Management and Security for Grid, Cloud and Cognitive Networks

Jean Paulo da Silveira
Alexandre Henrique
Leonardo Freitas

ADMINISTRATION AND MANAGEMENT OF COMPUTER NETWORKS - INE5619

Federal University of Santa Catarina

DECEMBER 28, 2012 - BRAZIL

INTRODUCTION

- Cloud computing poses new challenges for the development and management of their services.
- This paper presents a series of research being conducted for this technology. Especially in safety, environment, quality assurance, service composition and management system.

CONTENT

- Security framework for input validation;
- Intrusion detection for computation grids;
- Intrusion detection for grid and cloud;
- SLA in security management for cloud computing;
- Costumer security in cloud computing;
- Cloud computing for health care;
- Routing for grid and cloud computing;
- Management for green cloud computing;
- Radio layer operation in cognitive networks;
- Conclusion;

2 - SECURITY FRAMEWORK FOR INPUT VALIDATION

- Manipulation attacks entries are common in web applications and security.
- It is proposed to use an XML schema that contains the parameters for specifying security.
- The paper proposes a framework for applications mounting against ingress of manipulation attacks.

2 - SECURITY FRAMEWORK FOR INPUT VALIDATION

- Attacks from lack of input validation:
  - Not correct operation of validation fields or URL;
  - Running SQL to manipulate or URL fields;
  - Hidden field manipulation;
  - Sending messages larger than the maximum permitted to execute arbitrary commands.
- You should validate user input before application begins executing.

2 - SECURITY FRAMEWORK FOR INPUT VALIDATION

- Mechanism input validation and application:
  - The XML Schema specification defines the valid XML for table;
  - The XML file defines the valid entries;
  - The mechanism is called server to validate the user according to the XML specification;
  - Verification takes place according to any inconsistency XML input;
  - If access is validated is released, otherwise displays the error message.

2 - SECURITY FRAMEWORK FOR INPUT VALIDATION

- Advantages and conclusions:
  - It works on the server side - meaning that any customer input is validated before being processed;
  - Uses a single validation mechanism for the entire system;
  - Promotes reuse and standardization of systems;
  - An independent security specification for input validation.
  - Architecture that can be used for Web applications or Web services.

3 - INTRUSION DETECTION FOR COMPUTATION GRIDS

- The intrusion detection technology is current limited.
- Grid computing is emerging as tools to facilitate the secure sharing of heterogeneous resources environments.
- Intrusion detection systems (IDS) have an important role in the management of security of network.
- IDSs can not properly detect network intrusion.

3 - INTRUSION DETECTION FOR COMPUTATION GRIDS

- Proposals and Solutions:
  - Use of a method which utilizes high-level low-level functionality of the IDS through communication by reusing the already available software intrusion avoiding duplicate functionality;
  - Are installed in specific network nodes and network domains and work integrated with intrusion detection systems;
  - In order to achieve the maximum level of security, each grid node and grid network domain should have a lower level IDS installed.
  - Audits seeking anomalies or attacks on the network, where each node is collected and analyzed the data identifying the evidence of attack.

3 - INTRUSION DETECTION FOR COMPUTATION GRIDS

- Network security manager is alerted whenever an intrusion is detected by grid intrusion detection systems or an alert is sent by the lower-level IDSs.
- Agents are stored in databases, where they exchange data with the database in order to analyze user behavior and update the profiles.

3 - INTRUSION DETECTION FOR COMPUTATION GRIDS

- *Conclusions:*
  - The objective of this paper is to describe the shortcomings of available solutions for grid intrusion detection problem, where technology is limited.
  - Was listed basic requirements that must be met by a grid intrusion detection systems:
    - Coverage;
    - Scalability;
    - Compatibility grid.
  - It was assumed that the integration of IDS was feasible.

4 - INTRUSION DETECTION FOR GRID AND CLOUD

- Providing security in a distributed system requires:
  - More than user authentication with passwords or digital certificates;
  - Confidentiality of data transmission;
  - Strict control of the tasks performed;
  - Prevent malicious users;
  - Rapid detection of known attacks.

4 - INTRUSION DETECTION FOR GRID AND CLOUD

- Proposals and Solutions *:*
  - Data collection middleware and detection techniques are applied intrusion;
  - Analysis for anomaly detection for verifying the actions of users;
  - Analyze user behavior and knowledge;
  - Verification of violations of security policies and standards of known attacks.

4 - INTRUSION DETECTION FOR GRID AND CLOUD

- Because of its distributed nature, cloud computing environments are a big target for intruders.
- An IDS should be deployed to work in a cloud computing environment. Thus, each node is monitored by a portion of intrusion-detection system and when an attack occurs, an alert is sent to the other nodes of the environment.
- An attack on a system of cloud computing can be silent since communication is usually encrypted and invisible node.
- The described work presents an architecture called IDS cloud CCIDS – Could Computing Intrusion Detection System which makes the detection of network and host attacks to identify the environment.

4 - INTRUSION DETECTION FOR GRID AND CLOUD

- Proposals and Solutions:
  - Node is an entity that contains grid resources;
  - Functionality into the environment through the middleware;
  - Auditor is responsible for capturing data from multiple sources, such as messages that the system registry service and node;
  - IDS service that analyzes data captured with detection techniques based on user behavior knowledge of previous attacks;
  - Storage Service maintains the data required by the IDS service to perform the analysis;

4 - INTRUSION DETECTION FOR GRID AND CLOUD

- Conclusions:
  - One was described cloud computing intrusion detection system capable of identifying unknown attacks;
  - The solution is a service of DHS that captures audit data from one part of registry to increase the security level on each node;
  - Two techniques were applied:
    - He was made an artificial neural network to recognize patterns of user behavior and indicate abnormal activity;
    - Identification of tracks already known attacks from a set of rules, where we describe a system for capturing data from system audit log and message exchange between network nodes.
  - Processing cost is low and the yield is satisfactory for a real time implementation.

5 - SLA IN SECURITY MANAGEMENT FOR CLOUD COMPUTING

5.1. Service Level Agreements for Security (Sec-SLA):

- Preventing attacks and using computational mechanisms that involve levels of security service that is delivered.
- Is a formal negotiated document that defines in, specially, a quantitative way what service levels will be delivered from the provider to the customer.

5 - SLA IN SECURITY MANAGEMENT FOR CLOUD COMPUTING

5.1. Service Level Agreements for Security (Sec-SLA):

- Service level security requirements include: cryptography, data packet filtering, redundancy of hardware and software and so on.
- Monitoring and control of the agreements (Sec-Mon): monitoring whether the agreed metrics are being met. The architecture Sec-Mon is independent of a specific technology.

5 - SLA IN SECURITY MANAGEMENT FOR CLOUD COMPUTING

5.2. Overview on the subject

- Cloud computing, 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.
- An advantage of a SLA-Sec is the possibility of a better understanding of how security is being performed.

5 - SLA IN SECURITY MANAGEMENT FOR CLOUD COMPUTING

5.3. Difficulties to define security metrics to be used in SLA:

- The paradigm is still evolving, as well as the understanding of what are the security challenges that it brings. Services delivered in such conditions demand considerable effort in the process of defining security service levels.
- The negotiation of the SLA will have to be agile, in order to not affect the hiring of services, to allow demands to be met more quickly.

6. COSTUMER SECURITY IN CLOUD COMPUTING

6.1. Definition of cloud computing:

- 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.
- Cloud computing makes use of existing technologies, such as virtualization, distributed computing, grid computing, utility computing and Internet.

6. COSTUMER SECURITY IN CLOUD COMPUTING

6.2. Main Security Problems Pointed for Cloud Computing Security:

- Three main concerns of customers:
  - Vulnerability to attack;
  - Standard security practices;
  - Being subject to state or national data-storage laws related to privacy or record keeping

6. COSTUMER SECURITY IN CLOUD COMPUTING

6.3. Unique security risks, considering security conditions during the process of choosing a cloud provider:

- Privileged user access;
- Regulatory Compliance;
- Data location;
- Data segregation;
- Recovery;
- Investigative support;
- Long-term viability

7. CLOUD COMPUTING FOR HEALTH CARE

7.1. Solution to automate processes for atient‘s vital data collection

- Telemedicine allows remote diagnoses and monitoring of patients. 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.

7. CLOUD COMPUTING FOR HEALTH CARE

7.2. Several challenges associated to automation in this sort of environment:

- 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.

7. CLOUD COMPUTING FOR HEALTH CARE

7.3. Solution Presented:

- 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.

7. CLOUD COMPUTING FOR HEALTH CARE

7.4. Several practical advantages in this implementation:

- it provides always on, real-time data collecting;
- it eliminates manual collecting work and possibility of typing errors;
- it facilitated the deployment process.

- The proposed architecture covers the several elements in current systems.

8 - ROUTING FOR GRID AND CLOUD COMPUTING

8.1. Grid and Cloud computing technologies:

- These structures aim to support service applications by grouping devices and shared resources in one large computational unit.
- The need to connect many heterogeneous systems is one of the main necessities of grid and cloud computing, introducing new levels of complexity.

8 - ROUTING FOR GRID AND CLOUD COMPUTING

8.2. Problems of Management:

- The configuration and management is done by humans making slow and a subject of decision making problems.
- The solution would be no human intervention in the management. How to manage efficiently and in an automated way a heterogeneous and complex environment, like grid or cloud?

8 - ROUTING FOR GRID AND CLOUD COMPUTING

8.3. An experimental assessment of routing for grid and cloud :

- 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.
- 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.

8 - ROUTING FOR GRID AND CLOUD COMPUTING

8.3. An experimental assessment of routing for grid and cloud :

- The convergence time of the algorithm based on the direct interconnection to the neighbor node is really small and almost constant.
- The proposed solution to automatically manage the complexity of grid computing and cloud is on creating intelligent agents able to sense their environment and acting in accordance with pre-defined policies.

9 - MANAGEMENT FOR GREEN CLOUD COMPUTING

- A. Scope and Context
- B. Proposals and solutions
- C. Conclusion and future works

9 - MANAGEMENT FOR GREEN CLOUD COMPUTING

- Scope and Context:
  - Propose an integrated solution for environment, services and network management based on organization model of autonomous agent components.
  - The goal of green computing

9 - MANAGEMENT FOR GREEN CLOUD COMPUTING

- Scope and Context:
- Approaches to dealing with the problems of load prediction models include the following:
  - Allow for a margin of on-line resources
  - To turn on idle resources;
  - To temporarily use external resources on demand

9 - MANAGEMENT FOR GREEN CLOUD COMPUTING

- Scope and Context:
- Propose a solution based on integrated environment, services and network management that promotes:
  - Equitable load distribution through techniques like virtual machines;
  - Predictive resource allocation models through historical load analysis and pro-active allocation methods;
  - Aggregate energy management of network devices;
  - Integrated control over the environmental support units, which represent the larger share of energy consumption.

9 - MANAGEMENT FOR GREEN CLOUD COMPUTING

- Scope and Context:
- The objectives are the following:
  - To provide flexibility of the system configuration that allows for the easy introduction of new elements in the managed environment;
  - To provide a level of availability that keeps to higher standard SLA compliance rates and which contributes to system's stability and security;
  - To reduce cost in both capital and operational costs (CAPEX and OPEX) to support the business predicates;
  - To provide sustainability by using methods to reduce energy utilization and carbon emission footprints.

9 - MANAGEMENT FOR GREEN CLOUD COMPUTING

- Proposal and solutions:
  - Propose an organization theory model for integrated management of a green cloud computing environment.

9 - MANAGEMENT FOR GREEN CLOUD COMPUTING

- Proposal and solutions:
- Our research advances the state of the art as follows:
  - 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;
  - It analyses the network and system's behavior and operational principles;

9 - MANAGEMENT FOR GREEN CLOUD COMPUTING

- Proposal and solutions:
- It validates the proposal demonstrating the system's added-value in a case study scenario;

- It improves a simulator (the CloudSim framework) to validate the green cloud computing management approach.

9 - MANAGEMENT FOR GREEN CLOUD COMPUTING

- Proposal and solutions:
  - Was 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.

9 - MANAGEMENT FOR GREEN CLOUD COMPUTING

- Conclusion:
  - The Organization theory model was proposed;
  - The Concepts related to cloud computing and green cloud computing were presented;
  - Tests were realized to prove the validity of the system by utilizing CloudSim simulator.

10 - RADIO LAYER OPERATION IN COGNITIVE NETWORKS

- A. Scope and Context;
- B. Proposals and solutions;
- C. Conclusion and future works.

10 - RADIO LAYER OPERATION IN COGNITIVE NETWORKS

- Scope and Context:
  - Schema to classify the signal of band ocupation;
  - List of functionalities of information and operations;
  - Evaluate the expressivity of proposed schema.

10 - RADIO LAYER OPERATION IN COGNITIVE NETWORKS

- Scope and Context:
  - The increase in use of wireless networks led the USA FCC to publish a report showing that problem of spectrum shortage.
  - an effort has been conducted in order to that unlicensed users could use the spectrum already assigned to licensed users.

10 - RADIO LAYER OPERATION IN COGNITIVE NETWORKS

- Scope and Context:
  - We must assure cognitive capability and re-configurability.
  - There are two types of spectrum awareness:
    - Passive;
    - Active.

10 - RADIO LAYER OPERATION IN COGNITIVE NETWORKS

- Proposals and solutions:
  - Spectrum signal sensing - the cognitive radio must be able to perform PU detection, sensing control and, in cooperative mode, cooperation.
  - Spectrum management - requires three main aspects to be successful :
    - spectrum Characterization;
    - spectrum selection ;
    - Reconfiguration.

10 - RADIO LAYER OPERATION IN COGNITIVE NETWORKS

- Proposals and solutions:

  – Spectrum sharing - stems from the need in preventing, multiple CR networks colliding in spectrum overlapping portion. This concept is detailed and subdivided in intra-network spectrum sharing and internetwork.

  – Spectrum mobility - gives rise a new type of handoff in CR network, the so-called spectrum handoff. 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.

10 - RADIO LAYER OPERATION IN COGNITIVE NETWORKS

- Proposals and solutions:
  - 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.

10 - RADIO LAYER OPERATION IN COGNITIVE NETWORKS

- Conclusion and future works:
  - Evolution of cognitive radios and networks
    - framework composed by a schema for sensing signal and classify the spectrum.
  - 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.

11 - Conclusions

- Was presented some of the major contributions our work group has offered in the last few years like. Are these:
  - The work “A Security Framework for Input Validation”;
  - The work “Intrusion Detection for Computational Grids”;
  - The work “Intrusion Detection for Grid and Cloud;
  - Computing”.

11 - Conclusions

- The work “A SLA Perspective in Security Management for Cloud Computing”;
- The work “Customer Security Concerns in Cloud Computing”;
- The work “A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions”.

11 - Conclusions

- The work “Experimental Assessment of Routing for Grid and Cloud”;
- The work “Simulator Improvements to Validate the Green Cloud Computing Approach”;
- The work “A framework to Radio Layer Operation in Cognitive Networks”.