Revista de Sistemas de Informação da FSMA
n. 8 (2011) pp. 8-21

SISTEMAS DE INFORMAÇÃO
http://www.fsma.edu.br/si/sistemas.html

TRILHA PRINCIPAL

Management and Security for Grid, Cloud and Cognitive Networks

Carlos B. Westphall, Carla M. Westphall, Fernando L. Koch, Carlos O. Rolim, Kleber M. Vieira, Alexandre Schulter, Shirlei A. Chaves, Jorge Werner, Rafael S. Mendes, Rafael B. Brinhosa, Guilherme A. Geronimo, and Rafael R. Freitas

***Abstract*— This paper presents a number of research initiatives related to innovative and cut-edge technologies for Cloud Computing. These are chiefly in the fields of (i) environment security, (ii) quality assurance, (iii) service composition, and (iv) system management. We present technologies for intrusion detection; a SLA perspective in security management; customer security concerns; a Cloud-based solution for eHealth; experimental assessment of routing for grid and cloud; simulator improvements to validate the green cloud computing approach, and; a framework to radio layer operation in cognitive networks.**

***Index Terms*—Management and Security, Cloud Computing Grid Computing, Cognitive Networks**

I. Introduction

CLOUD computing technology imposes novel challenges to service development and management. The inherent features of vastly distributed processing open environment, and multi-user/multi-functional solutions require innovative, cutting-edge system management technologies. In this paper, we present a number of research initiatives being conducted in our group related to these technologies, chiefly in the fields of (i) environment security, (ii) quality assurance, (iii) service composition, and (iv) system management.

Our group has a long record of research on environmental security. In [1] we challenged the methods for **Security of Input Validation** in current Cloud-based Web Services, and propose a framework for new method of input validation. In [2], we dispute the efficiency of current **Intrusion Detection Systems** and present a novel intrusion detection method. Moreover, we demonstrate how the proposed method overcomes the current limitations through the detection of the typical attacks on host computers and networks. In addition, we present a solution where audit data is collected from the middleware and two intrusion detection techniques are applied [3].

Our research in the field of quality assurance is exemplified by the description in [4], where we present our research on **Service Level Agreements for Security** (Sec-SLAs). In this paper, we make an overview on the subject and elaborate on the difficulties related to defining security metrics and monitoring mechanisms. We concluded by analyzing the applicability of Sec-SLA for Cloud Computing environment. Another paper in the same research topic, [5] investigates the **Security Concerns** in Cloud Computing.

In the field of service composition, in [6] we proposed a framework for **Cloud Computing eHealth**, creating an architecture for Cloud-based Sensor Networks designed to integrate existing medical equipments in health institutions. In this environment, the information is collected, processed and becomes available in the Cloud. It encompasses the notions of expert systems, which may require extensively processing for data analysis, and ubiquitous interfaces

In the field of system management, in [7] we address the problems of system management considering the **Routing Problem**. We conclude by presenting an experimental assessment of routing for grid and cloud.

In the same field, we propose an **Integrated Solution for Cloud Computing Management** based on organization model [8]. We intend to develop new mechanisms for Green Cloud computing, which aims at a processing infrastructure that combines flexibility, quality of services, and reduced energy utilization.

Finally, in [9] we introduced a **method to classify the Spectrum Band Occupation based on cognitive networks**. We present a list of functionalities that ensure information and operations need to upper layers perform interference avoidance, power allocation, sensing control, spectrum characterization, spectrum selection and reconfiguration. We underscored the radio configuration features that are relevant to achieve cognitive network goals.

This paper is structured in sections, where each section discusses a specific issue, explaining its context, showing our proposals to tackle with its main issues and concluding with some general remarks and specific work that must be done in the field. We close the paper with a specific conclusions section, in order to complete the mental picture for our reader.

II. Security Framework for Input Validation

A. Scope and Context

Input manipulation attacks, such as Cross Site Scripting (XSS), are becoming one of the most common attacks against Web Applications and Web Services security. Using firewalls and other security mechanisms is not effective against application-level attacks, thus new methods of system security are required.

In [1], we proposed a framework to securing applications against input manipulation attacks. The mechanism offers a reusable approach by the use of XML files and a XML Schema for security parameters specification.

The input manipulation attack typically occurs from the application interface and could be used to exploit the Application Server. It allows the attacker to access databases, files and system configurations. This kind of attack is generally well known. However, the widespread usage of Web Services is leading to inventive (and previously unknown) methods of input manipulation attacks [10].

We highlight that using SSL and firewalls is not effective against application-level attacks. Hence, the work referenced proposes a framework for securing applications against input manipulation attacks using a reusable approach.

B. Proposals and Solutions

Attacks to Web Applications and Web Services are common due to incorrect or non-input validation. The lack of thorough input validation could result in different kinds of attack, the most common of which are defined bellow:

- Cross Site Scripting (XSS): consists of executing scripts on Web pages through the exploration of not correctly validated fields or URL.
- SQL injection: consists of the execution of SQL commands through the manipulation of the URL variables or fields.
- Hidden field manipulation: manipulation of hidden fields in order to explore some vulnerability.
- Buffer Overflows: sending messages bigger than the maximum allowed in order to execute arbitrary commands.

The proposed framework has the primary objective of validating the user inputs before the Application starts to execute. It consists of a XML Schema, a XML file, a server mechanism for input validation and the front-end application, whose functions are the following:

- The XML Schema defines the valid XML specification for the framework;
- The XML file defines the valid inputs for the required Application fields;
- The server mechanism is called to validate the user inputs according to the XML specifications;
- The front-end application is represented by any application which uses the framework for validating inputs.

When the user sends a request for an Application, the Input Validation mechanism receives the Request and checks for any inconsistence according to the pre-defined XML Input Validation specification. If the inputs sent are valid, the request is passed to the Web Application, otherwise, the user receives an error response.

The framework can be used with already developed or new applications. When using the framework with already developed application, the developer must adapt the application methods for calling the mechanism to validate inputs after receiving them.

On the other hand, when using the framework with new applications, the developer can define the application methods calling the mechanism every time an input is received.

This framework has some important characteristics. It works in the server-side – which means that any input from the Client will be validated before being processed.

Some developers usually perform the input invalidation in the client-side, but this is not correct and secure because the validation can be bypassed.

Another important characteristic of the framework is that it uses a single validation mechanism for the entire system, allowing for many applications from the same server to use the same mechanism, fostering reuse and systems standardization.

The framework is also XML based, what simplifies the application maintenance: if any changes are necessary, the developer just needs to change the XML application file.

This proposed framework addresses the big problem of Input Validation. Using it, Web Applications and Web Services will be secured against the various types of input manipulation attacks.

C. Conclusions and Future Works

This work presents the following major contributions:

- An independent specification of Security for Input validation, through the use of a separated XML file;
- A very reliable framework for validating user inputs in the server side instead of in the client side, assuring that all inputs will be validated before processing;
- A reusable approach with the implementation of the Validator mechanism;
- An architecture that could be used for Web Applications or Web Services; and
- An experiment result that present how easy is to find Web Applications with Security flaws related to the lack of input validation.

This study could be extended with the implementation of a system for input attacks detection and response, for instance, blocking the attacker access to the Web Application.

III. Intrusion Detection for Computation Grids

A. Scope and Context

Current intrusion detection technology is limited in providing protection against the intrusions that may violate the

security of computational grids. We present the problem of grid intrusion detection, describe the requirements of a system to detect them, propose a grid intrusion detection method, and show how it overcomes the limitations by integrating the detection of the typical host computer and network attacks with the detection of grid-specific attacks and user behavior anomalies. This integration is evaluated with a case study that makes use of simulations and a prototype implementation.

Computational grids are emerging as tools to facilitate the secure sharing of resources in heterogeneous environments [11]. Security is one of the most challenging aspects of grid computing and Intrusion Detection Systems (IDS) have an important role in grid security management. IDSs are responsible for the detection of intrusions in information systems and the responses to them, usually alert notifications sent to the security managers.

Intrusions can be characterized as unauthorized use by external parties or abuse of the system by insiders. Typical host-based IDSs and network-based IDSs can be deployed in a grid environment to improve its security. However, they cannot properly detect grid intrusions. The detection of these intrusions poses new challenges and current intrusion detection technology is limited in providing protection against them. In [2] we describe a grid intrusion detection method that overcomes the limitations.

B. Proposals and Solutions

For intrusion detection in computational grids we recommend a method in which grid-based intrusion detection systems (GIDS) is a high-level component that utilizes functionality of lower-level Host-IDS (HIDS) and Network-IDS (NIDS) provided through inter-IDS communication. This makes possible the reuse of intrusion detection software already available, avoiding re-implementation of functionality.

GIDS integration with the lower level components is the method's core. In this method, to achieve the desired security level for the grid, HIDS and/or NIDS are installed at certain grid nodes and network domains and work integrated with GIDS sending relevant information for the detection of intrusions.

In order to achieve the maximum security level, each grid node and grid network domain must have a lower level IDS installed. In this case, all NIDS located in each grid network domain capture network audit data and look for protocol anomalies and attack trails existent in network packets.

In addition to that, each grid node has a HIDS installed that collects and examines host audit data to identify evidence left by attacks and resource usage anomalies caused by local users. GIDS uses the audit data shared by the lower-level IDSs to identify grid attacks and to compare the behavior of grid users with their previously built historical profiles. The grid security manager is alerted whenever an intrusion is detected by GIDS or an alert is (iii) sent by the lower-level IDSs.

The organization of HIDS and NIDS components is illustrative and the audit information they share with GIDS Agents is stored in Grid Information Databases. Every time a user accesses the grid, GIDS Schedulers consult the user profile stored in a database and, depending on the demanded computing power for audit data analysis, submit one or more Analyzer jobs to nodes with available computing resources. The jobs) exchange data with the databases in order to analyze user behavior and update the profiles. The Analyzers are also responsible for correlating the stored audit data to identify grid attacks.

To show how the GIDS example satisfies the coverage requirement, consider a scenario where it protects a grid where an intruder wants to penetrate and follows these steps:

(1) The intruder launches a buffer overflow attack against an operating system (OS) process running on a grid node. The attack is successful and he is then able to execute arbitrary code.

(2) Now with OS root privileges, he runs an exploit script and impersonates a user with grid privileges, gaining facilitated access to several nodes.

(3) Continuing the malicious activity, he uses several grid nodes to run a distributed application.

(4) The application launches a coordinated network denial-of-service (DoS) attack against an external target.

The first step characterizes a (d) host intrusion detectable by HIDS. Supposing it's not detected, the intruder proceeds to the second step, which characterizes a (c) grid attack and a consequent (a) unauthorized access, both detectable by GIDS. If not stopped at that point, the intruder gets to the third step, where GIDS compares his behavior with the historical profile of the user he impersonated to identify (b) misuse. If somehow GIDS fails to identify a behavior anomaly, in the fourth step NIDS is responsible to detect the (d) DoS attack trails. In conclusion, in this scenario the GIDS example covers (a), (b), (c), and (d) intrusions, satisfying the requirement of (x) coverage. The system example is designed to distribute the detection problem among its components in order to achieve (y) scalability and, since it benefits from the grid by consuming its computing resources, it achieves (z) grid compatibility.

C. Conclusions and Future Works

The purpose of this work is to describe an approach that overcomes the weaknesses of the available solutions to the grid intrusion detection problem. As discussed the current technology is limited in detecting all the kinds of attacks that may violate the security of a grid. Typical IDSs cannot properly identify grid-specific attacks and grid users misusing resources.

The available GIDS architectures also lack protection against grid attacks and typical computer host and network attacks. We listed basic requirements that need to be satisfied by a GIDS: coverage, scalability, and grid compatibility. Related works on the subject of grid intrusion detection describe solutions which try to achieve scalability and grid compatibility, but lack in achieving complete coverage protection against the possible grid intrusions.

We described a grid intrusion detection method in which

GIDS is a high-level component that works in an integrated manner with lower-level IDSs (NIDS and HIDS). Then, assuming that integrating the IDSs was feasible, we showed with an example that this method can be used to satisfy the basic GIDS requirements.

We presented mechanisms to integrate GIDS with lower-level IDSs. The use of standard protocols and formats was focused: IDMEF, IDXP, RUR, and syslog. The case study performed with a simulated grid environment to evaluate the mechanisms was described. It demonstrated that the integration of lower-level IDSs with a GIDS using IDMEF messaging is possible and useful to detect the grid intrusions, although a complete case study involving all the types of grid intrusions was not performed, since signature databases of grid-specific attacks have not been made available to the scientific community yet. Research topics to be considered for future work are the distributed GIDS architecture that was left as an idea, the impact that a grid-wide intrusion detection service has on a grid's performance, and grid-specific attacks, including languages and tools for their manipulation. Also, other requirements could be considered for GIDS, such as accuracy, fault tolerance, timeliness, and performance.

IV. Intrusion Detection for Grid and Cloud

A. *Scope and Context*

Providing security in a distributed system requires more than user authentication with passwords or digital certificates and confidentiality in data transmission. Rigorous control of the executed tasks is needed in order to prevent malicious users from breaking grid policies, to identify the use of stolen passwords, and, also, to make possible the rapid detection of known attacks. In this work, a solution for grid and cloud computing intrusion detection is presented in which audit data is collected from the middleware and two intrusion detection techniques are applied. Analysis for anomaly detection is performed to verify if user actions correspond to known behavior profiles and knowledge analysis is performed to verify security policy violations and known attack patterns. This approach was evaluated and its resulting performance in regards to false positives, false negatives, and computational cost are discussed.

Because of their distributed nature, cloud computing environments are a great target for intruders willing to explore possible vulnerabilities existent in the services provided by them and, consequently, by impersonating legitimate users, can use the abundant resources inappropriately. An additional security measure that can be of great value in such systems is the employment of Intrusion Detection Systems (IDS) to investigate configurations, logs, network traffic, and user actions to detect typical attack behavior.

An IDS must be distributed in order to work in a cloud computing environment. In this manner, each node is monitored by a part of the intrusion detection system and, when an attack occurs, an alert is sent to the other nodes in the environment. To achieve this distribution, we need compatibility with heterogeneous hosts, communication mechanisms, and permission control over the system maintenance and updates since these features are typical in cloud computing, the problem becomes simpler, as these features are supported by cloud computing middleware and our effort can be focused only on implementing intrusion detection as a grid service.

An attack against a cloud computing system can be silent for a network-based IDS, since node communication usually is encrypted, and invisible to a host-based IDS, since clod computing attacks not necessarily affect a node's OS or the user registry but in cloud computing middleware so we will focus in this part. In this way, traditional IDS cannot appropriately identify suspicious activities in a cloud computing.

The work described in [3] presents an IDS architecture for cloud computing environment called CCIDS – Could Computing Intrusion Detection System - which integrates low-level detection, such as network and host detection, to identify attacks in the environment.

B. *Proposals and Solutions*

Could computing is distributed computing in essence and hence we suggest that intrusion detection and its alert system for this environment should be distributed and cooperative. In our solution, each node is responsible for identifying and alerting the other nodes of local events that may represent security violations. These individual IDS will cooperatively participate in the cloud computing intrusion detection, sharing of information between the cloud computing intrusion detection service and the elements that realize its architecture. These elements are described below:

- Node is a grid entity which contains resources. These resources are accessed homogeneously through the grid middleware, which also is responsible for controlling access control policies and supporting a service-oriented environment;
- Service provides its functionality in the environment through the middleware, which facilitates, for instance, communication.
- Event auditor is the key piece in the system and is responsible for capturing data from various sources, such as the log system, service and node messages.
- IDS Service analyzes data captured by the auditor and applies detection techniques based on user behavior and knowledge of previous attacks. In the event of a detection, it uses the communication means provided by the middleware to send alerts to other nodes. Therefore, cloud computing attacks are detectable. The middleware has also the task of synchronizing the known attacks database and the user behavior database.
- Storage Service holds the data needed by the IDS Service to perform analysis. It is important for all nodes to have access to the same data and a grid environment is responsible for virtualizing the homogeneous environment in a transparent way so that this database is unique.

C. Conclusions and Future Works

In this work we have described a cloud computing intrusion detection system capable of identifying unknown attacks, such as malicious usage through behavior deviation, and known attacks, with the help of a rule database that defines typical attacks.

Our solution is an IDS service that captures audit data from a log and a communication system part of grid middleware increasing the level of security in each node, as well as the cloud computing.

Two techniques were applied to achieve a higher level of security, intensively monitoring for possible malicious actions. Behavior-based intrusion detection was done with a feed-forward artificial neural network to recognize patterns of user behavior and indicate abnormal activity.

The prototype implementing this solution was demonstrably accurate, with a low rate of false positives and false negatives. Knowledge-based detection was added to the solution to ease the identification of trails from already known attacks. These attacks are previously defined with a set of rules that we presented as a contribution to the field.

In order to perform the required analysis for intrusion detection, we described a system for capturing audit data from a log system and messages exchange between grid nodes. In contrast to previous related work, this information is retrieved from the middleware, instead of lower-level systems such as the operating systems or network. The architecture was evaluated for feasibility with a prototype. We found out the processing cost is low and the performance is satisfactory for a real-time implementation. The individual analysis performed in each node reduces the complexity and the volume of data in comparison to previous solutions where the audit data is concentrated in single points. Communication, synchronization, and homogenization of resources were concerns in this work, since cloud computing provides services with these features.

V. SLA in Security Management for Cloud Computing

A. Scope and Context

One of the network and services management problems is security, either in preventing attacks and using computational mechanisms to protect data and systems or in administrative matters, which involves not just what needs to be protected, but also what security service levels will be delivered. This work explores Service Level Agreements for Security or just Sec-SLAs. Is tried to provide an overview on the subject, the difficulties faced during the security metrics definition process and the Sec-SLA monitoring, as well as an analysis on the Sec-SLA role in new paradigms like cloud computing.

Control systems and data security are important in any computer system. This demand can be covered by creating new devices or techniques and by making some adjustments in traditional ways of storing and controlling systems and data. In this sense, this work studies **Security Service Level Agreements** or just Sec-SLAs not as a brand new technique, but as a new design for the traditional Service Level Agreements or SLAs. Instead of considering traditional service levels like network throughput or delay, for example, it considers just service levels related to security.

To meet these security services levels, a set of security metrics needs to be defined and monitored. Defining these metrics is not a trivial task, but great research effort is being done to facilitate the process.

Service level security requirements or demands include cryptography, data packet filtering, redundancy of hardware and software and so on.

After this conversion, we get the second task in an effective Sec-SLA: monitoring if the metrics agreed are being met. It was proposed an architecture for monitoring and controlling these agreements, called Sec-Mon. This work explores Service Level Agreements for Security or just Sec-SLAs. We try to provide an overview on the subject and the difficulties faced to define security metrics to be used in such contracts, as also to outline its important role in new scenarios, like cloud computing.

B. Proposals and Solutions

Changes occurred in the traditional distributed computing paradigm lead to the need of enforcements in the traditional SLAs. The more recent is the notion of “computing in the cloud”, whose popular designation is cloud computing.

There is no clear consensus on what exactly cloud computing is, but several authors outline the fact that it is a new distributed computing and business paradigm, that provides computing power, software and storage and even a distributed data center infrastructure on demand, delivered over the Internet. The key words in the previous definition are on demand. Services delivered in such conditions demand considerable effort in the process of defining security service levels.

The definition of security metrics, as well as its monitoring, has to be done also on demand. The negotiation of the SLA will have to be agile, in order to not affect the hiring of services, as one of the greatest appeals of cloud computing is to allow unexpected demands to be met more quickly.

The security problem in cloud computing raises many questions, especially from customers, who need to understand the risks associated when migrating services to the cloud, as well as to know what are the ways available to ensure that the security of such data will be maintained.

Several recent work in cloud computing cites the importance of negotiating SLAs. For instance, The Cloud Security Alliance [12], whose formal debut was made at RSA Conference 2009 releasing a white paper entitled Security Guidance for Critical Areas of Focus in Cloud Computing, points the fact that more consideration should be given to the content of the SLA, considering its ‘auditability’. In [13] is pointed that to become a viable alternative to the enterprise, cloud computing infrastructures need to provide stable service level for business process. It is also pointed that "in cloud

computing environments SLAs are typically provided for basic platform services (e.g., system uptime, network throughput) [13]."

Due to its nature, cloud computing has several types of uses, i.e., one might be computing in the cloud when creating a datasheet in Google Docs, as well as when hiring a server in a data center to any enterprise purpose. Some cloud computing categorization was done, trying to differentiate these use possibilities, according to the main objectives of use. The categories more indicated in cloud computing related work are the three following, reproduced in this section like the definition given in [14]

C. *Conclusions and Future Works*

A Sec-SLA is a formal negotiated document that defines in, specially, a quantitative way what service levels will be delivered from the provider to the customer. In other words, the Sec-SLA deals with the "what", not the "how". Nevertheless, by defining good security metrics the "how" could be better visualized.

Usually the IT team faces lots of options in technological solutions and having a clear and documented understanding of what are the security requirements certainly would help. One of the main advantages of a Sec-SLA, beyond the legal one, is the possibility of a better understanding of how security is being accomplished.

It was also possible to notice that many research is being done focusing on the security metric subject. Fortunately, security metrics are of great concern in more areas than network and services management and much of the effort done to improve their definition and measurability is useful in a Sec-SLA context.

Proposed architectures like Sec-Mon represent an important subsidy in the search for ways to monitoring and controlling the Sec-SLA. The Sec-Mon architecture is independent of a specific technology and even that in the moment of its construction was not considered the cloud computing paradigm, it could easily be adapted to provide means of being deployed in a cloud environment.

As final remarks, we point out that a research to pre-design security metrics according to the cloud computing category, aiming to help the need for dynamic negotiation of Sec-SLAs in the cloud is in place. It is a great challenge because the paradigm is still evolving, as well as the understanding of what are the security challenges that it brings.

VI. COSTUMER SECURITY IN CLOUD COMPUTING

A. *Scope and Context*

There is no consensus on the exact definition of cloud computing, but some characteristics are clearly repeated. It is a new distributed computing and business paradigm. It provides computing power, software and storage and even a distributed data center infrastructure on demand. In [4], we investigate the main security concerns faced by the customers that are trying to better understand or profit from this new paradigm, especially considering a public cloud and we conclude that data confidentiality, integrity and availability are the biggest ones.

Despite of the fact that industry big players like Google, Amazon, SalesForce, Microsoft and others have products and services under the umbrella of 'cloud computing', 'cloud ready' or other similar denomination, there is no consensus about what exactly cloud computing is. Below we list two definitions made by researchers:

"A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers [15]."

"A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [16]."

From these definitions, it is possible to notice that some characteristics are clearly repeated. It is a new paradigm, not just a distributed computing paradigm, but also a new business paradigm. It is intended to provide computing power, software and storage and even a distributed data center infrastructure on demand.

In order to make these characteristics viable, cloud computing makes use of existing technologies, such as virtualization, distributed computing, grid computing, utility computing and Internet. However, even those industry big players have products and services available as also a definition of what are the basic cloud computing underlying technologies, a customer intending to better understand and profit from this new paradigm faces several concerns, especially the ones related to security.

Considering the customer point of view, we have made an extensive research to obtain what are the main security problems pointed in the available literature for cloud computing security, aiming to list and discuss the more recurrent ones.

B. *Proposals and Solutions*

Many cloud computing security problems are still unclear. Being cloud computing such a recent computing paradigm, it is natural that many aspects remain uncovered whereas the paradigm itself is being more developed and understood.

According to [17], there are three main customers' concerns:

- Vulnerability to attack: critical business information and IT resources are outside the customers firewall.

- Standard security practices: customers want to be confident that such practices are being followed. Most of those practices require disclosure and inspection, which leads to another concern as a customer: will my data be in the same virtual hardware and network resources with other customers, being susceptible to disclosure in someone else's inspection?

- Being subject to state or national data-storage laws related to privacy or record keeping: European Union (EU), for example, has privacy regulations that do not permit some personal data to be transmitted outside the EU. In the cloud, data can be stored anywhere in the world; it is important to attend such regulations.

In June 2008, the Gartner Group released a report entitled "Assessing the Security Risks of Cloud Computing" [17]. According to this report, widely commented and cited on the Internet, before jumping into the cloud, the customer should know its unique security risks, considering specially seven security conditions during the process of choosing a cloud provider. These unique security risks are:

- Privileged user access: outsourcing means allowing outsourced services to bypass internal controls, including personnel controls. With this in mind, the customer has to obtain as more information as possible about how the possible future provider hires people and what kind of controls their accesses have.
- Regulatory Compliance: if the cloud computing provider is not subject of external audits and security certifications, the customer probably should not use its services for non trivial tasks. Customers have to always remember that, unless stated or agreed otherwise, they are responsible for their own data.
- Data location: when using the cloud, the customer probably will not know where their data will be stored. Thus, it is recommended checking if the provider will commit to store and process data in specific jurisdictions and if a contractual commitment on behalf of the customer will be made by the provider.
- Data segregation: customers should check what is done to separate different customers' provider data, due to the fact that, in a cloud, the environment is shared. Using cryptography, for example, is effective, but do not solve all the problems. It must be checked also if the cryptographic schemes are designed and tested by specialists, because cryptographic accidents are able to make data unusable.
- Recovery: the provider capacity of restoring the entire system and how long it would take should be checked by the customer. Any provider that does not replicate its data or infrastructure is prone to total failures.
- Investigative support: In order to have confidence that inappropriate or illegal activities will be possible to be investigated, the customer needs a formal commitment from the provider. This commitment should state which kind of investigation will be possible and also gives evidence that similar support was already done by the provider. Otherwise, the customer almost can be sure that such investigations will be impossible.
- Long-term viability: if happens that the cloud computing provider be acquired or goes broke, the customer needs to know if the data will still be available and in a format that will allow being imported to a substitute application.

Summarizing the Gartner's report, customers should demand transparency and avoid providers that do not offer clear information about security programs.

C. *Conclusions and Future Works*

Maybe the cloud will evolve and become the largest information system we ever saw, having all sort of data and dealing with all kind of information, all kind of sensitive information. Hence, much research work is in progress to provide security for cloud computing, especially regarding do data confidentiality, integrity and availability.

The general belief, including ours, is that the larger adoption of cloud computing relies on how secure it is and that security should be addressed since the very beginning. Given that cloud computing is a still evolving paradigm, some new security concerns may appear during the definition process, but the concerns highlighted in the present survey probably will not change.

There are, however, a lot of good research and work in progress aiming to mitigate or to solve the security issues and to turn the cloud computing horizon less cloudy. Among these researches are government initiatives, like the cloud security group from US National Institute of Standards and Technology (NIST) and industry initiatives, like the Cloud Computing Security Alliance. Having data confidentiality, integrity and availability a strong legal side, some legal organizations like Strafford Publications are organizing events to discuss the subject, like a Teleconference entitled "Cloud Computing: Managing the Legal Risks", showing that other areas beyond information technology are watching cloud computing growing adoption more closely. Such initiatives bring advantages for the customer that can have more qualified background when analyzing the available cloud computing solutions to migrate his services to a cloud.

VII. CLOUD COMPUTING FOR HEALTH CARE

A. *Scope and Context*

Existing processes for patients' vital data collection require a great deal of labor work to collect, input and analyze the information. These processes are usually slow and error-prone, introducing a latency that prevents real-time data accessibility. This scenario restrains the clinical diagnostics and monitoring capabilities. In [5] we propose a solution to automate this process by using "sensors" attached to existing medical equipments that are interconnected to exchange service. The proposal is based on the concepts of utility computing and wireless sensor networks. The information becomes available in the "cloud" from where it can be processed by expert systems and/or distributed to medical staff. The proof-of-concept design applies commodity computing integrated to legacy medical devices, ensuring cost-effectiveness and simple integration.

Telemedicine allows remote diagnoses and monitoring of patients. It guarantees agility, safety, and reliability in modern

health-care institutions. There are several challenges associated to automation in this sort of environment, viz: heterogeneity of devices, protocols, and programming interfaces; the requirement for flexible, impact-free deployment; the requirement for easy to configure, easy to manage, scalable and, if possible, self-adjusting systems, and others.

We focus on the problem of patients' vital data collection, distribution, and processing. We suggest that current solutions based on manual note taking are slow, time consuming, and labor resource intensive. Besides, it imposes an obstacle to real-time data access that curbs the ability of clinical diagnostics and monitoring.

We present a solution to automate this process from bedside data collection to information distribution and remote access by medical staff. Our solution is based on concepts of wireless sensor networks and utility computing. "Sensors" are attached to existing medical equipments that are inter-connected to exchange services; these are integrated to the institution's computing network infrastructure. The information becomes available in the "cloud", from where it can be processed by expert systems and/or distributed to medical staff for analysis. We argue that these technologies provide desirable features for automation in telemedicine environment.

B. Proposals and Solutions

Our proposal is a system to automate the process of collecting patient's vital data via a network of sensors connected to legacy medical devices, and; deliver this information to the medical center's "cloud" for storage, processing, and distribution.

At the patient's bedside, there are sensor nodes which are loaded with software to collects, encode, and transmit data through wireless communication channels to be stored. The Exchange Service acts like a broker between local and remote services. It is responsible to receive collect data from sensors and to dispatch it to appropriate storage service hosted on cloud. It also receives requests from content service to retrieve data from the Cloud Service, whose functionality is two folded: (1) it is responsible to provide services to store collected data; and (2) it provides a platform for development, testing and deployment of applications needed by medical staff. Mobile and stationary devices interacts with applications using Content Service. This service acts like a "door" where medical staff devices can access all available information.

There are several practical advantages in this implementation, such as:

- it provides always-on, real-time data collecting;
- it eliminates manual collecting work and possibility of typing errors; and
- it facilitated the deployment process, as wireless networking means no need for cabling or other physical setup.

The proposed architecture covers the several elements in current systems, such as:

- Sensors attached to legacy medical devices replace the necessity of (i) manual data gathering and (ii) data entering on medical system.
- Computer resources available in the cloud are responsible to (iii) organize, index, and make the data accessible, and; distribute the data to (iv) medical staff.

At this level of abstraction, there is no need to specify "what" elements are available in the cloud (logical design) or to care for performance and scalability (physical design). It suffices to say that the "cloud" provides the standard interfaces for application integration.

C. Conclusions and Future Works

In short, our solution delivers an integrated telemedicine service that automates the process from data collecting to information deliver as a computing utility. There are several practical advantages in this implementation, such as: it provides always-on, real-time data collecting; it eliminates manual collecting work and possibility of typing errors, and; it eases the deployment process, as wireless networking means no need for cabling or other physical setup.

From the software engineering perspective, the proposed design promotes re-usability through the use of a standard services implemented and deployed by using a Platform as a Service (PaaS). In addition, it leverages others health-care institutions to use services through a Software as a Service (SaaS) model without investments on hardware or software licenses.

Moreover, we suggest that this project contributes to scientific and social fields. On the scientific field, the project generates new knowledge and applications for utility computing, cloud computing, sensor networks and mobile computing. These areas are being extensively explored by the academic community and the developments from this project will address some of the outstanding questions. There are many lines of research involved in this development, such as: information systems, system modeling, networking, mobile service development, service management, computational security and quality of service (QoS).

In addition, there is a contribution to the social field, as the proposed service helps to improve the quality of medical assistance delivery, especially in needy communities. It is difficult to gather medical staff with varying expertise in a single place, and it is even more challenging to enable medical assistance to remote patients located in remote communities. In addition, expert medical staff has restricted time and cannot monitor patients or collect additional data from patients at bedside. Thus, the proposal presents an innovative solution that addresses problems of integration, such as medical staff from one institution being able to monitor patients located at another. It also helps with releasing support staff workload that can use of saved time to focus on assistance. Finally, due to its pragmatic approach the project results in a cost-effective solution to address the requirements for modernization of health-care system in developing countries.

As future works, we intend to validate the proposal in a real world setup to assess the benefits of the solution in large scale scenarios. In addition, we intent to implement several services

enhancements of security and management with interaction of thirty-party infrastructure service provider.

VIII. Routing for Grid and Cloud Computing

A. Scope and Context

Grid and Cloud computing technologies are being applied as an affordable method to cluster computational power together. These structures aim to support service applications by grouping devices and shared resources in one large computational unit. However, the management complexity grows proportionally to the number of resources being integrated. This work claims to address the problems of management, considering the routing problem in a particular context. An experimental assessment of routing for grid and cloud is presented. In addition, it introduces a proof-of-concept implementation and case study scenarios.

According to IBM, traditionally, networks and management systems are manually controlled processes which demand one or more human operators to manage all the computing systems aspects. In this environment, the operator is strongly integrated to the management process and his task is to execute low level system calls to solve imminent problems. Even though this kind of management, which keeps a human into the system, was appropriate in the past, it cannot cope with modern systems.

The need to connect many heterogeneous systems is one of the main necessities of grid and cloud computing, introducing new levels of complexity. Even though it is a complex environment, the configuration and management is done by humans. This characteristic makes this task slow and a subject of decision making problems. Even administrator errors can occur at this task. In order to avoid this problem a solution is needed in which the management does not need human intervention. Observing this scenario, a question emerges: How to manage efficiently and in an automated way a heterogeneous and complex environment, like grid or cloud?

In order to answer this question the work in [7] proposes an experimental assessment of routing for grid and cloud computing that supports autonomic computing paradigm. The system has self-management properties, and redefines the human operator's responsibilities, where their experience is used to define general objectives and polices to control the system instead of placing them in a decision making position.

B. Proposals and Solutions

The piece that allows for the system to be called autonomic is the autonomic manager. Through the monitoring of managed elements and their external environment, the autonomic manager is able to build and execute plans for implementation, based on the analysis of sent information. Therefore, the autonomic manager is responsible for ensuring self-management, achieved when all its sub-areas (self-configuration, self-regeneration, self-optimization and self-protection) are guaranteed.

For this purpose, this work suggests that the manager is composed of some components, responsible for monitoring the data sent by the managed elements and others elements of the autonomic grid, analyze them, plan actions according to their objectives and implement these actions, thus achieving a high degree of autonomy.

The number of mobile devices is constantly changing, which can result in big changes in the overall system. For the interconnection among the devices, it is essential to keep the routing table consistent. The Routing Table Management component has the goal of detecting routing inconsistencies, but it cannot directly manipulate the routing table. The latter is done by the grid's routing algorithm.

The system proposed here implements two routing algorithms: one is based on the direct interconnection with a neighbor node, and the other is based on the interconnection among all nodes.

In grids, every element has its own routing table that contains the destination (node name) and a metric (the distance until the next element in hops). On the first algorithm, each node connects to the neighbor node only. Thus, the route to the neighbor node becomes a default route (gateway) to the other elements in the grid. For example, when an element wants to request a service, it sends a request to the gateway, and the gateway is responsible for forwarding the request to the others nodes connected to it. This process is repeated until the destination receives the request.

The other algorithm is a little different. As an element joins the grid, all the other elements add a direct route to it (metric 1). This makes the whole grid to be seen as a complete graph. The propagation of the information about a node joining or leaving the grid is coordinated by this same algorithm in an autonomic way. When all the nodes discover the topology changes, we have reached the convergence.

To this point, this work described the theory upon which the proposed system was based, the architecture details, its components and interactions, and the routing algorithms. To test it, we have implemented it on Grid-M [18]. Among the main benefits of the Grid-M middleware are: it is open source, it is easy to deal with small devices, it has a friendly API and it is portable [18].

C. Conclusions and Future Works

In [7] we have proposed an experimental assessment of routing for grid and cloud computing. The convergence time of the algorithm based on the direct interconnection to the neighbor node is really small and almost constant. As expected, the response time of the algorithm based on the restrict connection to the neighbor node is longer than the other one. The big question to be answered was: How to make a heterogeneous environment and with huge complexity, like grid and cloud computing, not being managed manually, which is inefficient? The solution proposal is the creation of autonomic elements acting as intelligent agents, capable of feel the environment where they are and act the same according to pre-defined policies.

IX. Management for Green Cloud Computing

A. Scope and Context

Green cloud computing aims at a processing infrastructure that combines flexibility, quality of services, and reduced energy utilization. In order to achieve this objective, the management solution must regulate the internal settings to address the pressing issue of data center over-provisioning related to the need to match the peak demand. In this context, we propose an integrated solution for environment, services and network management based on organization model of autonomous agent components. This work introduces the system management model, analyses the system's behavior, describes the operation principles, and presents a case study scenario and some results. We extended CloudSim to simulate the organization model approach and implemented the migration and reallocation policies using this improved version to validate our management solution.

The goal of 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. The problem is summarized as follows. The load prediction models in traditional architectures and cloud computing environments are based on the analysis of historical data and demand increments from business models. This information makes it possible to pre-allocate resources. However, load prediction models are challenged (and frequently broken) when unexpected peaks of demand occur.

Approaches to dealing with the problems of load prediction models include the following: (i) allow for a margin of on-line resources, i.e., over-provision resources; (ii) to turn on idle resources; (iii) to temporarily use external resources on-demand (i.e., federated clouds), and others. Each of these approaches has its advantages and disadvantages.

In [8] we propose a solution based on integrated environment, services and network management that promotes: (i) equitable load distribution through techniques like virtual machines; (ii) predictive resource allocation models through historical load analysis and pro-active allocation methods; (iii) aggregate energy management of network devices; (iv) integrated control over the environmental support units, which represent the larger share of energy consumption.

The objectives are the following: (i) to provide flexibility of the system configuration that allows for the easy introduction of new elements in the managed environment and the configuration processing distribution among services; (ii) to provide a level of availability that keeps to higher standard SLA compliance rates and which contributes to system's stability and security; (iii) to reduce cost in both capital and operational costs (CAPEX and OPEX) to support the business predicates, and thus promote the acceptability of the proposed method; (iv) to provide sustainability by using methods to reduce energy utilization and carbon emission footprints.

B. Proposals and Solutions

To achieve our objectives we propose an organization theory model for integrated management of a green cloud computing environment. It works based on organization models that regulate the behavior of autonomous components (agents) that view the environmental elements, network devices (e.g. switches, cards and ports) and service providers (e.g. processing servers, load distribution services, task processors and temperature reduction services). For example, the management system is able to turn off unused network devices and servers, turning off the environmental support units. This is reactive to characteristics of the predicted system load. The controlling elements are able to coordinate between themselves aiming at a higher-level system's objective, e.g. to keep overall energy utilization and SLA compliance metrics.

Our research advances the state of the art as follows: (i) it introduces an organization theory model for integrated management of the green clouds based on the concepts of organization models, network management, and distributed computing; (ii) it analyses the network and system's behavior and operational principles; (iii) it validates the proposal demonstrating the system's added-value in a case study scenario; (iv) it improves a simulator (the CloudSim framework) to validate the green cloud computing management approach.

We propose techniques to automatically detect the creation of data centers. We modeled the system using Norms (NM), Beliefs (BL) and Plan Rules (PR), inferring that we would need (NM) to reduce energy consumption, reduce the costs of the cloud and maintain a minimalist structure, based on a (PR) minimum of SLA violations and reduction of changes in the environment, not forgetting parameter settings (BL) of time provisioning of virtual machines. Based on these definitions and responsibilities, the agents' sensors respond more appropriately to balance the environment. Let's consider three services (i.e. web service, backup, remote boot) running concurrently and whose charge distribution appears to be complementary. Their high peaks (i.e., variation of workload) happen at different times. Based on inferences from NM, BL and PR agents would monitor the system and determine actions dynamically. In this proposal the agents have two solutions to the adequacy of servers and virtual machines: at a time before the peak, migrate the virtual machine to a more robust server or turn it off. Thus the system would act more dynamically and autonomically, according to the predefined requirements. Our environment is simply all the variations of workload (input), allocating and distributing services (moving/relocating) to the reduced use of resources (system output), searching environmental sustainability.

C. Conclusions and Future Works

In [8] we proposed an organization theory model for resource management of Green Clouds and demonstrated that the proposed solution delivers both reliability and sustainability, contributing to our goals of optimizing energy utilization and reducing carbon emission.

Concepts related to cloud computing and green cloud computing were presented. We also described the simulator employed in the practical part of the experiments and detailed improvements undertaken on it to validate the green cloud computing approach. The simulator we used is called CloudSim and was developed at the University of Melbourne in Australia. The improvements we implemented relate to services-based interaction and policies for migration and relocation of virtual machines, which are based on system monitoring and control.

Tests were realized to prove the validity of the system by utilizing CloudSim simulator from the University of Melbourne in Australia. We have implemented improvements related to services-based interaction. We implemented migration policies and relocation of virtual machines by monitoring and controlling the system. There was a reduction in migration (45% on average considering a day of simulation) as well as the number of SLA violations, found by reducing the number of lost requests (7.34% on average considering a day of simulation). Moreover, the approach simplifies the management model, in which it is possible to manage resources (connecting / disconnecting machines) of each element, reducing energy consumption.

X. Radio Layer Operation in Cognitive Networks

A. Scope and Context

In [9], we present a schema to classify the signal sensed as well as to classify the spectrum band occupation according to signals sensed. We also present a list of functionalities that ensure information and operations need to upper layers perform interference avoidance, power allocation, sensing control, spectrum characterization, spectrum selection and reconfiguration. With this list, we highlight the radio configuration features that are relevant to achieve cognitive network goals. Finally, we evaluate the expressivity of proposed schema to hit the main cognitive network goals and we conclude that our propose is relevant to cognitive radio research once it define de minimum behavior and responsibilities to cognitive radio layer.

The increase in use of wireless networks led the USA Federal Communications Commission (FCC) to publish a report showing that problem of spectrum shortage is, in fact, a problem of spectrum using. So, an effort has been conducted in order to that unlicensed (secondary) users could use the spectrum already assigned to licensed (primary) users. In this way, concept of cognitive networks was created and a lot of other concepts have been suggested and consolidated around this concept. Cognitive networks address the problem of spectrum occupation without or with the minimum interference in the primary user (PU) communication and, in the same way, cognitive radio (CR) is defined formally as soon: ”A ’Cognitive Radio’ is a radio that can change its transmitter parameters based on interactions with the environment in which it operates”.

To reach this aim we must assure cognitive capability and re-configurability where the first one is the ability to sense the spectrum and identify spectrum holes or white spaces that are unused portions of spectrum as well as infer or cognize interference in PU transmissions. The second ability is re-configurability, which means the ability of CR allowing change in its operating parameters like channel, transmission power, sensing threshold and any other in order to assure connectivity and minimum PU interference. In this work, we consider spectrum band and channel as synonymous because of we do not need to consider specificities like modulations that work with more than one channel, yet which this framework includes the possibility of treating these modulations.

There are two types of spectrum awareness, passive and active. Besides this classification, some authors classify awareness according to response time and topology as slow or rapid and distributed or centralized, respectively. These concepts are important once we want to situate our proposal as a schema for active and rapid awareness, allowing centralized or distributed topology. In fact, it effectively senses the spectrum where the device is inserted, supplies a rapid classification of the signal sensed and can easily share its state (signal and channel rating) with other partner devices. Finally, we can say that our method is adequate to perform spectrum sensing, spectrum decision, spectrum sharing and spectrum mobility.

B. Proposals and Solutions

Spectrum sensing - to achieve it, the cognitive radio must be able to perform PU detection, sensing control and, in cooperative mode, cooperation. We can find these requirement in a more detailed form, where some important abilities are presented in order to achieve the best sensing state such as define the observation time, bandwidth awareness, establish a sensing threshold for the sensing method and signal-to-noise awareness. Even so, all related works present three PU detection methods: matched filter detection, energy detection and feature detection.

Spectrum management (or decision) - requires three main aspects to be successful [19]: spectrum characterization, spectrum selection and reconfiguration, where the first consists of information collection about the channel regarding one (or more) aspects. Spectrum selection is performed after spectrum characterization, where once channels properly classified, it is necessary to select the appropriated band according to quality of service (QoS) parameters, being a common QoS parameter the interference level over PU transmissions. However, other parameters where requirements like to maximize discovery opportunities and to minimize delay in locating an idle channel are presented, besides classical network requirements, to maximize throughput and to minimize delay. Finally, the last aspect of spectrum management is re-configurability, which carries the needs of channel selection, modulation selection, bandwidth setting, observation time setting, transmission time setting and power setting.

Spectrum sharing - stems from the need in preventing

multiple CR networks colliding in spectrum overlapping portion. According to [19], this concept is detailed and subdivided in intra-network spectrum sharing and inter-network spectrum sharing, where the first can be achieved through its own transmission process. However, for the second one, there is none infrastructure to perform spectrum sharing with other CR users. Nevertheless, the CR must have mechanisms to be able to: resource allocation, channel allocation, power allocation and smart spectrum access (random access, time slotted, hybrid). All these concepts are properly explained in [19]. For our work, the only necessary concept the reader must keep in mind is that of multiple CR sharing a spectrum range each other (and with the PU). Despite of there are not requirements at CR level, the sensing mode must be expressive enough to differ a PU transmission and a secondary user (SU) transmission.

Spectrum mobility - gives rise a new type of handoff in CR network [19], the so-called spectrum handoff, that means the transfer of connection to another unused spectrum band. This transfer occurs in three situations: PU detection, connection lost due to mobility of users involved in communication or spectrum band can not meet QoS requirements.

Thus, for this work we understand that the proposed framework must be able to offer the following features: PU detection; channel classification; channel selection / bandwidth setting; modulation selection; observation time setting; transmission time setting; power setting; establish a sensing threshold; signal-to-noise awareness; quality of detection awareness; and bandwidth awareness. Because these are the requirements needed to achieve the follow other requirements: sensing control; cooperation; spectrum characterization; spectrum selection; reconfiguration; intra-network spectrum sharing; inter-network spectrum sharing; and spectrum handoff.

C. Conclusions and Future Works

In this we reviewed the evolution of cognitive radios and networks as well as presented a framework composed by a schema for sensing signal and classify the spectrum, a set of relevant operations to cognitive decision making and a set of states to control the cognitive radio.

The set of operations defined by us are the main operations that CR must turn available for upper layers, allowing implementation of: interference avoidance, power allocation, sensing control, spectrum characterization, spectrum selection and reconfiguration.

Furthermore, the set of state presented is consistent to ensure the awareness need for upper layers invoke the operations available in cognitive radio.

Our approach benefits the cognitive network research by treating the behavior definition of an important piece in the cognitive networks: the cognitive radio. Also, with this definition we make a contribution to define the radio layer responsibilities. This is an important contribution since the search by a cross-layer architecture has hampered the distribution of responsibilities by the layers of cognitive networks.

For future works, we will focus our efforts on the research challenges to describes optimization of cooperative sensing as a need for improvement of the cognitive networks.

XI. CONCLUSIONS

In this paper we presented some of the major contributions our work group has offered in the last few years.

The work “A Security Framework for Input Validation” presents the following major contributions: An independent specification of Security for Input validation, through the use of a separated XML file; A very reliable framework validating the user- inputs in the server-side instead of in the client- side, assuring that all inputs will be validated before processing; A reusable approach with the implementation of the Validator mechanism; The proposed architecture could be used for Web Applications or Web Services; and An experiment result that present how easy is to find Web Applications with Security flaws related to the lack of input validation.

The work “Intrusion Detection for Computational Grids” described a grid intrusion detection method in which GIDS is a high-level component that works in an integrated manner with lower-level IDSs (NIDS and HIDS). Then, assuming that integrating the IDSs was feasible, we showed with an example that this method can be used to satisfy the basic GIDS requirements. We presented mechanisms to integrate GIDS with lower-level IDSs. The use of standard protocols and formats was focused. The case study performed with a simulated grid environment to evaluate the mechanisms was described. It demonstrated that the integration of lower-level IDSs with a GIDS using IDMEF messaging is possible and useful to detect the grid intrusions.

The work “Intrusion Detection for Grid and Cloud Computing” presents an IDS service that captures audit data from a log and a communication system part of grid middleware increasing the level of security in each node, as well as the cloud computing. Two techniques were applied to achieve a higher level of security, intensively monitoring for possible malicious actions. Behavior-based intrusion detection was done with a feed-forward artificial neural network to recognize patterns of user behavior and indicate abnormal activity. The prototype implementing this solution was demonstrably accurate, with a low rate of false positives and false negatives. Knowledge-based detection was added to the solution to ease the identification of trails from already known attacks. These attacks are previously defined with a set of rules that we presented as a contribution to the field. To perform the required analysis for intrusion detection, we described a system for capturing audit data from a log system and messages exchange between grid nodes.

The work “A SLA Perspective in Security Management for Cloud Computing” presents a Sec-SLA that is a formal negotiated document that defines in, specially, a quantitative way what service levels will be delivered from the provider to the customer. In other words, the Sec-SLA deals with the

"what", not the "how". However, by defining good security metrics the "how" could be better visualized. Usually the IT team faces lots of options in technological solutions and having a clear and documented understanding of what are the security requirements certainly would help. One of the main advantages of a Sec-SLA, beyond the legal one, is the possibility of a better understanding of how security is being accomplished.

The work "Customer Security Concerns in Cloud Computing" presents the larger adoption of cloud computing relies on how secure it is and that security should be addressed since the very beginning. Being cloud computing a still evolving paradigm, some new security concerns may appear during the definition process, but the concerns highlighted in the present survey probably will not change. There are, however, a lot of good research and work in progress aiming to mitigate or to solve the security issues and to turn the cloud computing horizon less cloudy. Among these researches are government initiatives, like the cloud security group from US National Institute of Standards and Technology (NIST) and industry initiatives, like the Cloud Computing Security Alliance. Having data confidentiality, integrity and availability a strong legal side, some legal organizations like Strafford Publications are organizing events to discuss the subject, like a Teleconference entitled "Cloud Computing: Managing the Legal Risks", showing that other areas beyond information technology are watching cloud computing growing adoption more closely. Such initiatives bring advantages for the customer that can have more qualified background when analyzing the available cloud computing solutions to migrate his services to a cloud.

The work "A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions" presents an integrated telemedicine service that automates the process from data collecting to information deliver as a computing utility. There are several practical advantages in this implementation, such as: it provides always-on, real-time data collecting; it eliminates manual collecting work and possibility of typing errors, and; it eases the deployment process, as wireless networking means no need for cabling or other physical setup.

The work "Experimental Assessment of Routing for Grid and Cloud" proposed an experimental assessment of routing for grid and cloud computing. The convergence time of the algorithm based on the direct interconnection to the neighbor node is really small and almost constant. As expected, the response time of the algorithm based on the restrict connection to the neighbor node is longer than the other one. The big question to be answered was: How to make a heterogeneous environment and with huge complexity, like grid and cloud computing, not being managed manually, which is inefficient? The solution proposal is the creation of autonomic elements acting as intelligent agents, capable of feel the environment where they are and act the same according to pre-defined policies.

The work "Simulator Improvements to Validate the Green Cloud Computing Approach" proposed an organization theory model for resource management of Green Clouds and demonstrated that the proposed solution delivers both reliability and sustainability, contributing to our goals of optimizing energy utilization and reducing carbon emission. Concepts related to cloud computing and green cloud computing were presented. We also described the simulator employed in the practical part of the experiments and detailed improvements undertaken on it to validate the green cloud computing approach. The simulator we used is called CloudSim and was developed at the University of Melbourne in Australia. The improvements we implemented relate to services-based interaction and policies for migration and relocation of virtual machines, which are based on system monitoring and control.

The work "A framework to Radio Layer Operation in Cognitive Networks" reviewed the evolution of cognitive radios and networks. It presented a framework composed by a schema for sensing signal and classify the spectrum, a set of relevant operations to cognitive decision making and a set of states to control the cognitive radio. Our approach benefits the cognitive network research by treating the behavior definition of an important piece in the cognitive networks: the cognitive radio. Also, with this definition we make a contribution to define the radio layer responsibilities. This is an important contribution since the search by a cross-layer architecture has hampered the distribution of responsibilities by the layers of cognitive networks.

REFERENCES

[1] R. B. Brinhosa, C. B. Westphall, C. M. Westphall, "A Security Framework for Input Validation," *in Second International Conference on Emerging Security Information, Systems and Technologies*. 2008.

[2] K. M. Vieira, A. Schulter, C. B. Westphall, C. M. Westphall, A. Sekkaki, "Intrusion Detection for Computational Grids," *in IFIP Second International Conference on New Technologies, Mobility and Security*. 2008.

[3] K. M. Vieira, A. Schulter, C. B. Westphall, C. M. Westphall, "Intrusion Detection for Grid and Cloud Computing," *in IT Professional Magazine*. 2010.

[4] S. A. Chaves, C. B. Westphall, F. R. Lamin, "A SLA Perspective in Security Management for Cloud Computing," *in Sixth International Conference on Networking and Services*. 2010.

[5] S. A. Chaves, C. B. Westphal, C. M. Westphall, G. A. Geronimo, "Customer Security Concerns in Cloud Computing," *in International Conference on Networking*. 2011.

[6] C. O. Rolim, F. L. Koch, C. B. Westphall, J. Werner, A. Fracalossi, G. S. Salvador, "A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions," *in Second International Conference on eHealth, Telemedicine, and Social Medicine*. 2010.

[7] D. O. Balen, C. B. Westphall, C. M. Westphall, "Experimental Assessment of Routing for Grid and Cloud," *in International Conference on Networking*. 2011.

[8] J. Werner, G. A. Geronimo, C. B. Westphall, F. L. Koch, R. R. Freitas, "Simulator Improvements to Validate the Green Cloud Computing Approach," *in Latin American Network Operations and Management Symposium*. 2011.

[9] R. S. Mendes, C. B. Westphall, E. R. Garcia, "A framework to Radio Layer Operation in Cognitive Networks," *in Sixth International Conference on Networking and Services*. 2010.

[10] W. D. Yu, D. Aravind, P, Supthaweesuk, "Software Vulnerability Analysis for Web Services Software Systems," *in 11th IEEE Symposium on Computers and Communications*. 2006.

[11] I. Foster, C. Kesselman, "The Grid 2: Blueprint for a New Computing Infrastructure, 2. ed.," *Morgan Kaufmann,* 2003.
[12] "Security guidance for critical areas of focus in cloud computing," *Cloud Security Alliance*, Tech. Rep. 2009.
[13] V. Stantchev, C. Schröpfer, "Negotiating and Enforcing QoS and SLAs in Grid and Cloud Computing," *in 4th International Conference on Advances in Grid and Pervasive Computing*. 2009.
[14] N. Leavitt, "Is Cloud Computing Really Ready for Prime Time?" *Computer*, vol. 42, no. 1, pp. 15-20, January 2009.
[15] R. Buyya, Y. Chee Shin, S. Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities", *In 10th IEEE Conference on High Performance Computing and Communications*. 2008.
[16] P. Mell, and T. Grance, "Cloud Computing Definition". *NIST*. 2009.
[17] J. Heiser, and M. Nicolett, "Assessing the Security Risks of Cloud Computing," *Gartner Group*. 2008.
[18] H. A. Franke, C. O. Rolim, C. B. Westphall, F. L. Koch, and D. O. Balen. Grid-M: Middleware to Integrate Mobile Devices, Sensors and Grid Computing," *in Third International Conference on Wireless and Mobile Comunications*. 2007.
[19] I. Akyildiz, W. Lee, K. Chowdhury, K. "CRAHNs: Cognitive Radio ad hoc Networks," *Ad Hoc Networks*, vol. 7, no. 5, pp. 810-836. 2009.

Carlos B. Westphall is a full professor in the Department of Informatics and Statistics at the Federal University of Santa Catarina, where he is the leader of the Networks and Management Laboratory. His research interests include network and service management, security, and cloud computing. He received his D.Sc. in computer science at Paul Sabatier University, France. He was the founder of LANOMS. In 2011 he was named an IARIA Fellow. He has served as Technical Program and/or Organizing Committee member (since 1994) of IFIP/IEEE IM, IEEE/IFIP NOMS, IEEE/IFIP DSOM, IEEE LANOMS, and IEEE APNOMS. He has been on the Board of Editors (since 1995) and Senior Technical Editor (since 2003) of the Journal of Network and Systems Management of Springer and an Editorial Board member (since 2004) of the Computer Networks Journal of Elsevier. He has also been an Associate Editor (since 2006) of the Journal of Communication and Information Systems of IEEE ComSoc/SBrT. Since 1993 he has been a member of IFIP TC6 Working Group 6.6 (Management of Networks and Distributed Systems), and since 2003 a member of the core team of the TeleManagementForum Universities Program (TMF UP). Since 2008 he has been Latin America International Academy, Research, and Industry Association (IARIA) Liaison Board Chair. He was a member (2004–2005 and 2006–2007) of the IEEE ComSoc Membership Programs Development Board. From May 2000 to May 2005 he acted as Secretary of the IEEE Committee on Network Operation and Management (CNOM). From May 2005 to May 2009 he acted as Vice- Chair of IEEE CNOM. He has been a member of IEEE CNOM since 1994.

Carla M. Westphall is a professor in the Department of Informatics and Statistics at the Federal University of Santa Catarina, Brazil. Her research interests include distributed security, identity management, and grid and cloud security. Westphall received her PhD in electrical engineering from the Federal University of Santa Catarina. Contact her at carlamw@ inf.ufsc.br.

Fernando L. Koch obtained his Ph.D. in Computer Sciences (2009) in the Department of Information and Computing Systems, Utrecht University, Netherlands. He has over 17 years of R&D in IT Industry, having been engaged in many Projects in the area of Mobile Computing with large telecomm accounts. He collaborates with several research groups providing mentoring to R&D projects in IT Innovation in the area of Cloud Computing, Distributed Computing, and System Management. His research interests include Mobile Services, Distributed Computing, and Artificial Intelligence.

Carlos O. Rolim is doing his PhD in Computer Science at Federal University of Rio Grande do Sul (2011). He has a master's degree in Computer Science from UFSC (2007). He is participating in the Group of Parallel and Distributed Processing (GPPD) at UFRGS / II, and is associate researcher of the Networks and Management Laboratory at UFSC. He has experience in Networks and Distributed Systems acting on the following topics: ubiquitous and pervasive computing, wireless networks, wireless sensor networks, grid computing and cloud computing.

Kleber M. Vieira is a team leader for a software development company in Brazil and is a member of the Networks and Management Laboratory at UFSC. His research interests include information systems, software engineering, distributed systems, and security. Vieira received his MSc in computer science from the Federal University of Santa Cataria. Contact him at kleber@ inf.ufsc.br.

Alexandre Schulter is an IT analyst for a Brazilian government company. Previously, he was a researcher and software developer at several laboratories in the Technological Centre at UFSC, Brazil. His research interests include information systems, component-based systems, software engineering, distributed systems, and security. Schulter received his MSc in computer science from UFSC. Contact him at schulter@ inf.ufsc.br.

Shirlei A. Chaves holds an M.Sc degree in computer science from the Federal University of Santa Catarina, Brazil. During her M.Sc. she worked at the Networks and Management Laboratory as a cloud computing researcher. She currently works as a systems analyst at E3C Technology, Brazil. Her industrial experience includes network management, Linux development and customization, project feasibility reports on system changes and integration, and close work with clients and developers to ensure technical compatibility. Her research interests include network and service management, and distributed and cloud computing.

Jorge Werner has received his Master in Computer Science from Federal University of Santa Catarina (2011) and graduated from the Estacio de Sa University of Santa Catarina (2007) as Computer Network Technology. Currently student of College of Technology in Telecommunications Systems IFSC Campus in San Jose and guiding the course of Post Graduate (lato sensu) IT Governance at Senac / SC.

Rafael S. Mendes has received his master degree in Computer Science at Federal University of Santa Catarina. He is working at ELETROSUL.

Rafael B. Brinhosa has received his Master in Computer Science and Bachelor of Information Systems from Federal University of Santa Catarina. Currently pursuing MBA in Strategic Management from UFPR. Certificate ISEB /ISTQB, ITIL-F, ISC (2) CSSLP and ISO/IEC 27002. OWASP and CSA Brazilian chapter member.

Guilheme A. Geronimo is doing his master degree in Computer Science at Federal University of Santa Catarina. He is currently leased to the Federal Public Employee Data Processing Center of UFSC.

Rafael R. Freitas has received his Bachelor in Computer Scince from Federal University of Santa Catarina.