A Review of PACS on Cloud for Archiving Secure Medical Images

Ricardo Ferraro de Souza, Networks and Management Laboratory, Federal University of Santa Catarina, Florianópolis, Santa Catarina, Brazil

Carlos Becker Westphall, Networks and Management Laboratory, Federal University of Santa Catarina, Florianópolis, Santa Catarina, Brazil

Daniel Ricardo dos Santos, Networks and Management Laboratory, Federal University of Santa Catarina, Florianópolis, Santa Catarina, Brazil

Carla Merkle Westphall, Networks and Management Laboratory, Federal University of Santa Catarina, Florianópolis, Santa Catarina, Brazil

ABSTRACT

Clinics and Hospitals are acquiring increasingly technological resources that assist in a quicker and more accurate diagnosis, in order to make it more dynamic and effective. This is causing health entities seek more modern equipment and advanced technological resources. The exams come to doctors with information processed in many different software and hardware. With the large number of information contained in exam increases the size and number of images present in the patient exam. Over time the volume of images grows exponentially, saturated retention capacity of information contained in Storage. The acquisition of new hardware to support accumulation of Terabytes size has been a major problem in these institutions. Thus this article demonstrates a scalable and less impactful on the environment, because it promotes energy savings, consumption of film and paper used in the printing of reports. PACS on Cloud proves efficient for archiving medical images, enabling access to the examination / patient report of any locality, being independent platform used for access.

Keywords: *Cloud Computing, Healthcare Systems, Open Nebula, Picture Archive and Communication System (PACS), Shibboleth*

1. INTRODUCTION

Information Technology has revolutionized all areas significantly improving business models. The medicine is being improved through innovative technology solutions in numerous equipment with diverse functions, equipment for radiological imaging, blood analysis equipment, equipment to assist in surgeries, equipment for patient control the distance. The need to search

for a more accurate diagnosis that allows an effective treatment for patients, causes exists a constant technological evolution.

Within the hospitals and clinics of medical imaging is common to find Picture Archive and Communication System (PACS). PACS is intended to manage the storage and display of medical images. Through clinicians workstations can access PACS system that makes manipulation of images independent of the physical location where the physician is located.

The medical diagnosis is performed by analyzing the images or reading report by medical experts, these are not always present in the location where the test was conducted, especially in cases where there is need for the involvement of a second physician in the diagnosis, or cases training of medical residents. The involvement of these doctors may occur via teleconference, remote report, or any other technology that enables the communication of a doctor who is not physically on site, provided he can gain access to take pictures and / or reports.

Images from X-rays are used in clinics and hospitals for medical diagnosis. The interrelationship between clinics, hospitals and radiology departments, increasingly depends on the accessibility of these images, from any location within or outside the physical care unit. (Junior, 2009).

Cloud Computing has been a central theme of several studies in information technology. The ability to share resources across clusters, virtualization and ease of access to information is increasingly attracting researchers of information technology. Companies are seeking this new paradigm as a way to lower costs by hiring more computer resources and not acquiring hardware and software for better scalability, accessibility, availability and disaster recovery.

However, there is concern about the privacy of data, since such data are outside the domain of the client. That is, on the one hand we have the advantages of the services available, but, on the other hand, there is concern about security. For these services to be effectively enjoyed by organizations is necessary to provide access control. (Leandro, 2012).

Leandro (2012), the success of cloud computing depends on the evolution of the customer mechanisms of Identity and Access Management (IAM) to service providers. IAM systems need to be protected by federations, which are groups of organizations that establish trust among themselves to cooperate safely in business. Identities used in this context are called “federated identity”. The user can be authenticated in an organization and can use the services of another organization of the federation without the need to repeat the process of authentication (Single Sign-On). Some technologies implement federated identity, such as the SAML (Security Assertion Markup Language) and Shibboleth system.

This article is organized as follows: section 2 presents an approach to workflow exams and problems encountered by hospitals and clinics citing some concepts of cloud computing and concludes by proposing a solution cloud PACS; section 3 presents the expected results; section 4 presents some final comments of the article.

2. BACKGROUND

Patient’s medical records, consultations, laboratory and medical reports, medical imaging and drugs are some of the items of patient’s medical history, which becomes increasingly complex, containing important data growing exponentially. This history is the total care of the patient, which in addition to health care and other chores need to keep in a safe place all of this information. A growing number of cases that patients undergoing the query without the reports of examinations and other necessary documents, hindering and delaying an accurate diagnosis and effective.

Every day patients are treated at health centers, pharmacies and emergency rooms of hospitals in emergencies, requiring surgical intervention, or any other clinical procedure, these procedures require attention and historical conditions of the patient, which is not always this information comes the doctor’s hands.

Doctors in hospitals and clinics require a resource that enables access to information and the history of each patient, considering that in public service is a common patient change several times during a medical diagnosis or treatment, so many important data as well as diagnostics, tests, and prescriptions made by each doctor are not archived. This situation can lead to duplication of tests and requests for prescriptions drugs because patients often, perhaps naive, do not know the name of the medication they are taking or what the purpose, an attitude that generates increased consumption of drugs and diagnostic features, which could be minimized if all professionals, to provide customer service, have access to their health profile and historical diagnostics and treatments. Thus, any examination, consultation, appraisal, medicine, etc., the patient has in his historical physicians, pharmacists, biochemists, and other professionals could access.

In the case of imaging diagnostic, Ultrasound, MRI, CT, X-Ray, among others, the patient takes the previous reports for the physician to use as a reference in the current diagnosis. Often these reports are not received by the hospital or have a large digitized historical containing numerous scans there be inserted in the local server, this complicates the fundamental access medical information, delaying the clinical procedure.

Many doctors serve in various clinics or hospitals, or both, and patients with multiple locations, often in other cities and often need to be watching the exams giving support to all patients. In urgent cases, the patient needs an immediate procedure; the distance can influence the duration of the report and decision-making of the physician. To meet this need, clinics and hospitals invest large amounts in communications infrastructure, processing and storage of these exams.

The need for investment in processing and data storage this growing almost unbearable for most hospitals and clinics do not have many resources for investment in modern equipment, infrastructure and information technology. A store image of medical tests has become a serious problem. Exams mean a greater number of complex images are being stored, requiring greater processing capacity and infrastructure necessary for the establishment providing the services.

The need for certification of quality in hospitals and clinics has increased the need to meet the requirements of certification bodies. Information stored electronically and easily accessible need not be printed, thus preventing the generation of waste (films, papers, cartridges) and environmental pollutants is a requirement that must be met by companies who want some ISO or achieve the millennium development goals stipulated UN, among which is quality of life and respect for the environment, related to environmental preservation (Millennium Goals, 2000).

A green computing is to seamlessly integrate management of computing devices and environmental for control mechanisms to provide quality of service, robustness, and energy efficiency. The challenge in green cloud computing is to minimize resource usage and still satisfy quality of service requirements and robustness (Werner, 2012).

With the use of cloud computing, we managed to consolidate the number of servers using virtualization techniques. The immediate results were very positive: reduction of rack space utilization; lower heat emission due to the reduction in server utilization, with consequent optimization of the cooling infrastructure (Werner, 2012).

2.1. System Overview

The cloud computing approach enables the growth of processing and storage infrastructure for hospitals and clinics without causing much impact. Internet access and computing devices are available in any place or area, creating new opportunities to share and use online resources. A number of features unexplainable and Internet

services like e-mail and storage are used daily as a kind of commodity. Patients are continuously monitored undisturbed during your daily activities (Berndt, 2012).

With sensors connected to medical equipment that are interconnected in order to exchange information, data become available in the "cloud", where they can be processed by an intelligent and / or distributed to medical staff for review (Rolim, 2010).

The idea is to use as a model for cloud applications are delivered as services over the Internet. How the service works on demand, graphs and usage reports can be generated to justify the amounts to be paid by customers.

Cloud services are built in such a way that if a machine fails, the system readjusts, in order to prevent the service to crash or that the contractors know that there was some kind of problem.

In 2011, Brown at the National Institute of Standards and Technology (NIST) has defined cloud computing as "a model for convenient access, on demand and in any location, a network of shared computing resources (e.g., networks, servers, storage, applications and services) that can be readily used and released with minimal management effort or interaction with the service provider."

You could say that cloud computing is the result of the union of computational paradigms such as virtualization, service level agreement, grid computing, aimed at providing on-demand service based business models of utility computing (Chaves, 2010).

Brown (2011), cloud computing can be classified into three models:

- **Software as a Service (SaaS):** restricts the use of client software, without being able to have control over the infrastructure. It can be accessed through a web browser or directly accessing the interface of a program;
- **Platform as a Service (PaaS):** the client has control over the deployed applications and settings to the environment hosting applications in the cloud;
- **Infrastructure as a Service (IaaS):** the customer can deploy and run arbitrary software, has control over operating systems, storage and deployed applications.

In 2010, Chaves said that cloud can be implemented in five ways and security policy depends on the business process, the type of information and level of desired vision:

- **Private Cloud:** Administered by the company itself or by third parties, this cloud is accessed only by an organization;
- **Public Cloud:** Available to the general public;
- **Community Cloud:** shared by companies with interests in common;
- **Hybrid Cloud:** composition between two or more implementations of clouds.

2.2. Cloud PACS

A Cloud PACS solution must grant access to the file server from any place or platform. A traditional PACS server consists of the following components: DICOM repository system and database. The object repository calls an infrastructure with storage capacity to support all DICOM exams. The database module supports the DICOM Information Model, which contains metadata information related to patients, the series of examinations and images. When one receives PACS exams modalities, it stores the images in DICOM repository and updates the database with elements drawn from examination.

Through PACS cloud is expected that the patient can perform imaging exam anywhere in the world and receive a more specific medical diagnosis and quality. The patient no longer needs to take the clinical history when seeking a health professional.

For doctors, the PACS cloud allows access to historical images and report the selection of "key image", which by definition comes down to images that have a supposed variation in normal patterns, teaching files referred to files learning that emphasizes putting medical examination

and their opinion on this case history is available so that other doctors can use it as a parameter or continue researching the subject.

The information becomes available in the cloud, where it can be processed by expert systems and / or distributed to medical staff for analysis. (Rolim, 2010).

Figure 1 illustrates the workflow of a hospital through a connection of Virtual Private Network (VPN) sends images to the cloud, so that doctors can access the exam. Thus, access the cloud is performed via a workstation directly to the hospital or anywhere else over the Internet as an external user, passing through a firewall.

Outside the hospital environment or clinical doctors and patients can access the information from the tests that are in the cloud. The services of the cloud user are authenticated using user's privacy policies, providing minimal information to the SP (Leandro, 2012).

Digital identity is the "representation of an entity (or group of entities) in the form of one or more elements of information (attributes) that enable the entity to be recognized only within a context" (Leandro, 2012).

Identity Management (IdM) is a set of functions and capabilities, such as administration, management and maintenance, discovery, information exchange, policy enforcement and authentication, used to ensure identity information, thus assuring security. An identity management system (IMS) provides tools for managing individual identities in a digital environment (Leandro, 2012).

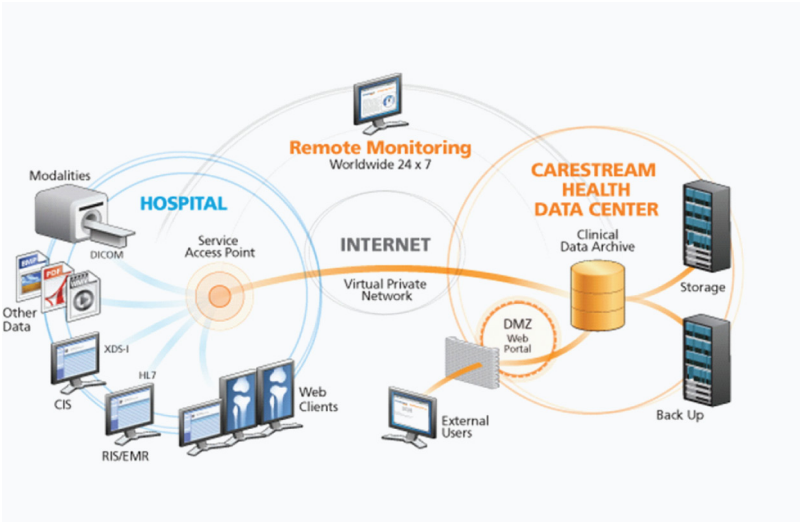
Some specialized features for IMS includes a Single Sign-On (SSO), where a user does not need to be signed on several times to call various applications, and can reuse the authenticated status of a previous application in the same session (Leandro, 2012).

An IMS consists of protocols and software components that address the identities of individuals throughout the life cycle of their identities. It involves three main types of entity: the user, the Identity Provider (IdP) and Service Provider (SP). IdPs are responsible for issuing and managing user identities and issue credentials. SPs (also known as relying parties) are entities that provide services to users based on their identities (attributes) (Leandro, 2012).

Functions of Identity Management Systems: Following are the main functions of an IMS:

- **Provisioning:** the practice of provisioning of identities within an orga-

Figure 1. Scope cloud PACS [CarestreamHealth, 2010]



nization addresses the provisioning and deprovisioning of several types of user accounts (e.g. end user, the application administrator, IT administrator, supervisor, developer, etc.) (Leandro, 2012);

- **Authentication:** is the process of ensuring that the individual is who he claims to be, and is identified through various mechanisms, such as login, password, biometrics, token, etc (Leandro, 2012);
- **Authorization:** a common need in security is to provide different access levels (e.g. deny/allow) for different parts or operations within a computing system. This need is called authorization (Leandro, 2012);
- **Federation:** it is a group of organizations or SPs that establish a circle of trust that allows the sharing of information of user identities to each other (Leandro, 2012).

B. Shibboleth:

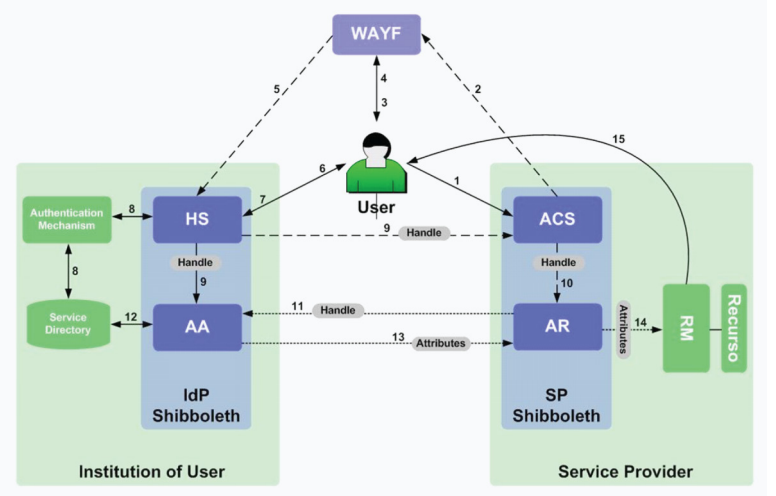
The OASIS SAML standard defines an XML-based framework for describing and exchanging security information between on-line business partners. This security information is expressed in the form of portable SAML assertions that applications working across security domain boundaries can trust. The OASIS SAML standard defines precise syntax and rules for requesting, creating, communicating, and using these SAML assertions (Leandro, 2012).

The Shibboleth is an authentication and authorization infrastructure based on SAML that uses the concept of federated identity. With it you can create a safe structure that simplifies the management of identities and provides the user with a SSO for different organizations belonging to the same federation, and who share their identity information in order to do so. The Shibboleth system is divided into two entities: the IdP and SP (Figure 2) (Leandro, 2012).

Leandro (2012), the IdP is the element responsible for authenticating users. It maintains and controls their credentials and attributes, disseminating this information to requests from entrusted organizations. It is composed of four components:

Handle Service (HS): authenticates users along with the authentication mechanism and creates a handle token (the SAML assertion that carries the credentials) to the

Figure 2. User authentication [Leandro, 2012]



user. Allows an organization to choose the authentication mechanism (Leandro, 2012);

2. **Attribute Authority (AA):** AA handles requests for SP attributes, applying privacy policies on the release of these attributes (Attribute Release Policies - ARP). Allows the user to specify who can access them. Allows the organization to decide which directory service is used (Leandro, 2012);
3. **Directory Service:** (external to Shibboleth) local storage of user attributes (Leandro, 2012);
4. **Authentication Mechanism:** (external to Shibboleth) allows users to authenticate with the central service with only a login/password pair (Leandro, 2012).

Leandro (2012), the SP Shibboleth is where the resources are stored, that are accessed by the user. It enforces access control on resources based on information sent by the IdP. A single SP may be composed of several applications, but will still be treated as a single entity by an IdP. It has three main components:

1. **Assertion Consumer Service (ACS):** responsible for receiving messages (SAML) to establish a secure environment (Leandro, 2012);
2. **Attribute Requester (AR):** responsible for obtaining and passing user attributes to RM (Leandro, 2012);
3. **Resource Manager (RM):** intercepts requests for resources and makes decisions to control access based on user attributes (Leandro, 2012).

The WAYF ("Where Are You From", also called the Discovery Service) is an optional feature on the Shibboleth system, responsible for allowing an association between a user and organization. When trying to access a resource, the user is forwarded to an interface that asks you to choose the institution to which it belongs. After choosing the institution, the user is redirected to start the authentication process. The WAYF service can be distributed as part of a SP or as part of the third code operated by a federation. In cases where it is used with SPs offering resources for registered users in several IdPs it becomes quite useful. The flow of operation of Shibboleth is represented in Figure 2 (Leandro, 2012).

In Step 1, the user navigates to the SP to access a protected resource. In Steps 2 and 3, Shibboleth redirects the user to the WAYF page, where he should inform his IdP. In Step 4, the user enters his IdP, and Step 5 redirects the user to the site, which is the component HS of the IdP. In Steps 6 and 7, the user enters his authentication data and in Step 8 the HS authenticate the user. The HS creates a handle to identify the user and sends it also to the AA. Step 9 sends that user authentication handle to AA and to ACS. The handle is checked by the ACS and transferred to the AR, and in Step 10 a session is established. In Step 11 the AR uses the handle to request user attributes to the IdP. Step 12 checks whether the IdP can release the attributes and in Step 13 the AA responds with the attribute values. In Step 14 the SP receives the attributes and passes them to the RM, which loads the resource in Step 15 to present to the user (Leandro, 2012).

2.3. Implementation

Using a cloud community concept this work presents the use of PACS cloud in order to organize the filing of exams from different sites into a centralized repository, reducing investments in storage infrastructure and processing by hospitals or clinics, for future readings or even in future diagnosis of any health institution. The use of PACS cloud contributes to reduction of printing images on film roles or reducing the emission of waste and garbage as a way to encourage environmental preservation.

The test is performed in a hospital or clinic and transferred to the local server, then to cloud or cloud to directly. Through a VPN between the hospital and clinical examination is transferred ensuring information security. The examination being on cloud any doctor who has access to

it can view it along with the entire history of the patient regardless of the physical location where the test was conducted. Access to this data is location-independent and platform used.

A community cloud is implemented with Open Nebula. Open Nebula is the open source toolkit for developing Cloud IaaS environments, offering many functions that facilitate the management of virtualized infrastructures. Provides interfaces compatible with EC2, OGF OCCI and interfaces vClouds. It also has features for integration, management, scalability, security and accounting. We highlight the standardization, interoperability and portability, providing cloud users and administrators the ability to choose between interfaces and hypervisors (XEN, KVM and VMware ESX) (Vitti, 2012).

The doctor's cloud access will be accomplished through a security policy for user privacy. This policy will provide minimal information to the physician SP access images of examinations as well as giving the award.

In 2010, Cordeiro said that architecture of Open Nebula was designed to conform to any kind of integration with more hypervisors and environments as possible. The physical infrastructure adopts the casts of classical architecture with the cluster front-end arrow and the nodes where the Virtual Machines (VM) is performed. There is a physical network that joins the cluster nodes with the front-end. The front-end executes the main processes while the Open Nebula cluster nodes are enabled by the hypervisor that provide the necessary resources to VMs.

Cordeiro (2010), Open Nebula was implemented in three layers: Tools, Core and Drivers. The tool layer contains modules that provide functionality for administrators and customers. In this layer implemented the Scheduler module, which is responsible for selecting and positioning the VM. The second layer is the core that is required to deal with customer requests and control features. Its main component is the Request Manager, which handles the requests from customers via XML-RPC interface. Stomayor (2009), the core is also responsible for controlling the lifecycle of VM. Modules called drivers to support different platforms form the third layer. These drivers run in different processes communicate with the kernel through simple text message.

3. EXPECTED RESULTS

The cloud community to be implemented with Open Nebula will provide the necessary infrastructure to meet the expectations of storage and processing on a large scale. This cloud will bring many benefits for imaging services using the PACS.

A cloud PACS deploying in hospitals and clinics will benefit these institutions and especially the patients. These health service institutions will have greater storage capacity and processing, decline in infrastructure spending, reduce expenses with specialist physician opening the possibility of contracting with fees paid by report and not per hour exam through access to any place or platform, not requiring the presence of the most professional on-site physical work.

The patients and users of health services will have greater flexibility in medical care and diagnosis and treatment. Besides the reliability and safety generated in providing the service, the health history of the patient may be accessed at any hospital or clinic where he is met by preventing important information or examinations are no longer reported to the attending physician that patient. This fact also brings greater convenience and confidence to the patient, because not to worry about storing prescription medications and old exams to present at future medical appointments, especially when dealing with elderly patients, where the difficulty of conducting these materials is higher.

This practice comes from meeting with prevention measures to the environment where the disposal of some wastes will no longer be required resulting in decreased use of X-ray films, CT, MRI, Mammography and the consumption of too much paper and ink printing.

4. CONCLUSION

The way it is implemented PACS in hospitals and clinics are becoming a serious problem, the need for this growing investment and lower revenue. More complex tests require more processing and more storage capacity, requiring an infrastructure better designed in order to provide differentiated services and quality.

The use of cloud PACS enables the centralization of IT service business, saving on labor, services, processing and storage infrastructure beyond the maintenance of equipment and systems.

The adoption of secure IdM in a cloud environment addresses the issues of identity provisioning, authentication, authorization and federation. The use of federations in IdM plays a vital role in enabling organizations to authenticate their users cloud services using any chosen IdP (Leandro, 2012).

Shibboleth was very flexible with regards to its use in a cloud environment, allowing a service to be provided reliably and securely. In addition, Shibboleth is based on SAML, which means it is compatible with international standards, thus ensuring interoperability (Leandro, 2012).

The implementation of the cloud community for using PACS as service aims to organize the filing of exams from different locations into a centralized repository decreasing investments in storage infrastructure and processing by hospitals or clinics. In the cloud physician and patient can view it on any device that has access to it.

REFERENCES

Berndt, R.-D., Takenga, M. C., Kuehn, P. P., Sommer, G., & Berndt, S. (2012). SaaS-platform for mobile health applications. In *Proceedings of the Ninth International Multi-Conference on Systems, Signals and Devices*.

Brown, E. (2011). *Published final definition of cloud computing*. Retrieved from http://www.inovacaotecnologica.com.br/noticias/noticia.php?artigo=definicao-computacao-em-nuvem&id=010150111128

CareStreamHealth. (2010). Retrieved from http://www.carestream.com/ehealthdisasterrecovery-testimonial-m1-889.pdf

Chaves, S., Uriarte, R., & Westphall, C. (2012). Toward an architecture for monitoring private clouds. *IEEE Communications Magazine*, 130–137.

Cordeiro, T., Damalio, D., Pereira, N., Endo, P., Palhares, A., Gonçalves, G., Sadok D., Kelner, J., Melander, B., Souza, V., & Mangs, J.-E. (2010). Open source cloud computing platforms. In *Proceedings of the Ninth International Conference on Grid and Cloud Computing*.

Junior, E. M. B. (2009). *Teleradiology: Central remote diagnostic imaging digital integrated portal to a distributed medical information. Application of the public*. Sao Paulo, Brazil: Federal University of Sao Paulo.

Leandro, M. A. P., Nascimento, T. J., dos Santos, D. R., Westphall, C. M., & Westphall, C. B. (2012). Multi-tenancy authoriza-tion system with federated identity for cloud-based environments using Shibboleth. In *Proceedings of the Eleventh International Conference on Network.*

Melleniun Goals. (2000). Retrived from http://www.objetivosdomilenio.org.br

Rolim, C., Koch, F., Westphall, C., Werner, J., Fracalossi, A., & Salvador, G. (2010). A cloud computing solution for patient's data collection in health care institutions. IEEE Computer Society, 95-99.

Sotomayor, B., Montero, R. S., Llorente, I. M., & Foster, I. (2009). Virtual infrastructure management in private and hybrid clouds. *IEEE Internet Comput-ing*, *13*, 14–22. doi:10.1109/MIC.2009.119.

Vitti, P. (2012). *Integration PCMONS and OpenNebula for management and monitoring of private clouds. Undergraduate Final examination of Federal University of Santa Catarina*. Brazil: Florianopolis.

Werner, J., Geronimo, G., Westphall, C., Koch, F., Freitas, R., & Westphall, C. (2012). Environment, services and network management for green clouds. *Clei Electronic Journal*, *15*(2), 2.