist special publication 800-12 : An introduction to computer security: The nist handbook,” tech. rep., NIST: National Institute of Standards and Technology, U.S. Department of Commerce, Oct 1995.

[12] M. Wilson and J. Hash, “Nist special publication 800-50: Building an information technology security awareness and training program,” tech. rep., NIST: National Institute of Standards and Technology, U.S. Department of Commerce, Oct 2003.

[13] R. Ross, A. Johnson, S. Katzke, P. Toth, G. Stoneburner, and G. Rogers, “Nist special publication 800-53a: Guide for assessing the security controls in federal information systems,” tech. rep., NIST: National Institute of Standards and Technology, U.S. Department of Commerce, July 2008.

[14] A. Sharma, “Cloud computing and open source,” May 2010. Available at: http://ldn.linuxfoundation.org/article/cloud-computing-and-open-source.

[15] OASIS, “Security assertion markup language (saml) 2.0 technical overview,” tech. rep., OASIS, Feb 2008.

[16] G. Hancke and M. Kuhn, “An rfid distance bounding protocol,” in *IEEE/Create-Net SecureComm*, pp. 67–73, IEEE Computer Society Press, 2005.