# Grid and Cloud Computing Management and Security

Carlos Becker Westphall

Federal University of Santa Catarina
Networks and Management Laboratory

# Outline

1. Grid and Cloud Computing Management and Security

1.1. Tutorial Organization

2. Grid and Cloud Computing Autonomic Management

2.1. Introduction

2.2. Autonomic Computing

2.3. Grid and Cloud Computing

# Outline

2.4. Autonomic Grid and Cloud Management

2.5. Implementation and Tests

2.6. Conclusions

3. Intrusion Detection Techniques in Grid and Cloud Computing

3.1. Introduction

3.2. Features of Related Works

3.3. Architecture of the Intrusion Detection System

# Outline

3.4. Prototype to Evaluate the Architecture

3.5. Conclusions

4. Cloud Computing Security

4.1. Introduction

4.2. Cloud Computing Types

4.3. Cloud Computing Security Overwiew

4.4. Conclusions

5. Final Considerations

# 1. Grid and Cloud Computing Management and Security

1.1. Tutorial Organization

- Grid and Cloud Computing Autonomic Management.

- Intrusion Detection Techniques in Grid and Cloud Computing.

- Cloud Computing Security.

- Final Considerations.

# 2. Grid and Cloud Computing Autonomic Management

## 2.1. Introduction (Motivation)

- 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.

# 2. Grid and Cloud Computing Autonomic Management

## 2.1. Introduction (Motivation)

- Management complexity grows proportionally to the number of resources being integrated.

- From a given point up, manual management of large grid and cloud structures is unfeasible.

# 2. Grid and Cloud Computing Autonomic Management

## 2.1. Introduction (Motivation)

- This scenario calls for automated management methods to support availability, quality of service and optimized configurations.

- How to manage efficiently and in an automated way a heterogeneous and complex environment, like grid or cloud?

# 2. Grid and Cloud Computing Autonomic Management

## 2.1. Introduction (Objectives)

- The design of a grid and cloud computing management system based on autonomic elements acting as intelligent agents, which aims to promote characteristics of self-management.

- Proof-of-concept implementation and case study scenarios.

# 2. Grid and Cloud Computing Autonomic Management

2.1. Introduction (Organization)

- Section 2.2 provides some comments on autonomic computing.
- Section 2.3 discusses grid and cloud computing.
- Section 2.4 proposes an autonomic management system for grid and cloud computing.
- Section 2.5 describes the implementation and tests performed.

# 2. Grid and Cloud Computing Autonomic Management

## 2.2. Autonomic Computing

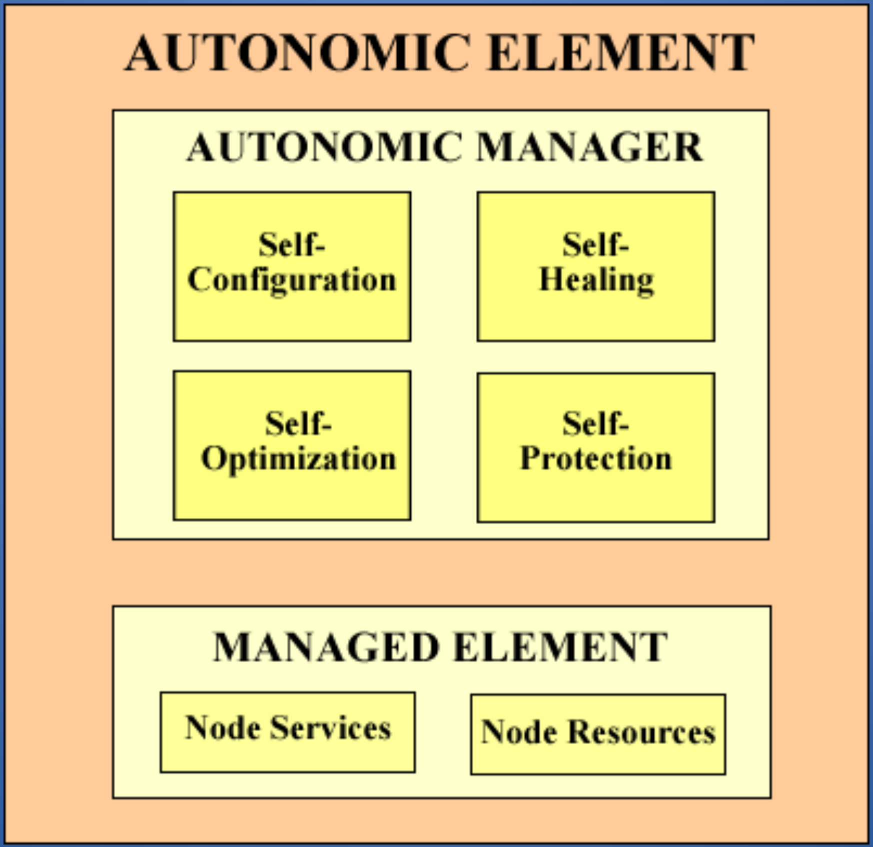
- Main characteristics: self-configuration, self-healing, self-optimization, and self-protection.

- The autonomic elements (AE), considered to be like the bricks of a building, are the functional units of autonomic systems.

- They control the resources and offer services to the users and other AEs.

# 2. Grid and Cloud Computing Autonomic Management

## 2.2. Autonomic Computing



# 2. Grid and Cloud Computing Autonomic Management

## 2.2. Autonomic Computing

- What differentiates an autonomic from a non-autonomic system is the presence of the autonomic manager.

- The autonomic manager is able to build and execute plans based on the analysis of sent information, which removes the need for human intervention.

# 2. Grid and Cloud Computing Autonomic Management

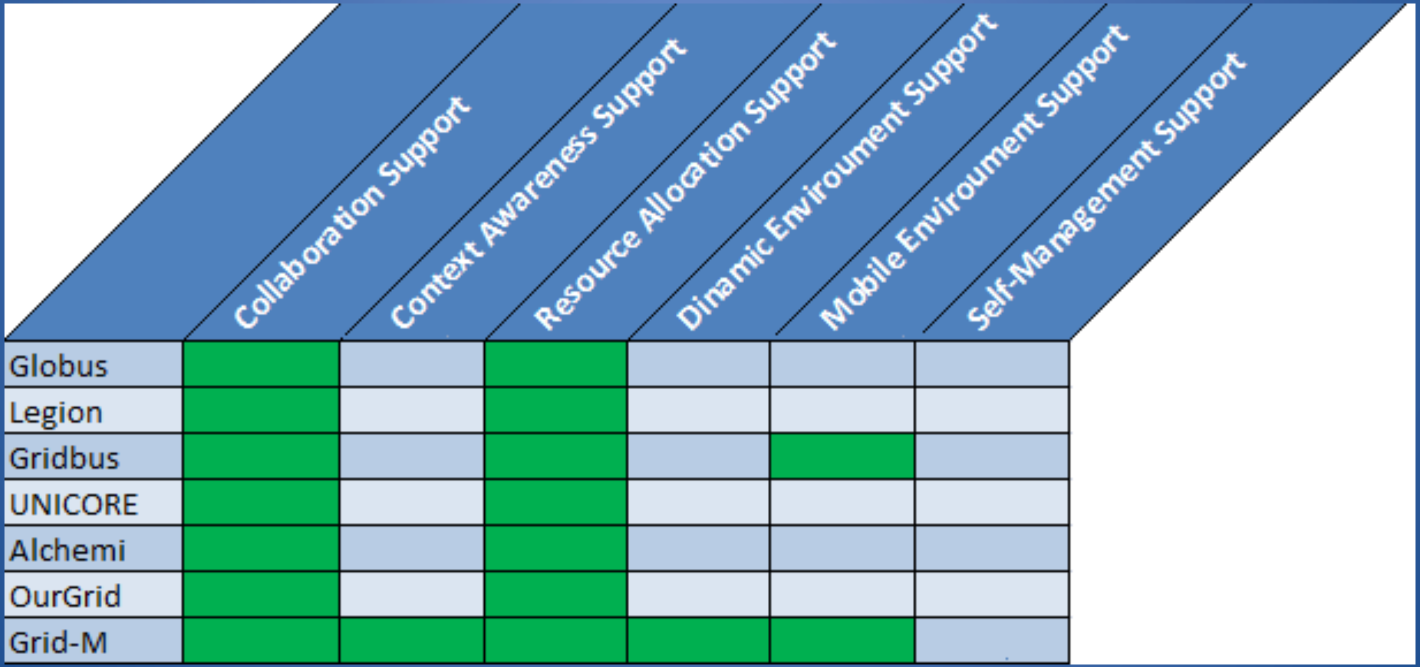
## 2.3. Grid and Cloud Computing

- Grid and cloud computing solutions aim to simplify the access to resources of a distributed system, some times giving the idea that they form a unique and powerful computer. This is achieved by techniques such as virtualization.

- Resource virtualization minimizes the impact of heterogeneity by providing access to well defined interfaces or to work units in terms of virtual machines.

# 2. Grid and Cloud Computing Autonomic Management

## 2.3. Grid and Cloud Computing



| | Collaboration Support | Context Awareness Support | Resource Allocation Support | Dinamic Enviroument Support | Mobile Enviroument Support | Self-Management Support |
|---|---|---|---|---|---|---|
| Globus | 🟩 | | 🟩 | | | |
| Legion | 🟩 | | 🟩 | | | |
| Gridbus | 🟩 | | 🟩 | | 🟩 | |
| UNICORE | 🟩 | | 🟩 | | | |
| Alchemi | 🟩 | | 🟩 | | | |
| OurGrid | 🟩 | | 🟩 | | | |
| Grid-M | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | |

# 2. Grid and Cloud Computing Autonomic Management

## 2.3. Grid and Cloud Computing

- All listed middleware support collaboration and resource allocation.

- Only two systems support execution on mobile environments.

- Only one provides context sensibility.

- None supports autonomic behavior. There is a need for middleware that supports autonomic.

# 2. Grid and Cloud Computing Autonomic Management

## 2.3. Grid and Cloud Computing

- Cloud computing is a new distributed computing and business paradigm. It can provide computing power, software and storage resources, and even a distributed data center infrastructure on demand.

- To make these characteristics viable, it uses existing technologies, such as virtualization, distributed computing, grid computing, utility computing and the network infrastructure provided by the Internet.

# 2. Grid and Cloud Computing Autonomic Management

## 2.4. Autonomic Grid and Cloud Management

- A middleware capable of supporting this new computational environment must offer large scale distributed computing that permits to integrate sensors and mobile devices.

- The computational grids and clouds are known as a dynamic and heterogeneous computational environment, even though, the configuration of these environments is done manually and susceptible to slow decision making or errors of the administrators.

- In order to avoid this problem a solution is needed to take the responsibility away from the human administrators.

# 2. Grid and Cloud Computing Autonomic Management

## 2.4. Autonomic Grid and Cloud Management

- [Liu, 2005] proposes an autonomic architecture to manage the heterogeneity and dynamics of the grid environments.

- [Beckstein, 2006] presents the SOGOS architecture aimed to support self-organization in computational grids.

- [Brennand, 2007] presents the AutoMan, a system which has the objective of offering certain levels of automatic management to the computational grids in pairs.

# 2. Grid and Cloud Computing Autonomic Management

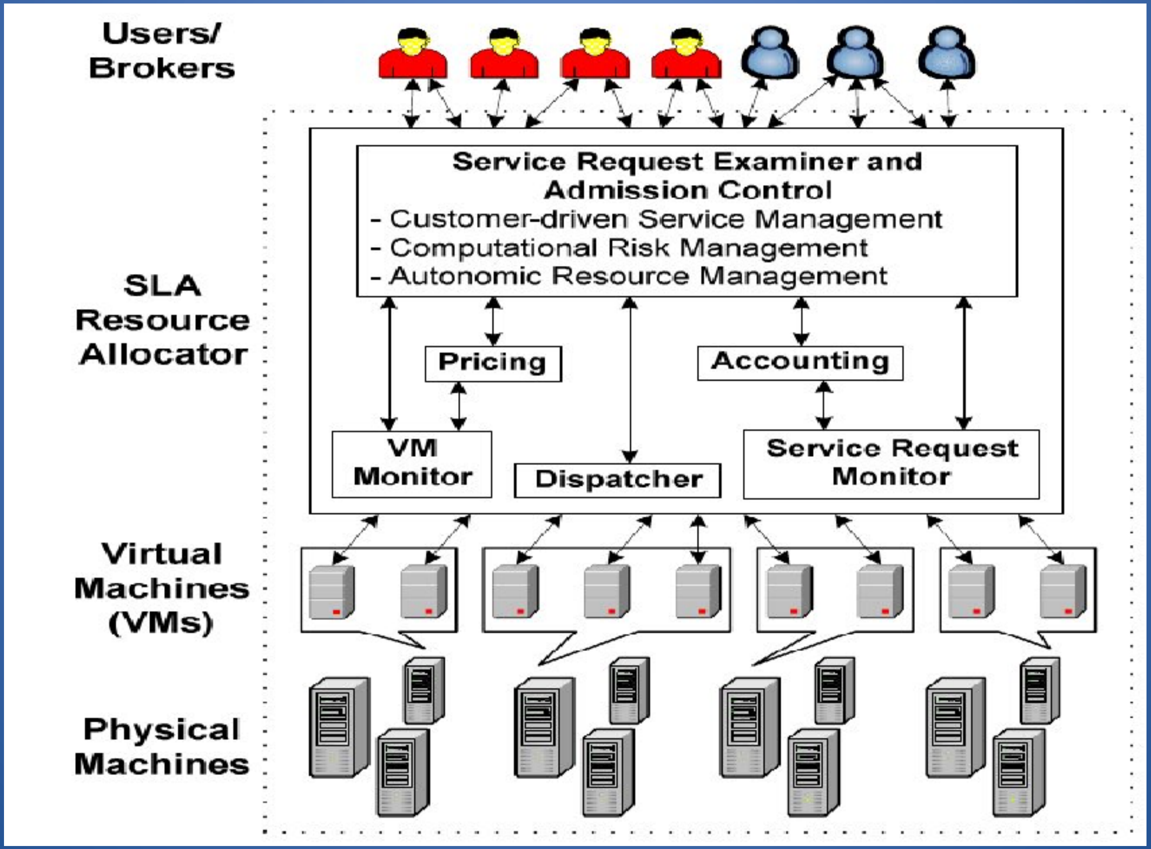
## 2.4. Autonomic Grid and Cloud Management

- [Xiao, 2008] adapts web pages to small screen devices, utilizing the large computing and storage resource capabilities of cloud computing infrastructures.

- [Buyya, 2008] defines Cloud computing and provides the architecture for creating market-oriented Clouds by leveraging technologies such as Virtual Machines (VMs).

# 2. Grid and Cloud Computing Autonomic Management

## 2.4. Autonomic Grid and Cloud Management


Users/ Brokers
SLA Resource Allocator
Service Request Examiner and Admission Control
- Customer-driven Service Management
- Computational Risk Management
- Autonomic Resource Management
Pricing
Accounting
VM Monitor
Dispatcher
Service Request Monitor
Virtual Machines (VMs)
Physical Machines

# 2. Grid and Cloud Computing Autonomic Management

## 2.4. Autonomic Grid and Cloud Management

- An autonomic management system for grid and cloud computing, built using intelligent agents that will create a multi-agent system. Each agent has its own objectives that is responsible to follow its actions.

- The autonomic elements be built by agents (responsible to "understand" the context, take decisions according to high-level polices and act over it). The union of many autonomic elements creates an autonomic system, which can be viewed as a multi agent system.

# 2. Grid and Cloud Computing Autonomic Management

## 2.4. Autonomic Grid and Cloud Management

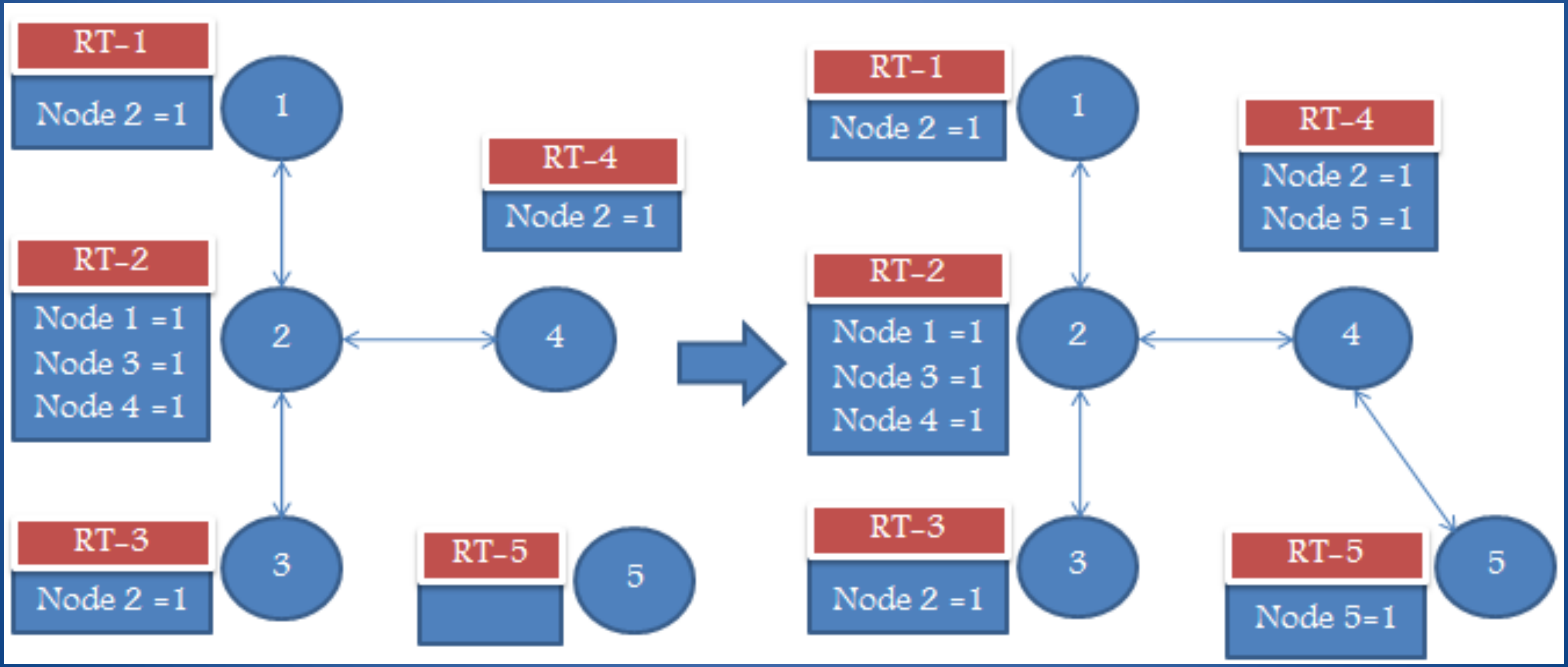
- What allows a system to be called autonomic is a presence of an autonomic manager. Through the monitoring of managed elements and their external environment, the autonomic manager is able to build and execute plans for implementation, based on the analysis of sent information.

- The system proposed 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.

# 2. Grid and Cloud Computing Autonomic Management

## 2.4. Autonomic Grid and Cloud Management

Routing algorithm based on the direct interconnection to the neighbor node



RT-1
Node 2 =1

RT-4
Node 2 =1

RT-2
Node 1 =1
Node 3 =1
Node 4 =1

RT-3
Node 2 =1

RT-5

RT-1
Node 2 =1

RT-4
Node 2 =1
Node 5 =1

RT-2
Node 1 =1
Node 3 =1
Node 4 =1

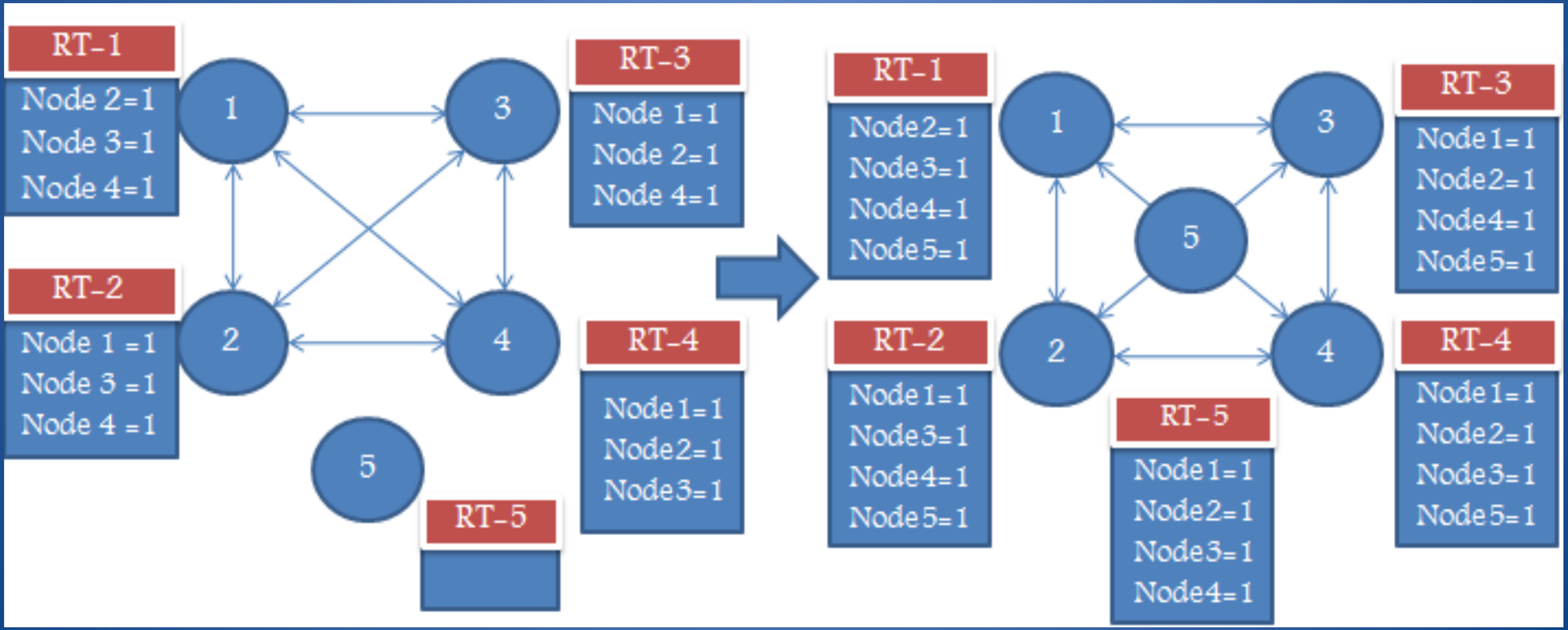
RT-3
Node 2 =1

RT-5
Node 5=1

# 2. Grid and Cloud Computing Autonomic Management

## 2.4. Autonomic Grid and Cloud Management

Routing algorithm based on the complete connection among nodes



RT-1
Node 2=1
Node 3=1
Node 4=1

RT-3
Node 1=1
Node 2=1
Node 4=1

RT-2
Node 1 =1
Node 3 =1
Node 4 =1

RT-4
Node1=1
Node2=1
Node3=1

RT-5

RT-1
Node2=1
Node3=1
Node4=1
Node5=1

RT-3
Node1=1
Node2=1
Node4=1
Node5=1

RT-2
Node1=1
Node3=1
Node4=1
Node5=1

RT-5
Node1=1
Node2=1
Node3=1
Node4=1

RT-4
Node1=1
Node2=1
Node3=1
Node5=1

# 2. Grid and Cloud Computing Autonomic Management

## 2.5. Implementation and Tests

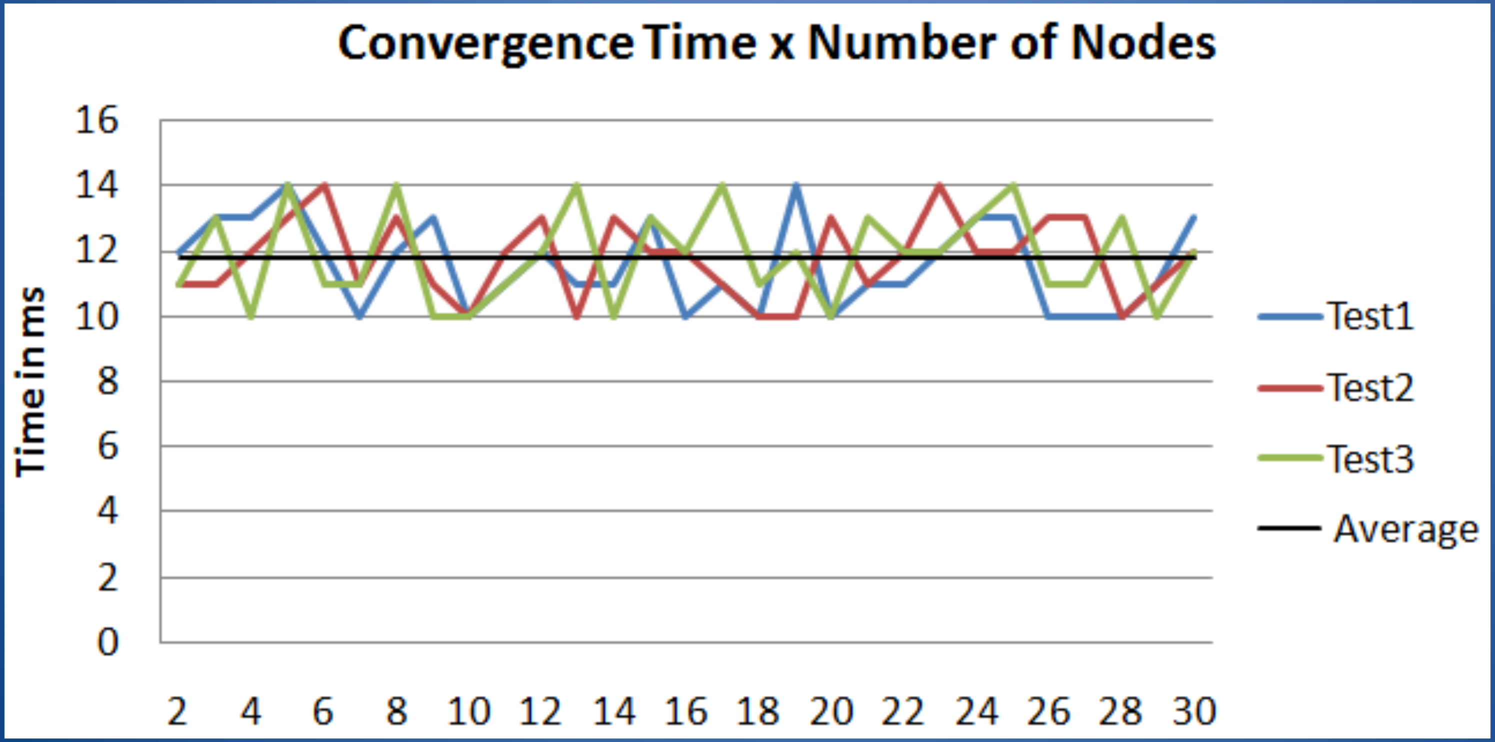
- This section shows the results of a few quantity tests performed during the implementation with the purpose of showing the proposed system efficiency in different use situations.

- To test it, we have implemented it on Grid-M [Franke, 2007]. A grid of 30 nodes was created. These devices are personal computers with an Intel Core Duo 1.66Ghz CPU, 2GB of RAM memory and running Window XP. All devices ran the same programs.

# 2. Grid and Cloud Computing Autonomic Management

## 2.5. Implementation and Tests

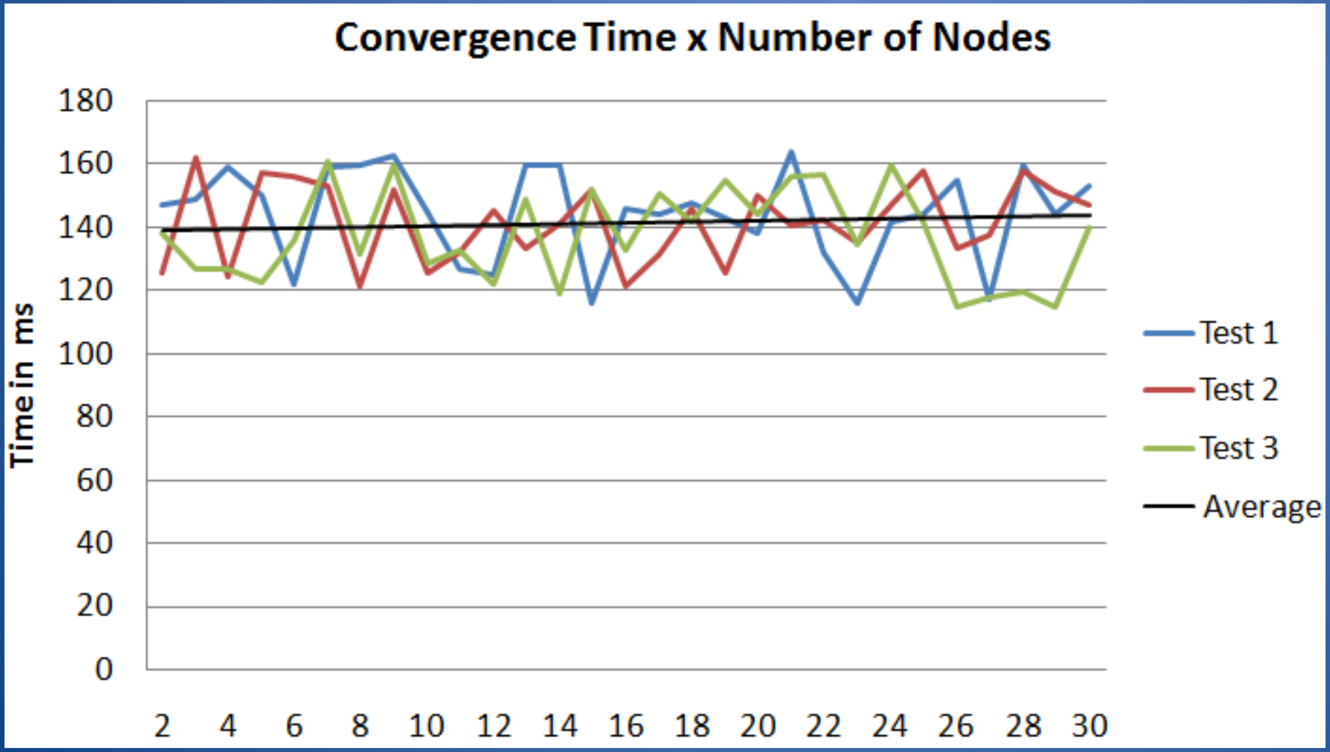
Routing algorithm based on the direct interconnection to the neighbor node



# 2. Grid and Cloud Computing Autonomic Management

## 2.5. Implementation and Tests

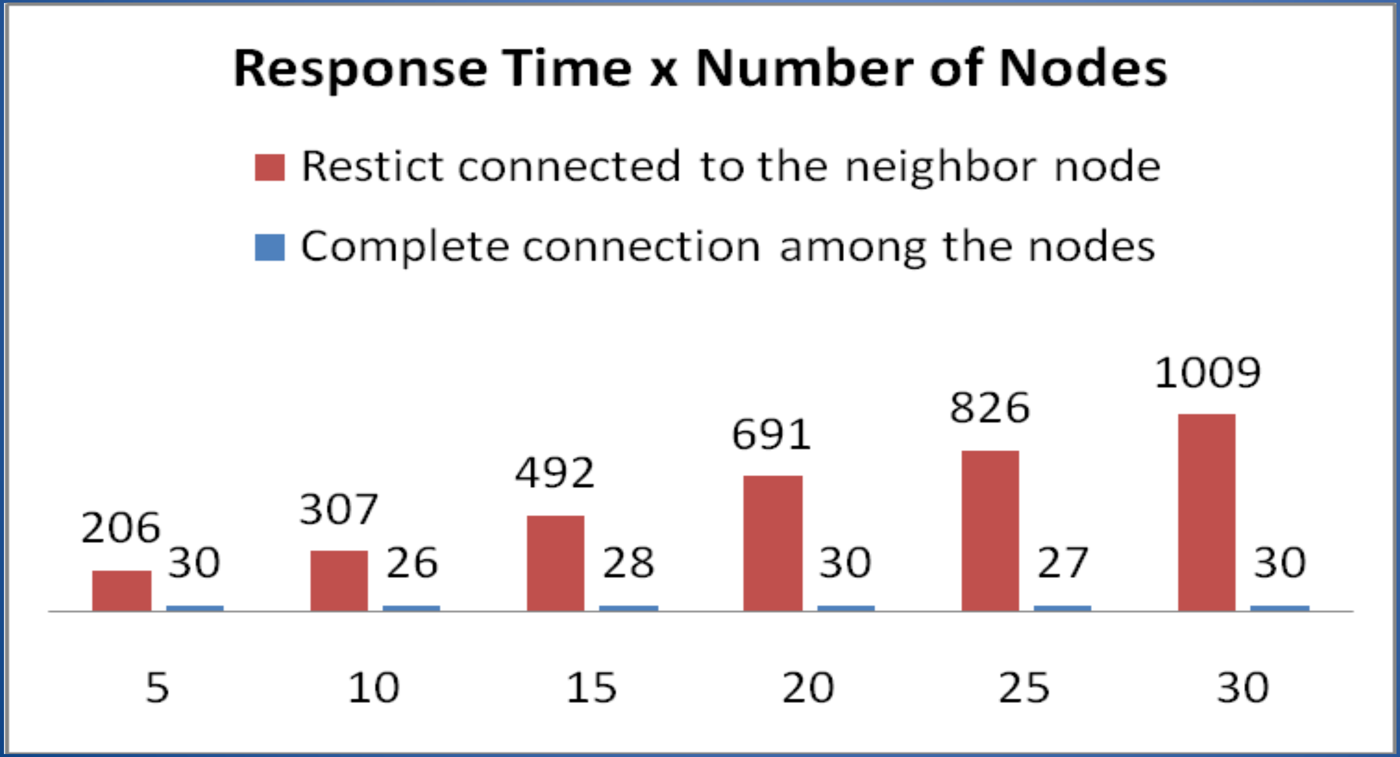
Routing algorithm based on the complete connection among nodes



# 2. Grid and Cloud Computing Autonomic Management

## 2.5. Implementation and Tests

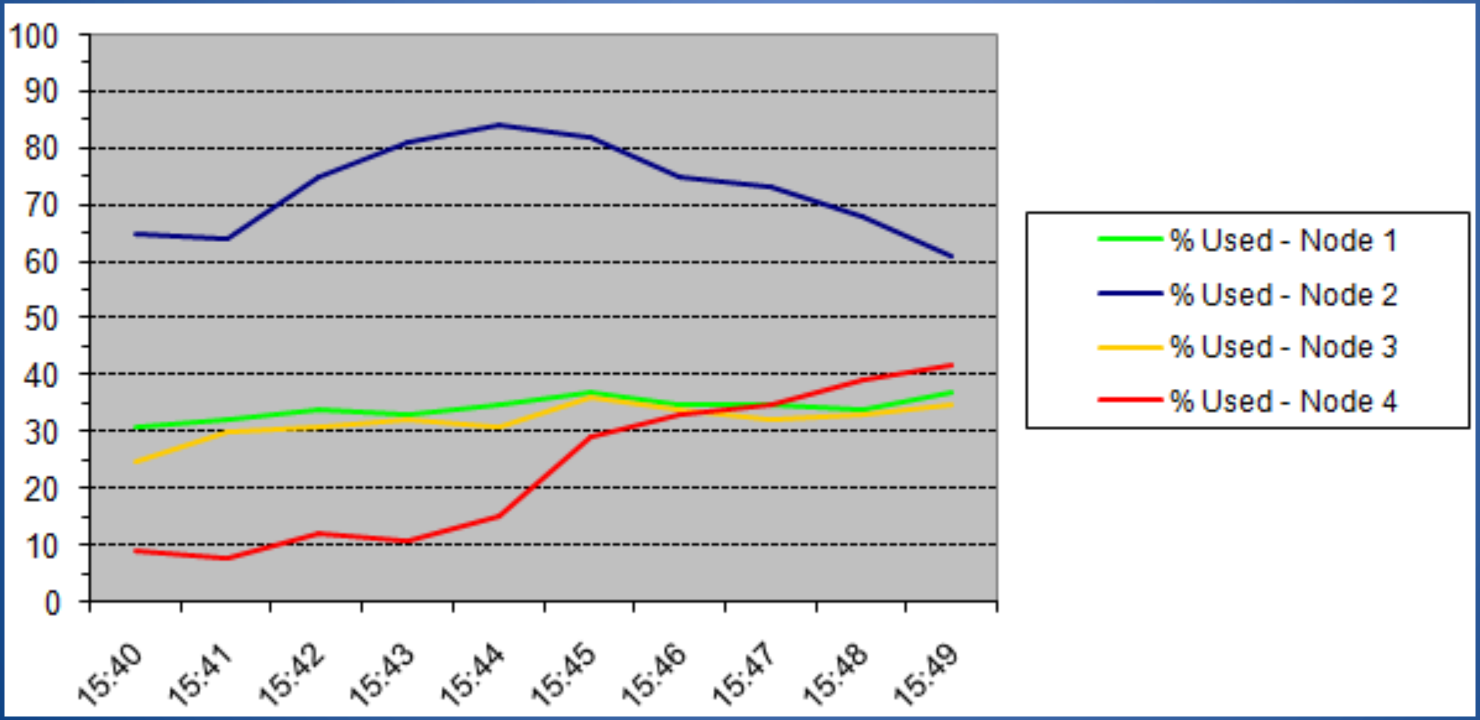
Response time results



# 2. Grid and Cloud Computing Autonomic Management

## 2.5. Implementation and Tests

The resources utilized by the nodes and the services replications



# 2. Grid and Cloud Computing Autonomic Management

- 2.6. Conclusions

- An autonomic grid and cloud computing system with self-management support, using intelligent agents.

- The question we aimed to answer was: How to automate the management of a complex and heterogeneous environment, like grid and cloud computing?

- The solution proposed was the creation of autonomic elements acting as intelligent agents, capable of feel the environment where they are and act upon it according to pre-defined policies.

# 2. Grid and Cloud Computing Autonomic Management

2.7. References

- IBM-Corporation. An architectural blueprint for autonomic computing. *http://www.ibm.com/developerworks/autonomic/library/ac-summary/ac-blue.html*
- P. Horn. Autonomic computing: IBM’s perspective on the state of information technology. Technical report, *International Business Machines Corporation*, Armonk, NY, USA, 2001.
- J. Joseph and M. Ernest. Evolution of grid computing architecture and grid adoption models. *IBM Systems Journal*, 2004, 43(4).
- I. Foster and C. Kesselman. Globus: A metacomputing infrastructure toolkit. *Internacional Journal of Supercomputer Applications*, 1997, 11(2): 115–128.
- R. Buyya. Market-oriented grid computing and the gridbus middleware. *16th International Conference on Advanced Computing and Communications*, 2008. ADCOM 2008.

# 2. Grid and Cloud Computing Autonomic Management

## 2.7. References

- A. Grimshaw and A. Natrajan. Legion: Lessons learned building a grid operating system. *Proceedings of the IEEE*, 2005, 93(3):589–603.
- UNICORE. UNIform Interface to Computer Resources.
- A. Luther, R. Buyya, R. Ranjan, S. Venugopal. Alchemi: A net-based grid computing framework and its integration into global grids, 2005.
- F. Brasileiro, E. C. de Araujo, W. Voorsluys, M. Oliveira, F. Figueiredo. Bridging the high performance computing gap: the our grid experience. *In Proceedings of the Seventh IEEE International Symposium on Cluster Computing and the Grid/First Latin American Grid Workshop (LAGrid07)*, 2007.
- H. A. Franke, C. Rolim, C. B. Westphall, F. Koch and D. O. Balen. Grid-M: Middleware to integrate mobile devices, sensors and grid computing. *The Third International Conference on Wireless and Mobile Comunications – ICWMC* 2007.

# 2. Grid and Cloud Computing Autonomic Management

## 2.7. References

- H. Liu,V. Bhat, M. Parashar, S. Klasky. An autonomic service architecture for self-managing grid applications. InGRID’05: *Proceedings of the 6th IEEE/ACM Internation Workshop on Grid Computing*, 2005.
- C. Beckstein, P. Dittrich, C. Erfurth, D. Fey, B. Konig-Ries, M. Mundhenk and H. Sack. Sogos-distributed meta level architecture for the self-organizing grid of services. *In MDM’06: Proceedings of the 7th International Conference on Mobile Data Management*, 2006.
- C. Brennand, M. Spohn, A. Souza, G. Ferreira, D. Candeia, G. Germoglio, F. Santos. Automan: Autonomic Management on Ourgrid. *V Workshop for Grid Computing and Aplications,* 2007.
- R. Buyya, C. S. Yeo, S. Venugopal, Srikumar. Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. *10th IEEE International Conference In High Performance Computing and Communications*, 2008.
- Y. Xiao, Y. Tao, Q. Li. A New Wireless Web Access Mode Based on Cloud Computing. *Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, 2008.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.1. Introduction (Motivation)

- Rigorous control of the executed tasks is needed in order to prevent malicious users from breaking policies, to identify the use of stolen passwords, and also to make possible rapid detection of known attacks.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.1. Introduction (Objectives)

- Solution for intrusion detection in grid and cloud computing environment is presented in which audit data is collected and two intrusion detection techniques are applied.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.1. Introduction (Objectives)

- 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 in terms of performance results.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.1. Introduction (Organization)

- Section 3.2. discusses the Features of Related Works.

- Section 3.3. presents the Architecture of the Intrusion Detection System.

- Section 3.4. describes the Prototype to Evaluate the Architecture.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.2. Features of Related Works

- Research on intrusion detection for grids has been published and here we try to describe relevant ones in terms of techniques they apply and the source of the data they analyze.

- Each one is classified according to audit data source (host, network, or grid), analysis technique (knowledge or behavior-based), and if the solution was properly evaluated.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.2. Features of Related Works

- [Fang-Yei, 2005] and [Kenny, 2005] solutions are based on analyzing data from a grid's network, although they don't support the detection of grid-specific attacks, since no high-level data is captured.

- [Feng, 2006] integrates a host-based IDS to a grid environment, providing protection against typical operating system attacks, but not the ones which may target middleware vulnerabilities.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.2. Features of Related Works

- [Tolba, 2005] and [Schulter, 2008] considers a computational grid one big host of resources, and the audit data is collected from the operating systems as in typical host-based IDS.

- In comparison to our goal, we conclude that the available solutions approach the problem in a different way, especially in regards to the threats we try to defend against by combining two distinct auditing techniques.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

3.3. Architecture of the Intrusion Detection System

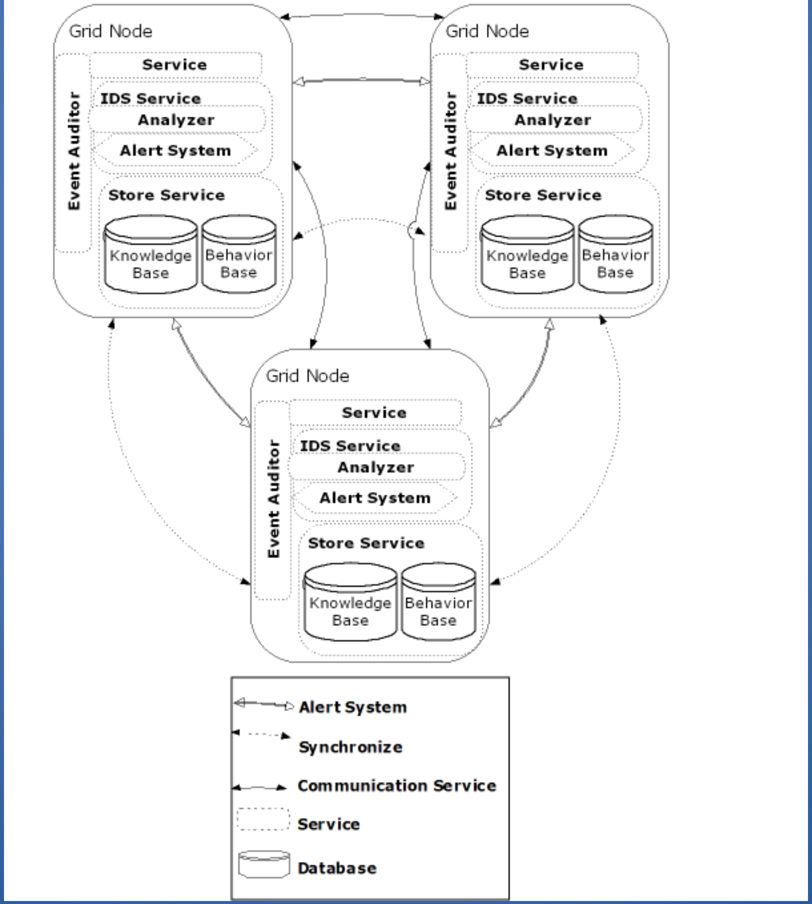
- Grid and cloud computing are distributed computing in essence and because of this we suggest that intrusion detection and its alert system should be distributed and cooperative.

- 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 intrusion detection.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.3. Architecture of the Intrusion Detection System



# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.3. Architecture of the Intrusion Detection System

- Node is an entity which contains resources.

- Service provides its functionality in the environment through the middleware.

- 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.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

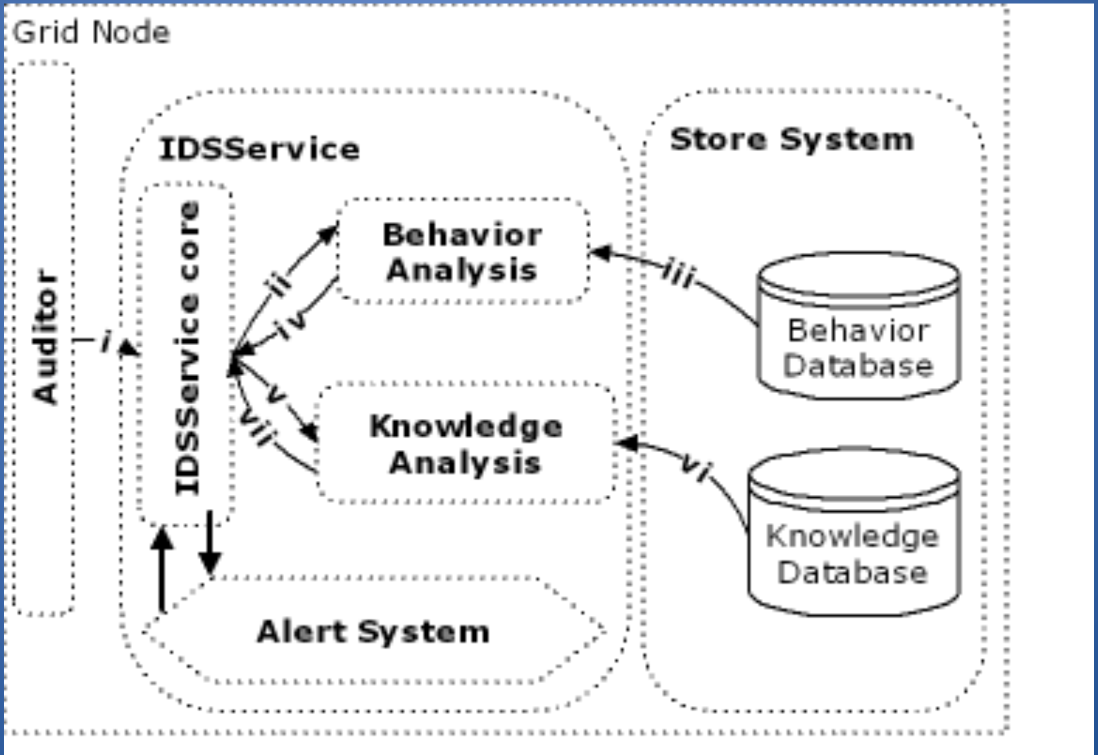
## 3.3. Architecture of the Intrusion Detection System

- IDS Service analyzes data captured by the auditor and applies detection techniques based on user behavior and knowledge of previous attacks.

- Storage Service holds the data needed by the IDS Service to perform analysis.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.3. Architecture of the Intrusion Detection System



# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.3. Architecture of the Intrusion Detection System

- The audited data is sent (i) to the IDSService core which starts the behavior analysis task (ii). This task uses artificial intelligence tricks to detect user behavior deviations. With the help of a profile history database (iii), the analyzer is able to determine the distance between this behavior and the usual one and (iv) communicates this to the IDSService. The rules analyzer receives audit packages (v) and verifies with the policies if any rule in the database (vi) is being broken. The result is returned to the IDSService core (vii). With these responses (iv, vii), the IDS calculates the probability that the action represents an attack. The other nodes are alerted if the probability is high enough

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.3. Architecture of the Intrusion Detection System

- ***Behavior Analysis.*** Numerous methods try to solve the problem of behavior-based intrusion detection, such as data mining, artificial neural networks, and artificial immunological systems. In this work we focused on using a feed-forward artificial neural network because, in contrast to traditional methods, this type of network can achieve fast processing of information, self-learning, and a great ability to tolerate little deviations of behavior.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

3.3. Architecture of the Intrusion Detection System

- ***Knowledge Analysis.*** Knowledge-based intrusion detection is the most often applied technique in the field because it results in a low false alarm rate and high positive rates, although it cannot detect unknown attack patterns. It is based on rules (also called signatures) and monitoring a stream of events to find malicious characteristics. With the support of an expert system, it is possible to describe a malicious behavior with a rule.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.3. Architecture of the Intrusion Detection System

- The two intrusion detection techniques are distinct. As the knowledge-based intrusion detection is characterized by a high hit rate of known attacks, its deficiency in detecting new attacks is complemented with the behavior-based technique.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.4. Prototype to Evaluate the Architecture

- The prototype to evaluate the architecture described in this work uses Grid-M [Franke, 2007], a middleware developed at the same research group where this work was done.

- Data tables were created to perform the experiments with audit elements coming from both the log system and data captured from the node communications.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.4. Prototype to Evaluate the Architecture

- We prepared three types of simulation data to perform the tests with:
- Data representing legitimate actions;
- Data representing behavior anomalies; and
- Data representing policy violation.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

3.4. Prototype to Evaluate the Architecture

- All the requests received by a node and their corresponding responses and other messages are captured by the communication auditor. The capturing of this data is fundamental for behavior analysis.

- For each action performed by a node a log entry is generated to register the methods and parameters invoked during the action.

- The evaluation of the behavior-based technique was performed with artificial intelligence enabled by a feed forward neural network [Idris, 2005].

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.4. Prototype to Evaluate the Architecture

- To measure the efficiency of an intrusion detection system the following parameters can be used [Debar, 1999]:

- Accuracy evaluates the attack detection and the absence of false alarms. A system is imperfect when a legitimate action is accused of being malicious. Accuracy measures the number of false positives and false negatives;

- False positive is an alert about an action that is actually legitimate; and

- False negative is occurrence of an attack and subsequent absence of an alert action.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

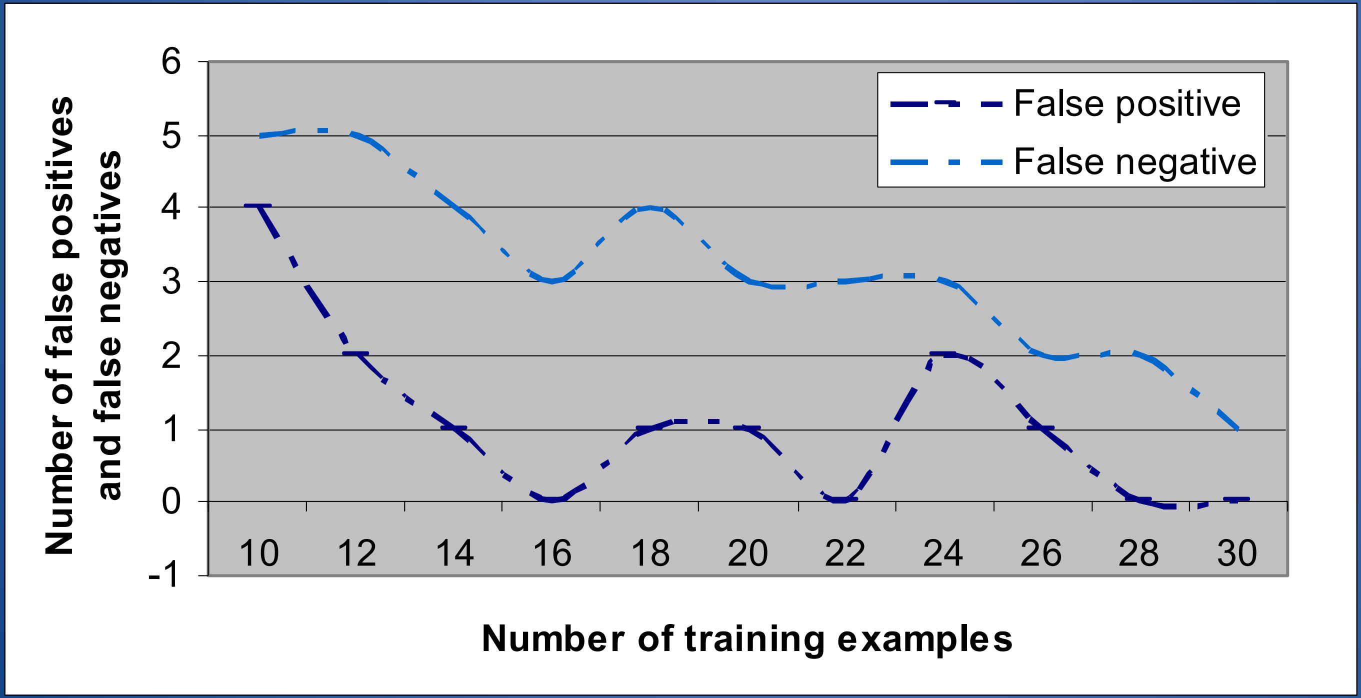
## 3.4. Prototype to Evaluate the Architecture

- A load test was performed where the program analyzed 1 to 100,000 actions.
- An action takes 0.000271 seconds on average to be processed with our setup.
- The training time for an input of 30 days of sample behavior took 1.993 seconds.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.4. Prototype to Evaluate the Architecture

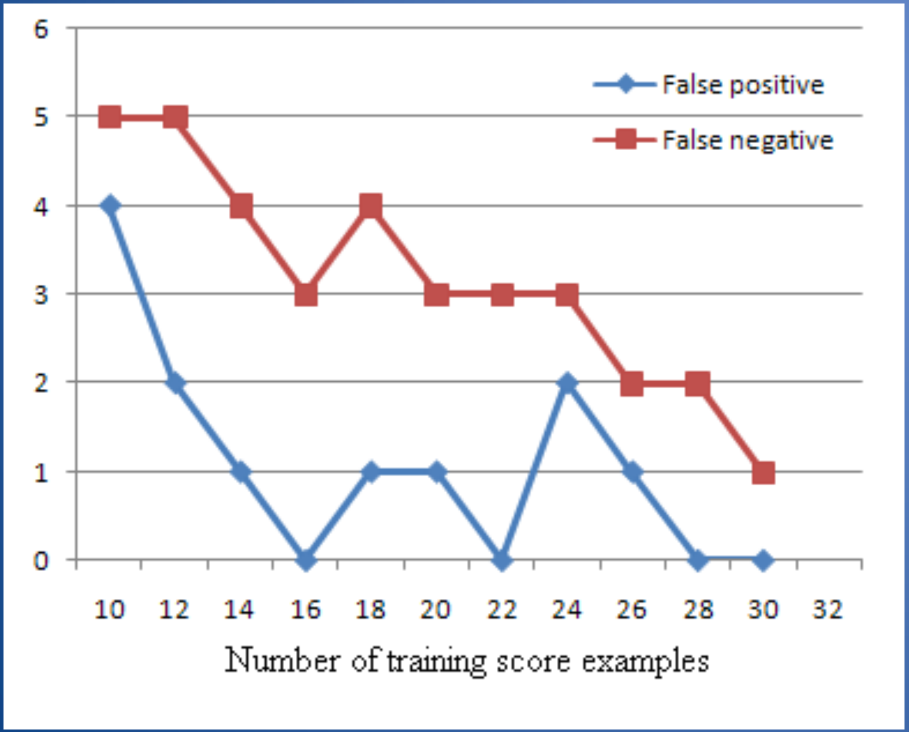
Behavior score results



# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.4. Prototype to Evaluate the Architecture

Behavior score results



# 3. Intrusion Detection Techniques in Grid and Cloud Computing

3.4. Prototype to Evaluate the Architecture

- Starting the training with 16 days of simulation no false alarms occurred, although the uncertainty level was still high with several outputs near zero.

- With 28, 29, and 30 days input periods, the algorithm showed a very low number of false positives.

- In contrast to the behavior-based system, not only audit data from a log system, but also from the communication system was taken as input. A series of rules was elaborated to illustrate security policies to be monitored by the IDS.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

3.4. Prototype to Evaluate the Architecture

1. At startup, the rules stored in a XML file are loaded into a data structure;

2. The auditor starts to capture data from the log and communication systems;

3. The data is pre-processed to create a data structure dividing log data from communication data in order to provide easy access to each element;

4. The corresponding policy for the audit package is verified; and

5. An alert is generated in case an attack or violation occurred.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.4. Prototype to Evaluate the Architecture

- The behavior-based analysis accuracy experiments showed a low number of false positives and false negatives when a large number of examples exist in the user profile database.

- The experiment showed that the algorithm consumes 2.6 seconds to process 10,000 actions. The knowledge-based technique prototype consumed 2.7 seconds to analyze one million rules.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.5. Conclusions

- Behavior-based intrusion detection was achieved 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.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.5. Conclusions

- To perform the required analysis for intrusion detection was described a system for capturing audit data from a log system and messages exchange between nodes.

- 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.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.6. References

- H. Debar, M. Dacier, A. Wespi. “Towards a taxonomy of intrusion detection systems,” Int. J. Computer and Telecommunications Networking, vol. 31, no. 9, pp. 805-822, 1999.
- Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing. April, 2009. http://www.cloudsecurityalliance.org/
- I. Foster, C. Kesselman, G. Tsudik, S. Tuecke. A Security Architecture for Computational Grids. Proc. 5th ACM Conference on Computer and Communications Security Conference, pp. 83-92, 1998.
- S. Axelsson. Research in Intrusion-Detection Systems: A Survey. Technical Report TR-98-17, Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden, 93 p. aug. 1999.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

## 3.6. References

- L. Fang-Yie, et al. Integrating Grid with Intrusion Detection. In: International Conference On Advanced Information Networking And Applications (AINA), 19., 2005, Taipei, Taiwan. IEEE Computer Society, 2005. v. 1, p. 304-309.
- S. Kenny, B. Coghlan, “Towards a grid-wide intrusion detection system,” in Proc. European Grid Conference (EGC2005), pp. 275-284, Amsterdam, The Netherlands, February 2005.
- G. Feng, X. Dong, L. Weizhe, L. Chu, J. Li. GHIDS: Defending Computational Grids against Misusing of Shared Resource. In: Asia-Pacific Conference on Services Computing (APSCC’06), 2006.
- M. Tolba, et al. Distributed Intrusion Detection System for Computational Grids. In: International Conference On Intelligent Computing And Information Systems, 2., 2005, Cairo, Egypt. ACM, 2005.

# 3. Intrusion Detection Techniques in Grid and Cloud Computing

3.6. References

- A. Schulter, K. Vieira, Kleber; C. B. Westphall, C. M. Westphall, A. Sekkaki. Intrusion Dectection for Computational Grids. The Second International Conference on New Technologies, Mobility and Security. November 5 - 7, 2008 Tangier - Marocco, 2008.
- H. Franke, F. Koch, C. Rolim, C. B. Westphall, D. Balen. Grid-M: Middleware to Integrate Mobile Devices, Sensors and Grid Computing. In: ICWMC 2007 - The Third International Conference on Wireless and Mobile Communications, 2007,
- N. B. Idris, B. Shanmugam. Artificial Intelligence Techniques Applied to Intrusion Detection. IEEE Indiscon 2005 Conference, India, pp.52-55, 2005.
- P. F. Silva, C. B. Westphall. Improvements in the Model for Interoperability of Intrusion Detection Responses Compatible with the IDWG Model. International Journal of Network Management, v. 17, p. 287-294, 2007.

# 4. Cloud Computing Security

## 4.1. Introduction (Motivation)

- Cloud computing is a new distributed computing and business paradigm.

- It provides computing power, software and storage and even a distributed data center infrastructure on demand.

- To make these characteristics viable, it makes use of existing technologies, such as virtualization, distributed computing, grid computing, utility computing and Internet.

# 4. Cloud Computing Security

## 4.1. Introduction (Objectives)

- We investigate what are the security problems involving this new paradigm, trying to obtain what are the main security problems cited in the available literature and, when possible, trying to point some directions in how to solve them.

# 4. Cloud Computing Security

4.1. Introduction (Some definitions)

- *"Cloud computing is an emerging computing paradigm. It aims to share data, calculations, and services transparently among users of a massive grid* [Mei, 2008]."

- *"'Cloud computing' is the next natural step in the evolution of on-demand information technology services and products. To a large extent cloud computing will be based on virtualized resources.(…) Cloud computing embraces cyber infrastructure and builds upon decades of research in virtualization, distributed computing, grid computing, utility computing, and more recently networking, web and software services* [Vouk, 2008]."

# 4. Cloud Computing Security

## 4.1. Introduction (Some definitions)

- “*A Cloud is a type of parallel and distributed system consisting of a collection of interconnected 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* [Buyya, 2008].”

- “*A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet* [Foster, 2008].”

# 4. Cloud Computing Security

## 4.1. Introduction (Some definitions)

- "(…) *cloud computing is a nascent business and technology concept with different meanings for different people. For application and IT users, it's IT as a service (ITaaS) - that is, delivery of computing, storage, and applications over the Internet from centralized data centers. For Internet application developers, it's an Internet-scale software development platform and runtime environment. For infrastructure providers and administrators, it's the massive, distributed data center infrastructure connected by IP networks* [Lin, 2009]."

# 4. Cloud Computing Security

## 4.1. Introduction (Organization)

- Section 4.2. discusses the Cloud Computing Types.

- Section 4.3. presents the Cloud Computing Security Overwiew.

# 4. Cloud Computing Security

## 4.2. Cloud Computing Types

- *Infrastructure as a Service (IaaS)*. Products in this case "deliver a full computer infrastructure via the Internet [Leavitt, 2009]."

- *Platform as a Service (PaaS)*. In this case, is offered "a full or partial application development environment that users can access and utilize online, even in collaboration with others [Leavitt, 2009]."

- *Software as a Service (SaaS).* In this case, is provided "a complete, turnkey application—including complex programs such as those for CRM or enterprise-resource management via the Internet [Leavitt, 2009]."

# 4. Cloud Computing Security

## 4.2. Cloud Computing Types

- Public: *in this model, resources are available to the general public over the Internet.*

- Private: *in this model, resources are accessible within a private organization.*

- Hybrid: *this model mixes the techniques from public and private clouds.*

# 4. Cloud Computing Security

## 4.3. Cloud Computing Security Overwiew

- **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?

# 4. Cloud Computing Security

## 4.3. Cloud Computing Security Overwiew

- **Privileged user access**: outsourcing means allowing outsourced services to bypass internal controls, including personnel controls.

- **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.

# 4. Cloud Computing Security

## 4.3. Cloud Computing Security Overwiew

- **Data location**: when using the cloud, the customer probably will not know where their data will be stored.

- **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.

# 4. Cloud Computing Security

## 4.3. Cloud Computing Security Overwiew

- **Recovery**: the provider capacity of restoring the entire system and how long it would take should be checked by the customer.

- **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.

# 4. Cloud Computing Security

## 4.3. Cloud Computing Security Overwiew

- **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.

- In a Tech News from forbes.com, published online in February 02, 2008, by Andy Greenberg is cited that when customers store their data in someone else's software and hardware, "they lose a degree of control over their often-sensitive information".

# 4. Cloud Computing Security

4.3. Cloud Computing Security Overwiew

*- Customers' Security Concerns X Security Functions related*

Customers' security concern

- Vulnerability to attack / data breaches
- Standard security practices / regulatory compliance
- Conformance to state or national data-storage / privacy laws
- Privileged user Access
- Data segregation
- Recovery
- Investigative support
- Long-term viability

# 4. Cloud Computing Security

4.3. Cloud Computing Security Overwiew

- *Customers' Security Concerns X Security Functions related*

Security function related

- Providing security to resources against malicious acts from cloud computing users, intrusion detection systems, viruses checking
- Information security standards, Sec-SLAs
- License agreements
- User authentication and authorization
- Cryptography
- Backup
- Intrusion detection systems
- Data format standards, backup

# 4. Cloud Computing Security

4.3. Cloud Computing Security Overwiew

*A. Intrusion detection systems*

- Some of the intrusion detection systems problem in cloud computing are the same as in other distributed environments, i.e., monitoring of several resources at once.

- In a cloud computing environment, these resources, at least most of the time, will not be constant or fixed. These resources can even be in different domains.

- So, an intrusion detection system for cloud computing needs to do the basics – to detect intruders, and also to deal with resources being deployed on demand and spanning multiple domains.

# 4. Cloud Computing Security

4.3. Cloud Computing Security Overwiew

*B. User authentication and authorization*

- Managing identities and their acesses is still a challenge for the IT community. In the cloud, the basic problems are the same: single sign-on, cross domain user account provisioning, cross domain user attribute exchange and so on.

- According to [www.cloudsecurityalliance.org], if an enterprise have their own federated identity management infrastructure then it will be more easy to have success in managing identities in the cloud. Otherwise, the enterprise will have sensitive internal identity information spread into several cloud providers. So, to have success in effectively managing identities in the cloud, it is necessary a robust federated identity management.

# 4. Cloud Computing Security

4.3. Cloud Computing Security Overwiew

*C. Cryptography*

- Cloud provider should have a detailed cryptographic plan, explaining what algorithms will be used, how the key management will be done, when encryption will be used and so on.

- The Cloud Security Alliance Guide provides some guidance. Cloud computing divorces components from location and this creates security issues that result from this lack of any perimeter. Hence there is only one way to secure the computing resources: strong encryption and scalable key management.

- Cloud customers and providers must encrypt all data in transit and also static data, since all communications and all storage may be visible to arbitrary outsiders.

# 4. Cloud Computing Security

## 4.3. Cloud Computing Security Overwiew

### *D. Backup*

- Backup is probably the more simple way of recovering data. However, being crucial to ensure that a point-in-time data is available to restore business operations and given the special nature of a cloud environment, some questions need to be clearly answered by the provider and understood by the customer: Who performs the backup? How frequent the backup is performed? Who is responsible for storing the backup? Which backup format is used? Is it dependent of a specific technology? Logical segregation of data is maintained through the backup execution?

# 4. Cloud Computing Security

4.3. Cloud Computing Security Overwiew

*E. Information security standards*

- The ISO/IEC 27000 Series refers to information security.

- There is also the ISO/IEC 13335 IT Security Management.

- ISO/IEC 15408 Series are the Common Criteria (CC) for Information Technology Security Evaluation.

- There are other non-ISO information security standards and methods, like the 800 Series from the National Institute of Standards and Technology (NIST), COBIT (Control Objectives for Information and related Technology), SAS 70 (Statement on Auditing Standards No. 70) and others.

- The cloud computing provider should have internationally recognized standards for which they are audited on a regular basis. These questions need to be answered: What certifications does the vendor maintain? Do they undergo regular audits?

- All the cited information security standards and methods certificate or validate the enterprise and provide a way to visualize how committed is the cloud provider with security practices.

# 4. Cloud Computing Security

4.3. Cloud Computing Security Overwiew

*F. Security Service Level Agreements or Sec-SLAs*

- According to the earlier referred white paper from Cloud Security Alliance, “Service Level Agreements focus upon availability of services and may not explain service quality, resolution times, critical success factors, key performance indicators, or offer any recourse to the user.”

- We believe that SLAs will play an important role in the security matters. We call these SLAs relating to security issues a Sec-SLA. A Security Service Level Agreement or just Sec-SLA is a specific SLA that deals with metrics related to security instead of the traditional telecommunication metrics such as throughput, delay, packet loss and others.

# 4. Cloud Computing Security

4.3. Cloud Computing Security Overwiew

*G. Data format standards*

- Specifically relating to cloud computing we do not know at the moment of this research any established data standard aiming to provide interoperability of application data between cloud providers.

- Some standardizations initiatives are in progress, like the Cloud Computing Effort announced on April 27, 2009 by DMTF (Distributed Management Task Force). It seems vital to have a data format that allows customers to take their data from one provider and leverage it inside another provider's application.

# 4. Cloud Computing Security

## 4.3. Cloud Computing Security Overwiew

*H. License agreements*

- Service Level Agreements main focus is characteristics related to the quality of service being delivered. When comes to conformance to state or national data-storage / privacy laws, other kinds of agreements are necessary.

- We believe that license agreements and other legal issues are greatly related to the legal area and the habitual interchange of expertise is needed. Actually, doing some research on Internet, we found out that some legal organizations like Strafford Publications are organizing events to work the subject, like a Teleconference entitled "Cloud Computing: Managing the Legal Risks", showing that other areas than just information technology is watching cloud computing growing adoption more closely.

# 4. Cloud Computing Security

## 4.4. Conclusions

- 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. So, much research work is in progress to provide security for cloud computing.

- The general believe, including ours, is that the larger adoption of cloud computing relies on how secure it will be and that this security should be addressed since the very beginning.

# 4. Cloud Computing Security

## 4.4. Conclusions

- 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.

- We also noticed that at this moment is difficult to answer all the security questions, as we intended during the introduction of this tutorial.

- As more deeply we go into the subject, more questions come to the surface. So, we can expect lots of research to answer every one of this questions and a promising research field.

# 4. Cloud Computing Security

## 4.4. References

- Lijun Mei, W.K. Chan, T.H. Tse.: A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues. In: 2008 Asia-Pacific Service Computing Conference, pp. 464-469, 2008.
- Vouk, M.A. : Cloud Computing – Issues, research and implementations. In: 30th International Conference on Information Technology Interfaces, pp. 31-40, 2008.
- Foster, I., Yong Zhao, Raicu, I., Lu, S.: Cloud Computing and Grid Computing 360-Degree Compared. In:  2008 Grid Computing Environments Workshop, p. 1-10, 2008.
- Geng Lin, David Fu, Jinzy Zhu, Glenn Dasmalchi, "Cloud Computing: IT as a Service," IT Professional, vol. 11, no. 2, pp. 10-13, Mar./Apr. 2009

# 4. Cloud Computing Security

## 4.4. References

- Buyya, R.; Chee Shin Yeo; Venugopal, S.; 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. IEEE Computer Society, 2008, pp.5-13.
- Leavitt, N.; Is Cloud Computing Really Ready for Prime Time?, Computer, vol. 42, no. 1, pp. 15-20, IEEE Computer Society, 2009.
- Security Guidance for Critical Areas of Focus in Cloud Computing, www.cloudsecurityalliance.org
- Henning, R. R.: Security Service Level Agreements: Quantifiable Security for the Enterprise? In: Proceedings of the workshop on New Security Paradigms, pp. 54–60. ACM, New York (1999).
- Zhen Hua Liu   Murthy, R.: A Decade of XML Data Management: An Industrial Experience Report from Oracle. In: IEEE 25th International Conference on Data Engineering, pp. 1351-1362. IEEE Computer Society, 2009

# 5. Final Considerations

Books in Cloud Computing

- Cloud Computing, A Practical Approach... By Toby Velte
- Cloud Application Architectures: Building Applica... by George Reese
- Cloud Security and Privacy: An Enterprise Perspecti... by Tim Mather
- Cloud Computing and SOA Convergence in Your... by David S.
- Cloud Computing For Dummies by Judith Hurwitz
- Cloud Computing Explained: Implementation Handbook... by John Rhoton
- Dot Cloud: The 21st Century Business Platform Bui... by Peter Fingar
- Cloud Computing: Implementation, Management,... by John Rittinghouse

# 5. Final Considerations

Books in Cloud Computing

- Software as a Service Inflection Point: Usi... by Melvin B. Greer Jr
- Cloud Computing: Web-Based Applications That Ch... by Michael Miller
- Cloud Computing with the Windows Azure Platform... by Roger Jennings
- Behind the Cloud: The Untold Story of How Salesfo... by Marc Benioff
- Beginning Linux Cloud Administration: Using Ub... by Sander van Vugt
- Cloud Computing Foundation Complete Certificatio... by Ivanka Menken
- Host Your Web Site On The Cloud: Amazon Web Services... by Jeff Barr
- Cloud Computing Best Practices for Managing and Me... by Haley Beard

# 5. Final Considerations

Call for Papers in Cloud Computing

- 1st IFIP/IEEE International Workshop on Cloud Management (CloudMan 2010) http://cloudman2010.lncc.br
- The 2nd International Workshop on Security in Cloud Computing. (SCC'2010)

http://bingweb.binghamton.edu/~ychen/SCC2010.htm

- International Workshop on Cloud Computing, Applications and Technologies. (CloudCAT 2010)

http://www.cs.thu.edu.tw/cloudcat2010

- 5th Workshop on Virtualization in High-Performance Cloud Computing VHPC'10 http://vhpc.org
- First International Workshop on Mobile Cloud Computing
- First International Conference on Cloud Computing

  www.cloudcomp.eu

# 5. Final Considerations

Call for Papers in Cloud Computing

- First International Workshop on Cognitive Wireless Cloud Networks 2009 (CogCloud'09) http://www.ieee-pimrc.org/index.html
- The First IEEE International Workshop on Emerging Applications for Cloud Computing http://compsac.cs.iastate.edu/workshop_details.php?id=23
- First ICDCS Workshop on Security and Privacy in Cloud Computing (ICDCS-SPCC 2010) http://www.ece.iit.edu/~ubisec/workshop.htm
- Mobile Cloud Computing Workshop http://sce.umkc.edu/mdm2010/workshops.html
- 2nd International Symposium on Cloud Computing (Cloud 2010) http://www.cloudbus.org/cloud2010/
- International Workshop of Software Architecture Principles for and with Cloud Computing (ArchiteCloud 2010) http://www.nicta.com.au/people/tosicv/architecloud2010

# 5. Final Considerations

Papers in Cloud Computing

- Resource management with hoses: point-to-cloud services for virtual private networks
- Cloud Security Issues
- Analysis of Energy Efficiency in Clouds
- Interfaces for Placement, Migration, and Monitoring of Virtual Machines in Federated Clouds
- SLA-Aware Virtual Resource Management for Cloud Infrastructures
- Ensuring data storage security in Cloud Computing
- An Active Trusted Model for Virtual Machine Systems

# 5. Final Considerations

Papers in Cloud Computing

- Cloud Computing: Distributed Internet Computing for IT and Scientific Research
- Digital Ecosystems in the Clouds: Towards Community Cloud Computing
- Overcast: Forensic Discovery in Cloud Environments
- A Declarative Language Framework for Cloud Computing Management
- Agent-based Cloud Commerce
- Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual MachinePerformance model driven QoS guarantees and optimization in clouds