Efficient Architecture Design For Connecting and Automating of work flows and Cloud Security Control

N.Ashok Kumar[1]

[1]M.Tech., Assistant professor, Department of CSE, Narayana Engineering College, Nellore.

[1]ashok.nadadura@gmail.com

R.Ganga Sagar[2]

[2] M.Tech(CSE),13711D5815 , Narayana Engineering College, Nellore

[2]rgsagar108@gmail.com

ABSTRACT: Cloud computing is an upcoming paradigm that offers tremendous advantages in economical aspects, such as reduced time to market, flexible computing capabilities, and limitless computing power. To use the full potential of cloud computing, data is transferred, processed and stored by external cloud providers. However, data owners are very skeptical to place their data outside their own control sphere. This paper discusses to which degree this skepticism is justified, by presenting the Cloud Computing Confidentiality Architecture. The Cloud Computing Confidentiality Architecture is a step-by-step Architecture that creates mapping from data sensitivity onto the most suitable cloud computing architecture. The concept is extended by providing a Reference Architecture which includes a complete overview of the actors and their roles and the necessary architectural components for managing and providing cloud services.

Keywords: Cloud computing, cloud computing confidentiality architecture, Reference architecture.

1. INTRODUCTION:

The most thorough security controls needed to protect the most sensitive data may not be guaranteed in public cloud computing architectures, while they can be realized in private cloud computing architectures. These days, you're frequently processing, storing, or transmitting data that's subject to regulatory and compliance requirements. When that data falls under regulatory or compliance restrictions, your choice of cloud deployment (whether private, hybrid or public) hinges on an understanding that the provider is fully compliant. Otherwise, there's the risk of violating privacy, regulatory or other legal requirements. The implications for maintaining the security of information are significant when it comes to privacy.

Today almost all PC users have access to the internet. More and more users are using at least some cloud services, like e-mail, Facebook, Google Docs and so forth. But not only private users are switching to cloud services, also companies and governments are adopting them. Cloud computing offers many benefits for its users, e.g. cost savings, increased flexibility and ubiquitous access to the data just to mention a few. There have been enough privacy violations outside the realm of cloud computing for there to be concern about any system—cloud-based or traditional—when storing, processing or transmitting sensitive information. The cloud has its own examples as well. In 2010, several cloud privacy information exposures occurred with a number of cloud-based services, including Facebook, Twitter and Google.

Privacy concerns within the cloud model aren't new. As a tenant with legal privacy obligations, your handling of privacy issues is no different if you use the cloud. Just as you wouldn't store such information on a server without adequate controls, you wouldn't select any cloud provider without verifying it meets the same benchmarks for how it protects data at rest, in transmission or while processing.

Your policies may exclude any external provider managing sensitive information for you, including cloud providers. While there may be a perception that the computer on your desk is safer than a public cloud, it's probably not (unless you're taking unusual technical and procedural precautions). Safety and governance are two separate issues, and as part of due diligence, you'll need to fully understand your provider's privacy governance, as well as its security practices and guidelines.

1.1 Cloud Computing

The main concept of cloud computing is not new, but it took quite some time until its successful realization. Many authors state that cloud computing can be regarded as next step in the evolution of distributed computing. Cloud computing enables its users to access almost unlimited computing resources in a comfortable and scalable way.

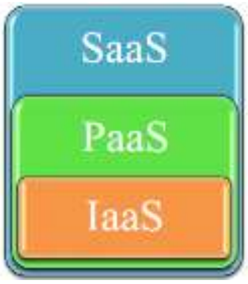
1.2 Cloud Computing Definition

There is no single definition for cloud computing but according to recent literature cloud computing refers to: both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services.[2].

Cloud computing is further distinguished between private and public clouds. Private clouds are mainly clouds which are operated by companies and are used inside their intranet only or via VPN access also from outside, but are not accessible for non-company members. Public clouds are open and accessible for everyone, not only business users but also private users can use the cloud services. Of course open means not free and any cloud service providers charge the users for providing their services. Besides that there are also community and hybrid clouds. A community cloud can only be accessed by a specific community of consumers from different organizations that have shared concerns. A hybrid cloud is a composition of two or more distinct cloud infrastructures (e.g. a public and a private cloud).

1.2.1 Software as a Service (SaaS)

This is the level which consumers are most familiar with. Providers are gaining access to an application running on their web servers, usually as web application. Common examples are email, social networking and other software applications like word processing.



1.2.2 Platform as a Service (PaaS)

Providers are as a platform where the consumers can deploy and run their own applications on without having to manage the underlying hardware. Tools and libraries as well as the network and storage space are also provided. Examples are Windows Azure and Google App Engine.

1.2.3 Infrastructure as a Service (IaaS)

Raw computing power and storage space is provided. Consumers can fully control the underlying virtual machines, including operating system, network and storage space. Providers in this category are Amazon EC2 and Rackspace Cloud Services.

1.3 Cloud Computing Issues

Cloud computing does not only have advantages. There are some disadvantages and issues arising with the use of cloud services as well. One obvious disadvantage is that an active internet connection is necessary for using a cloud service. Another concern of many users have is that their data is no longer stored locally and they may loose control over it as soon as it is stored in the cloud. But some users may not even have a choice to use cloud services or not or may not be aware that they are using a cloud service at all which can also be an issue.

The transmission of data over the internet also imposes threats to data confidentiality, on the one hand during transmission, especially in case an unsecure connection is used and on the other hand while the data is stored, if it is stored unencrypted because there may be possible data leaks on a provider's server.

Not only for private users but especially for companies several legal issues arise due to different laws. Many laws are only applicable in one country, or inside the European Union or the USA. As the exact position where the data is stored in the cloud is not known, it is also unclear which laws are applicable. In addition many local laws treat data which is stored locally different than data which is stored somewhere on the web. This makes it even harder to decide which law is applicable. Different countries also have different perspectives regarding privacy[13] so in some cases companies may not even be allowed to use cloud services due to an uncertain legal situation. To cope with this problem, e.g. Europe has introduced its safe harbor convention where a cloud service provider can decide to obey stricter privacy conventions than demanded by the law and is therefore treated like a European company.

1.4 Attackers and their Interest in Private Data

There are three different groups of attackers which may have an interest in getting access to private user data stored in the cloud: hackers, cloud service providers and governments.

1.4.1 Hackers

The main interest for hackers in a user's private data is for illegal activities. Therefore, the most interesting data is credit card information, bank account details, health records, bank login details and so on. Hackers may gain a reasonable profit by selling this data. Unlike the service providers and governments hackers have no legal possibilities to access the user's data; instead their activities are also subject to criminal prosecution.

1.4.2 Cloud Service Providers

Like hackers cloud service providers want to gain access to their users' data as well, mainly because of achieving profit. In contrast to hackers they have legal possibilities to access this data, mainly due to the terms of service agreement, a contract which every user has to agree. Many service providers scan user data on tags which are then used to show highly personalized ads. But also more complex data and statistics are recorded, bundled and analysed (data mining) to be able to do so called user profile marketing, making prediction on what items a user might buy in the near future, what is his next travel destination etc.

2. LITERATURE REVIEW

To explore the available knowledge on the area of cloud computing and confidentiality, a literature review is conducted using a systematic approach. The role of a literature review is depicted in Figure 2-1. The objectives of a literature review are:

1.To understand the current state of knowledge in a research area .

2.What is known/generally accepted

3.What questions remain unanswered

4.Where do conflicting results exist

5.To show how the current research project is linked to previous research (cumulative tradition)

6.To summarize and synthesize previous research

7.To critically analyze previous research: strengths and weaknesses

8.To learn from others and stimulate ideas .

The first step in a literature review is selecting the top 25 journals to search information in. This ranking is researched and published by several groups, of which the Association of Information Systems is the most recent one (AIS 2009a). The second step is selecting one or more search engines that index these top 25 journals, after which the journals can be examined by searching on a predetermined set of keywords.

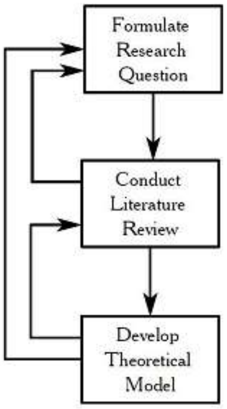

Formulate Research Question
Conduct Literature Review
Develop Theoretical Model

Figure 2-1: Literature Review Role.

2.1 RELATED WORK:

Improving the confidentiality of information stored in cloud databases represents an important contribution to the adoption of the cloud as the fifth utility because it addresses most user concerns. Our proposal is characterized by two main contributions to the state of the art:architecture and cost model.

Although data encryption seems the most intuitive solution for confidentiality, its application to cloud database services is not trivial, because the cloud database must be able to execute SQL operations directly over encrypted data without accessing any decryption key.Natıve solutions encrypt the whole database through some standard encryption algorithms that do not allow any SQL operation directly on the cloud. As a consequence, the tenant has two alternatives for any SQL operation: downloading the entire database, decrypting it, executing the query and, if the operation modifies the databases, encrypting and uploading the new data decrypting temporarily the cloud database, executing the query, and re-encrypting it. The former solution is affected by huge communication and computation overheads, and costs that would make the cloud database services quite inconvenient; the latter solution does not guarantee data confidentiality because the cloud provider obtains decryption keys.

The right alternative is to execute SQL operations directly on the cloud database, but avoiding that the provider obtains the decryption key. An initial solution in this direction was presented in [5]. This proposal is based on data aggregation techniques [8], that associate plaintext metadata to sets of encrypted data to allow data retrieval. moreover, plaintext metadata may leak sensitive information and data aggregation introduces unnecessary network overheads. The use of fully homomorphic encryption [11] would guarantee the execution of any operation over encrypted cloud data, but existing implementations are affected by huge computational costs [11] to the extent that they would make impractical the execution time of SQL operations over a cloud database. Other encryption algorithms characterized by acceptable computational complexity support a subset of SQL operators [12], [13], [14].For example, an encryption algorithm may support the order comparison command [12], but not a search operator [14]. The drawback related to these feasible encryption algorithms is that in a medium-long term horizon,the database administrator cannot know at design time which database operations will be required over each database column. This issue is in part addressed in [10] by proposing an adaptive encryption architecture that is founded on an intermediate and trusted proxy. This tenant's component, which mediates all the interactions between the clients and a possibly untrusted DBMS server,is fine for a locally distributed architecture, but it cannot be applied to a cloud context. Indeed, any centralized component at the tenant side prevents the scalability and availability that are among the most important features of any cloud utility service. A solution to this problem was presented in [9]: the proposed architecture allows multiple clients to issue concurrent SQL operations to an encrypted database without any intermediary trusted server, but it assumes that the set of SQL operations does not change after the database design. A first idea to integrate adaptive encryption schemes with a proxy free architecture was proposed by the same authorsin [15].

3. ARCHITECTURE DESIGN

Before entering into any commercial agreement, an organization that considers using an outsourcing service shall carry out a specific analysis in order to:

1. Clearly identify the data and processing operations which will be passed to the Cloud;
2. Define its own requirements for technical and legal security;
3. Carry out a risk analysis to identify the security measures essential for the organization;
4. Identify the relevant type of Cloud for the planned processing;
5. Choose a service provider offering sufficient guarantees;
6. Review the internal security policy;
7. Monitor changes over time.

The above steps are followed to guarantee data confidentiality:

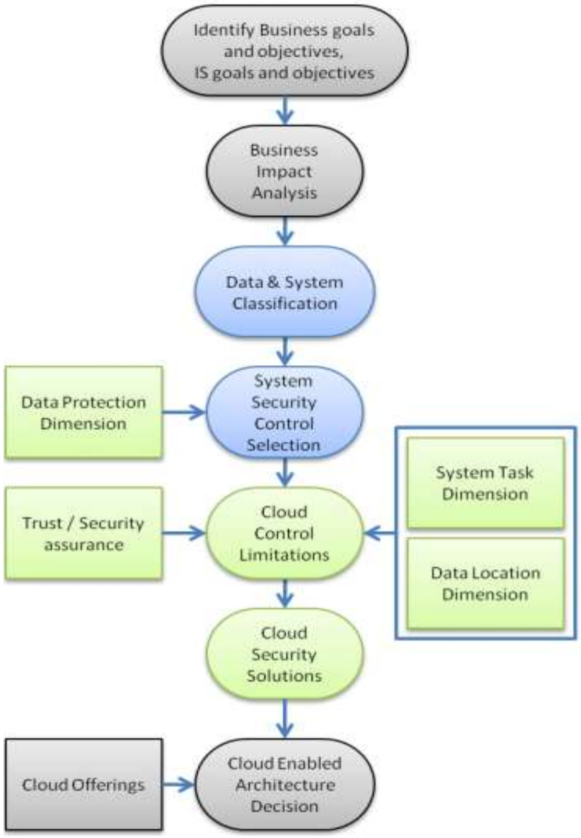

Identify Business goals and objectives, IS goals and objectives
Business Impact Analysis
Data & System Classification
Data Protection Dimension
System Security Control Selection
Trust / Security assurance
Cloud Control Limitations
System Task Dimension
Data Location Dimension
Cloud Security Solutions
Cloud Offerings
Cloud Enabled Architecture Decision

Figure 3-1: The Cloud Computing Confidentiality Architecture

3.1 The Cloud Computing Confidentiality Architecture

The Cloud Computing Confidentiality Architecture will enable companies to review the possibilities to engage in cloud based services, based on the confidentiality of the data used within the company.

The goal of the Architecture is to explain the differences between security in cloud computing environments, and the security in present-day information security practices[5]. This explanation is done by describing the first steps of the IT risk management strategy, and identify which differences will appear when these steps are performed in a cloud computing environment and propose possible solutions to compensate the differences[20]. As it is a good practice for every enterprise to follow such a risk management strategy to secure their data and information systems, the architecture presented here will be relevant to every entity interested to work with cloud based information systems.

Based on the topic of integrated network analysis and design[23], the architecture is approached from top-down perspective to ensure that security development is consistent with organizational goals and objectives and overall information system goals and objectives.In this top-down approach,The explination starts from the need of IT security in the context of strategic goals of the business. From this abstract high level we go down to more concrete parts of the framework. Via a Business Impact Analysis we obtain the business processes and information systems that are deemed important to the business, both in terms of criticality and confidentiality.

With the identified information systems supporting these processes and the information types involved in these information systems, we classify each information type on the topic of confidentiality. When all information types involved in a system have been classified, we can label the confidentiality of an information system by low, moderate or high confidentiality impact level.

With the confidentiality labels associated with the information systems, **we** the risk involved can be ascertained, and define which controls are needed for each confidentiality level.These basic recommendations are adjusted for cloud computing environments, by involving knowledge from our literature review in the form of three dimensions. These dimensions are:

1.Protection mechanisms, which refers to the controls that protect information systems and data.

2.Data location, which refers to the amount of control the data owner can exert over the data itself, depending on where the data is located.

3.System tasks, which refers to whether the data is processed, transferred, stored, or a combination of the three.

Each dimension has its peculiarities in relation to cloud computing, Data protection concerns the layers of protection, from higher abstract level controls to the low technical and physical controls. The Architecture is presented in Figure 3-1. The gray boxes are described to identify goals and objectives at two levels The blue boxes represent the present-day information security practices, in the form of recommendations concerning data classification and control selection. The green rectangles represent important variables in our architecture, in the form of the dimensions from the literature review, and trust related issues. These variables either have their effect on the control selection in section 3.2, or on identification of cloud control limitations.

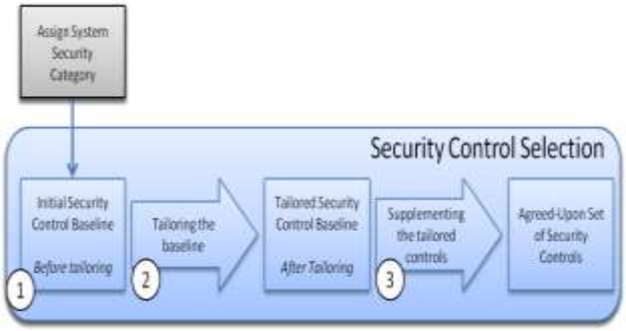

Assign System Security Category
Security Control Selection
Initial Security Control Baseline
Before tailoring
1
Tailoring the baseline
2
Tailored Security Control Baseline
After Tailoring
Supplementing the tailored controls
3
Agreed-Upon Set of Security Controls

Figure 3-2: The process of security control selection

3-2 Security control selection

In this section, the control selection process is described.The process is started by describing security controls classes and which security control families there are. Then description of the control selection process, presenting a recommended baseline of controls for each impact level of an information system. How this baseline can be refined to match the specific requirements of an organization is also shown. The result will be a list of required technical controls to match the security requirements of an information system given the confidentiality impact level of the system.Security controls, when used correctly, can prevent, limit or determine threat-source damage to organization.

Security controls can be placed into three classes:

Technical security controls
Technical controls can be used to protect against specific types of threats. These controls can range from simple to complex measures and consist of a mix of software, hardware and firmware. Next to standalone controls, technical controls also support the management and operational controls described below.

Management security controls
Management security controls are implemented to manage and reduce risks for the organization and to protect an organization's mission. Management security controls can be considered of the highest level of controls, focusing on the stipulation of policies, standards and guidelines, which are carried out by operational procedures to fulfill the organization's goals and missions.

Operational security controls
Operational security controls are used to correct operational deficiencies that might be exploited by potential attackers. These controls are implemented following good industry practices and a base set of requirements in the form of technical controls. Physical protection procedures and mechanisms are examples of operational security controls.

When organizations start the selection process, there are three steps to be executed sequentially:

1. Selecting the initial security control baseline
2. Tailoring the security control baseline
3. Supplementing the tailored security controls

3.2.1 Selecting the initial security control baseline

The selection process begins with a baseline of controls, which are later on tailored and supplemented when the need arises.

3.2.2 Tailoring the security control baseline

After selecting the initial security control set the organization continues the selection process by tailoring this baseline to their specific business conditions.

3.2.3 Supplementing the tailored security controls

The tailored security control baseline acts as the starting point for determining whether or not this selection of controls provides enough security for the information system. This is done by comparing the organizations assessment of risk and what is required to sufficiently mitigate the risks to the organization. In many cases, additional controls and control enhancements must be selected to supplement the tailored security control baseline. Two approaches can be taken to identify which additional controls and control enhancements must be included in the final agreed-upon set of controls; the r*equirements definition* approach and the *gap analysis* approach, which will be explained next.
Following the *requirements definition* approach, the organization investigates possible threats and acquires credible and specific information about what adversaries may be capable of, as well as what damage human errors may inflict. With this assessment of possible threats, additional security can be obtained by adding controls and control enhancements.
In contrast to the above requirement definition approach, the *gap analysis* approach begins with an assessment of the current security capabilities, followed by a determination of what threats can be expected. This approach identifies the *gap* between the current security capabilities and selects additional controls and control enhancements.
The result of the whole control selection process will be the list of required technical security controls to match the requirements of an information system given the confidentiality impact level of the system.

3.3 Composition of system components

Composition of system components to support the Cloud Providers activities in arrangement, coordination and management of computing resources in order to provide cloud services to Cloud Consumers. Figure 3-3 shows a generic stack diagram of this composition that underlies the provisioning of cloud services. A three-layered model is used in this representation, representing the grouping of three types of system components Cloud Providers need to compose to deliver their services. In the model shown in Figure 3-3, the top is the service layer, this is where Cloud Providers define interfaces for Cloud Consumers to access the computing services[2]. Access interfaces of each of the three service models are provided in this layer. It is possible, though not necessary, that SaaS applications can be built on top of PaaS components and PaaS components can be built on top of IaaS components. The optional dependency relationships among SaaS, PaaS, and IaaS components are represented graphically as components stacking on each other; while the angling of the components represents that each of the service component can stand by itself. For example, a SaaS application can be implemented and hosted on virtual machines from an IaaS cloud or it can be implemented directly on top of cloud resources without using IaaS virtual machines.

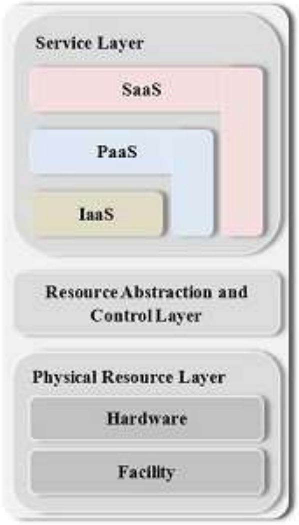


Figure 3-3: Cloud Provider - composition of system components.

The middle layer in the model is the resource abstraction and control layer. This layer contains the system components that Cloud Providers use to provide and manage access to the physical computing resources through software abstraction. Examples of resource abstraction components include software elements such as hypervisors, virtual machines, virtual data storage, and other computing resource abstractions. The resource abstraction needs to ensure efficient, secure, and reliable usage of the underlying physical resource[22]s. While virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are also possible. The control aspect of this layer refers to the software components that are responsible for resource allocation, access control, and usage monitoring. This is the software fabric that ties together the numerous underlying physical resources and their software abstractions to enable resource pooling, dynamic allocation, and measured service. Various open source and proprietary cloud software are examples of this type of middleware. The lowest layer in the stack is the physical resource layer, which includes all the physical computing resources. This layer includes hardware resources, such as computers, networks,storage components and other physical computing infrastructure elements. It also includes facility resources, such as heating, ventilation and air conditioning, power, communications, and other aspects of the physical plant. Following system architecture conventions, the horizontal positioning, i.e., the layering, in a model represents dependency relationships – the upper layer components are dependent on adjacent lower layer to function. The resource abstraction and control layer exposes virtual cloud resources on top of the physical resource layer and supports the service layer where cloud services interfaces are exposed to Cloud Consumers, while Cloud Consumers do not have direct access to the physical resources.

Conclusion:

The Cloud Computing Confidentiality Architecture presented is a step-by-step Architecture that creates mapping from data sensitivity onto the most suitable cloud computing architecture. The Architectural Components of the Reference Architecture describes the important aspects of service deployment and service composition of system components. This concept can be further enhanced by cloud provider by conducting activities in the areas of service deployment, cloud service management, security, and privacy.

References:

[1]Amazon. (2009b). Amazon Virtual Private Cloud (Amazon VPC). Retrieved December 28, 2009, from http://aws.amazon.com/vpc/.

[2]Andrzejak, A., Kondo, D. and Anderson, D. (2010). Exploiting Non-Dedicated Resources for Cloud Computing. In Proceedings of 12th IEEE/IFIP Network Operations & Management Symposium (NOMS 2010), Osaka Japan.

[3]Antón, A., Bertino, E., Li, N. and Yu, T. (2007). A roadmap for comprehensive online privacy policy management. *Communications of the ACM*, *50*(7): 116.

[4]Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R. et al. (2009). Above the clouds: A Berkeley view of cloud computing. *EECS Department*, *University of California*, *Berkeley*, *Tech. Rep. UCB/EECS-2009-28*.

[5]Baralis, E. and Chiusano, S. (2004). Essential classification rule sets. *ACM Transactions on Database Systems*, *29*(4): 635-674.

[6]Bardin, J., Callas, J., Chaput, S., Fusco, P., Gilbert, F. et al. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing v2.1, Retrieved January 28, 2010, from Cloud Security Alliance, from http://www.cloudsecurityalliance.org/guidance/

[7] NIST SP 800-145, "A NIST definition of cloud computing", http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

[8] NIST SP 800-146, "NIST Cloud Computing Synopsis and Recommendations", http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

[9] NIST SP 800-53, "Recommended Security Controls for Federal Information Systems and Organizations", http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[10] Federal Cloud Computing Strategy, http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

[11] Chief Information Officers Council, "Privacy Recommendations for Cloud Computing", http://www.cio.gov/Documents/Privacy-Recommendations-Cloud-Computing-8-19-2010.docx

[12] Office of Management and Budget, Memorandum 07-16, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

[13] NIST SP 800-144, "Guidelines on Security and Privacy Issues in Public Cloud Computing", http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

[14] NIST Cloud Computing Use Cases, http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/UseCaseCopyFromCloud

[15] Gartner, "Gartner Says Cloud Consumers Need Brokerages to Unlock the Potential of Cloud Services", http://www.gartner.com/it/page.jsp?id=1064712.

[16] IETF internet-draft, "Cloud Reference Framework", http://tools.ietf.org/html/draft-khasnabish-cloud-reference-framework-00

[17] IBM, "Cloud Computing Reference Architecture v2.0", http://www.opengroup.org/cloudcomputing/doc.tpl?CALLER=documents.tpl&dcat=15&gdid=23840

[18] GSA, "Cloud Computing Initiative Vision and Strategy Document (DRAFT)", http://info.apps.gov/sites/default/files/Cloud_Computing_Strategy_0.ppt

[19] Cloud Taxonomy, http://cloudtaxonomy.opencrowd.com/

[20] OASIS, the charter for the OASIS Privacy Management Reference Model Technical Committee, http://www.oasis-open.org/committees/pmrm/charter.php

[21] Open Security Architecture (OSA), "Cloud Computing Patterns", http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing

[22] Juniper Networks, "Cloud-ready Data Center Reference Architecture", www.juniper.net/us/en/local/pdf/reference-architectures/8030001-en.pdf

[23] Federal Information Security Management Act of 2002 (FISMA), http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

[24] NIST IR-7756, DRAFT "CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture", http://csrc.nist.gov/publications/drafts/nistir-7756/Draft-nistir-7756_feb2011.pdf .