Current Issues in Cloud Computing Security and Management

Pedro Artur Figueiredo Vitti, Daniel Ricardo dos Santos,
Carlos Becker Westphall, Carla Merkle Westphall, Kleber Magno Maciel Vieira
Network and Management Laboratory - Department of Informatics and Statistics
Federal University of Santa Catarina - Florianopolis, Santa Catarina, Brazil
{pvitti, danielrs, westphal, carlamw, kleber}@inf.ufsc.br

***Abstract*—Cloud computing is becoming increasingly more popular and telecommunications companies perceive the cloud as an alternative to their service deployment models, one that brings them new possibilities. But to ensure the successful use of this new model there are security and management challenges that still need to be faced. There are numerous threats and vulnerabilities that become more and more important as the use of the cloud increases, as well as concerns with stored data and its availability, confidentiality and integrity. This situation creates the need for monitoring tools and services, which provide a way for administrators to define and evaluate security metrics for their systems. In this paper, we propose a cloud computing security monitoring tool based on our previous works on both security and management for cloud computing.**

Keywords–cloud computing; security management; monitoring; security metrics

I. INTRODUCTION

Cloud computing is a new way to provide computational resources over the Internet in a transparent and easy manner. According to the National Institute of Standards and Technology (NIST), it is a model for enabling on-demand network access to a shared pool of computational resources, comprised of three service models and four deployment models [1].

These service models are: Software as a Service (SaaS), in which the service provided to the user is in the form of an application that runs on a cloud infrastructure; Platform as a Service (PaaS), in which the user can deploy its own applications in the provider's infrastructure; and Infrastructure as a Service (IaaS), in which the user has access to the computational resources themselves, in the form of virtual machines, storage, networks and others.

The deployment models are the private, community, public and hybrid cloud, and refer to the location of the cloud infrastructure, who has access to it and who is responsible for its management. The most used models are the public cloud, when the infrastructure is run by an organization and provisioned to be used by the public; and the private cloud, when an organization provisions its own infrastructure to be used by their business units.

In an era where telecommunication providers face ever greater competition and technology evolution, the basic features of cloud computing such as virtualization, multi-tenancy and ubiquitous access provide a viable solution to their service provisioning problems.

Telecoms are now using their own private clouds, or sometimes public clouds, to host their services and enjoy the benefits of this new model. With a multi-tenant cloud they can support an increasing number of subscribers and maintain the Quality of Experience of their services even when dealing with high demand. The use of the cloud also helps these companies transition from a product based business model to a service based one.

The main advantages of cloud computing are the reduction of IT costs and increased flexibility, scalability and the possibility to pay only for the used resources. The users of the cloud range from individuals to large government or commercial organizations, and each one has their own concerns and expectations about it.

Among these concerns, security and privacy are the biggest ones [2]. This comes from the fact that the data that belongs to users and organizations may no longer be under their absolute control, being now stored in third party locations and subject to their security policies, in the case of public clouds.

But even in private clouds, the most common case in telecom companies, there are new security challenges, such as providing access to an ever growing number of users while maintaining efficient and well monitored access control.

It becomes necessary to characterize what are the new risks associated with the cloud and what other risks become more critical. These risks must be evaluated and mitigated before the transition to the cloud.

It is already possible to find in the literature a lot of work being done in the security aspects of Cloud Computing, describing its challenges and vulnerabilities and even proposing some solutions [3].

In the rest of this paper, we provide some background in security concerns in cloud computing, briefly describe a previous implementation of a monitoring tool for the cloud, show how security information can be summarized and treated under a management perspective in an Service Level Agreement (SLA) and then propose a system for monitoring security information in the cloud.

In Section II, some works, related to security in cloud computing environments, are cited. In Section III, currently existing concerns in cloud computing security area are presented. In Section IV, an architecture for monitoring clouds is described. In Sections V and VI, safety concerns with SLA, and the definition of entities, components, metrics and, actions of security monitoring cloud computing are shown. Section VII shows the case study. In Section VIII, lessons learned from this work are described. Finally, in Section IX, a conclusion is presented and some future work proposals are made.

II. RELATED WORK

Uriarte and Westphall [4] proposed a monitoring architecture devised for private Cloud that focuses on providing data

 ISBN: 978-1-61208-376-6

analytics capabilities to a monitoring system and that considers the knowledge requirements of autonomic systems. While, argue that in the development of an analytical monitoring system for public Clouds, security, privacy and different policies need to be considered, their proposal does not consider specific security metrics and Sec-SLAS.

Fernades et al. [5] surveys the works on cloud security issues. Their work addresses several key topics, namely vulnerabilities, threats, and attacks, and proposes a taxonomy for their classification. Their work, however, does not consider metrics monitoring or any implementation details.

CSA [6] has identified the top nine cloud computing threats. The report shows a consensus among industry experts, focusing on threats specifically related to the distributed nature of cloud computing environments. Despite identifying, describing and analyzing these threats, their work does not consider the monitoring of security metrics related to the identified threats.

Murat et al. [7] proposed a cloud network security monitoring and response system, which is based on flow measurements and implements an algorithm that detects and responds to network anomalies inside a cloud infrastructure. Their proposal however does not take into account security metrics and Sec-SLAs, instead it generates and monitors profiles of network traffic to detect for anomalies, hence it is limited in the scope of security issues it can monitor.

III. Security Concerns in Cloud Computing

A. Technologies

A lot of different technologies are necessary to create and manage a cloud environment, according to the kind of service that this cloud will provide. Cloud computing relies heavily on virtualization and network infrastructure to support its elasticity. Technologies such as Web Services, Service Oriented Architecture (SOA), Representational State Transfer (REST) and Application Programming Interfaces (API) are employed to provide users with access to their cloud resources. Each of these technologies presents some kind of known vulnerability and possible new exploits in the cloud [8].

B. Challenges, Threats and Vulnerabilities

The usual three basic issues of security: availability, integrity and confidentiality are still fundamental in the cloud and remain a big challenge in this scenario. Each sector has its main concerns when it comes to the cloud. Industry services are mostly worried about availability, so that they keep providing services even during peaks of access, while academia may be more concerned with integrity and individual users usually care about the confidentiality of their data. But every security aspect must be considered together to achieve security as a whole in this scenario. Because of the multi-tenant characteristic of cloud computing, one single vulnerable service in a virtual machine may lead to the exploitation of many services hosted in the same physical machine. Also, virtualization has an inherent security threat that a user may escape its confined environment and gain access to the physical machine resources or to other virtual machines. This requires complex attacks, but is possible.

Web applications and web services have a long history of security vulnerabilities, and if not well implemented they are susceptible to a lot of easily deployed and very well-known attacks such as SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) and session hijacking.

Cryptography is the most important technology to provide data security in the cloud, but problematic implementations and weak proprietary algorithms have been known problems for a long time and are still exploited.

Another important topic in cloud security is Identity and Access Management, because now data owners and data providers are not in the same trusted domain. New mechanisms for authentication and authorization that consider cloud-specific aspects are needed and are being actively researched [9].

The main security management issues of a Cloud Service Provider (CSP) are: availability management, access control management, vulnerability management, patch and configuration management, countermeasures, and cloud usage and access monitoring [10].

To remain effective in this new paradigm, some security tools have to be adapted, such as Intrusion Detection Systems (IDS), which are critical to monitor and prevent incidents in the cloud. Because of its distributed nature, the cloud is an easy target for an intruder trying to use its abundant resources maliciously, and because of this nature, the IDS also has to be distributed, to be able to monitor each node [11].

C. Attacks

While the cloud serves many legitimate users, it may also host malicious users and services, such as spam networks, botnets and malware distribution channels. Cloud providers must be aware of those problems and implement the necessary countermeasures.

Besides that, Distributed Denial of Service (DDoS) attacks can have a much broader impact on the cloud, since now many services may be hosted in the same machine. When an attacker focuses on one service it may affect many others that have no relation with the main target. DDoS is a problem that is still not very well handled. On the other hand, since the cloud provides greater scalability and may allocate resources almost instantaneously it becomes more resilient to denial of service, but it comes with a cost to the users.

D. Data Security

The security and privacy of the data stored in the cloud is, perhaps, the most important challenge in cloud security. To maintain data security a provider must include, at least: an encryption schema, an access control system, and a backup plan [12].

However, data encryption can be a hindrance in the cloud because of the current impossibility to efficiently process or query over encrypted data [2]. There is active research in these areas, with techniques such as Searchable Encryption and Fully Homomorphic Encryption, but their applications are still limited and they cannot yet be used in large scale environments.

When moving to the cloud it is important that a prospective customer knows to what risks its data are being exposed. Some of the key points a user must consider in this migration are [13]: The cloud administrators will have privileged access to user data, and possibly bypass access controls; The provider must comply to legal requirements, depending on the kind of data the user intends to store; The location of the user's data may now be unknown to them; How the data of one user are kept separate from others; The provider must have a capacity to restore a system and recover its data through backup and replication; The provider must formally ensure full support in

 ISBN: 978-1-61208-376-6

the case of an investigation over inappropriate activities; and The data must be in a standardized format and be available to the user even in the case the provider goes out of business.

E. Legal Compliance

Legal compliance is fundamental when dealing with cloud computing. In the cloud world, it is possible that data cross many jurisdiction borders and have to be treated in compliance to many different laws and regulations. This is one of the reasons why security plays such an important role in cloud adoption and development, especially for the CSPs.

To achieve compliance both providers and users must be held responsible for how data is collected, stored and transmitted, especially sensitive data, such as Personally Identifiable Information (PII).

Among the most important tools to ensure legal compliance are external audits and security certifications.

F. Telecommunications

The deployment and provisioning of telecommunication services becomes easier in the cloud, and it empowers telecom providers with greater scalability and flexibility. Those advantages, however, come with the cost of new security challenges.

Security plays such a vital role in telecommunications that many telecommunication networks are built from the ground-up with security requirements in mind. This, however, is not true for many Internet protocols. When transitioning to the cloud, telecom providers must be aware that their services are being deployed in a different scenario, one that has to be well understood before this transition is considered.

Availability, for instance, is critical to the telecom business and if services are being deployed in a public cloud without a proper SLA, server downtime will cause a lot of trouble. Confidentiality is also fundamental, since telecoms collect and store a lot of data from their clients, from personal data to information about their communications.

IV. Cloud Monitoring

The provisioning of cloud services represents a challenge to service monitoring. It requires complex procedures to be well accomplished, which leads to the development of new management tools. Our team has previously proposed and implemented an open-source cloud monitoring architecture and tool called the Private Cloud Monitoring System (PCMONS) [14].

The architecture of the system is divided in three layers (see Figure 1):

- Infrastructure - Consists of basic facilities, services and installations and available software, such as operating systems and hypervisors;
- Integration - Responsible for abstracting the infrastructure details for the view layer; and
- View - The interface through which information is analyzed.

The main components of the architecture are (see Figure 1):

- Node information gatherer: Gathers local information on a node;
- VM monitor - Injects scripts into the virtual machine (VM) that send data to the monitoring system;
- Configuration Generator - Generates the configuration files for the tools in the view layer;
- Monitoring tool server - Receives data form different resources and take actions such as storing it;
- Database - Stores data needed by the Configuration Generator and the Monitoring Data Integrator.

V. Security Concerns in SLA

Security is not only a matter of preventing attacks and protecting data, it also has to be considered in a management perspective. Providers must have ways to ensure their clients that their data is safe and must do so by monitoring and enhancing security metrics.

A SLA formally defines the level of service a provider must guarantee. SLAs are a fundamental part of network management, and are also applied in cloud computing. They are defined in terms of metrics that must be monitored to ensure that the desired levels of service are reached.

SLAs may also be used in the definition, monitoring and evaluation of security metrics, in the form of Security SLAs, or Sec-SLAs [15]. In this case, the SLA considers security service levels.

To accomplish this, the first step is to define a set of security metrics, which in itself is not easy. Though there is not a definitive set of security metrics that is considered relevant in every case, researchers tend to use or adapt concepts gathered from international standards such as ISO 27002. Some issues that are usually considered are cryptography, packet filtering, redundancy, availability, and backup.

VI. Cloud Security Monitoring

Security monitoring is inherently hard, because the agent-manager approach normally used in the monitoring of other kinds of SLA, does not fit easily to every security characteristic [15].

Cloud computing has been evolving for many years and so, only now we are able to have a broader view of what exactly it is and hence what are its security requirements, based on recent definitions and publications.

With this new perspective it is now possible to define good security metrics that can be used to provide a clear view of the level of security being employed in a CSP and its virtual machines.

We now propose an extension to the PCMONS architecture and tool to enable security monitoring for cloud computing. We also present the security metrics which we consider adequate to be monitored in a cloud infrastructure and which provide a good picture of security as a whole in this environment.

The tool uses data and logs gathered from security software available in the monitored systems, such as IDSs, anti-malware software, file system integrity verification software, backup software and web application firewalls, and presents these data to the cloud administrators.

Besides providing to administrators reliable metrics and information about the security of their systems, this monitoring architecture can also be used in the auditing and outsourcing of security services.

The main components of the proposal can be seen in Figure 1 and are described below.

A. Entities

The entities involved in the definition, configuration and administration of the security SLAs and metrics are:

- Cloud users - The users of the cloud infrastructure. They negotiate the SLAs with the CSP and expect

 ISBN: 978-1-61208-376-6

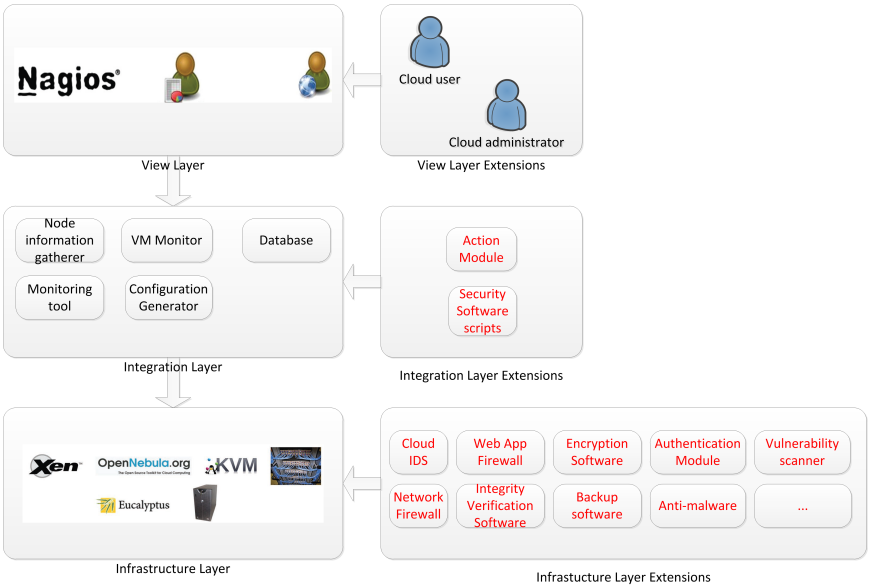

Figure 1. Three Layers Monitoring Architecture

them to be accomplished;
- Cloud administrators - The administrators of the CSP. Their role is to monitor the cloud infrastructure; and
- Security applications - The applications which produce the security information that will be gathered.

The two first entities were a part of the previous PCMONS, while the third one was inserted in our extension.

B. Components

Since PCMONS is modular and extensible, the components used in the new architecture are the same already available, but with extensions that allow the monitoring of security metrics.

The extensions are new scripts to gather the security data from the many sources needed and an extension to the visualization tool to show this data.

C. Metrics

As mentioned in Section IV, the definition of security metrics is not an easy task, and it becomes even harder in the cloud.

Here, we present the basic metrics we intended to monitor. These metrics were chosen because we consider they cover a great part of what was considered critical in a cloud provider, based on the survey presented in Section II.

We divided the set of metrics into subsets related to each security aspect that will be treated. There are four subsets of metrics. The first three are related to each individual virtual machine. Data Security Metrics, Access Control Metrics and Server Security Metrics are shown in Table I, Table II, and Table III, respectively.

D. Actions

We decided to introduce a new module to take actions based on the monitored metrics and possible violations to the Sec-SLA. As an example, if a virtual machine has had a huge number of failed access attempts in the last hours we may want to lock any further access to it and communicate the possible issue to the administrator of that machine. Also, if malware was detected on a machine we may want to shut it down to prevent it from infecting other VMs in the same physical machine. These actions will be predefined scripts available to cloud administrators and may be enabled or disabled by them at any time.

VII. Case Study

We have implemented the metrics presented in Tables I-III and gathered the data generated in a case study. The implementation of the data gathering scripts was done in Python and the data shown in the Nagios interface.

Our infrastructure consisted of two physical servers, one hosting the OpenNebula cloud platform and another hosting the virtual machine instances.

Several virtual machines running the Ubuntu operating system and the security software needed to provide the security metrics were instantiated. The following software were used to gather the security information: dm-crypt (encryption), rsync (backup), tripwire (filesystem integrity), ssh (remote access), clamAV (anti-malware), tiger (vulnerability assessment) and uptime (availability).

The VMs were automatically attacked by brute force login attempts and malware being downloaded and executed, as well as access attempts to ports blocked by the firewall. During the tests there were also simulations of regular usage, encompassing valid accesses and simple user tasks performed on the machines, such as creating and deleting files. The malware scans, vulnerability scans, integrity checks and backups were performed as scheduled tasks on the operating system using latest versions of Linux Malware Detect [16], OpenVAS [17], AFICK [18] and, Amanda [19] respectively. We did not stress the environment to test for scalability issues because it had already been done with the previous versions of PCMONS.

Figure 2 shows an example of an early snapshot of the monitoring environment. It represents how the metrics are shown in Nagios and it is possible to see the vision that a network administrator has of a single machine. The metrics HTTP_CONNECTIONS, LOAD, PING, RAM and SSH are from the previous version of PCMONS and are not strictly related to security, but they are show combined.

 ISBN: 978-1-61208-376-6

TABLE I. DATA SECURITY METRICS

Metric	Description
Encrypted Data?	Indicates whether the data stored in the VM is encrypted
Encryption Algorithm	The algorithm used in the encryption/decryption process
Last backup	The date and time when the last backup was performed
Last integrity check	The date and time when the last file system integrity check was performed

TABLE II. ACCESS CONTROL METRICS

Metric	Description
Valid Accesses	The number of valid access attempts in the last 24 hours
Failed access attempts	The number of failed access attempts in the last 24 hours
Password change interval	The frequency with which users must change passwords in the VM's operating system

TABLE III. SERVER SECURITY METRICS

Metric	Description
Malware	Number of malware detected in the last anti-malware scan
Last malware scan	The date and time of the last malware scan in the VM
Vulnerabilities	Number of vulnerabilities found in the last scan
Last vulnerability scan	The date and time of the last vulnerability scan in the VM
Availability	Percentage of the time in which the VM is online

It is important to notice that the accuracy of the obtained information depends on the security software being monitored. Our solution aggregates these data to present it in a way that is more clear and easy to monitor. The tool helps network and security administrator perceive violations to Sec-SLAs and actively respond to threats.

In this case study, considering the automatic attacks previously described, the most violated metrics were the failed access attempts and the anti-malware events, as well as availability, because of malware that would cause denial of service.

Since we obtained a high number of violations in an environment that was supposed to be under constant attack, it suggests that the chosen metrics are good indicators of overall security for the virtual machines.

VIII. KEY LESSONS LEARNED

A. Background

Monitoring and managing security aspects remains a challenge that has to be faced to enable the full potential of the cloud and only now, with a recent agreed upon definition of exactly what is cloud computing, this can be achieved. The major piece of technology used to provide security in the cloud is cryptography.

Data leakage and data loss are possibly the greatest concerns of cloud users. If the CSP acts unfaithfully the users may not even become aware of incidents that compromise their data. There must be ways to verify data integrity, so that users are certain their data were not corrupted. Backup and recovery are also fundamental tools to ensure the availability of customer data.

The greatest challenge to security monitoring in a cloud environment is the fact that the cloud provides services on demand, creating a highly dynamic and flexible system to which the metrics have to be adapted.

SLAs are fundamental to provide customers with the needed guarantees that the service they are hiring will be adequately provided, their machines will be secure and their data will be securely stored, transmitted and processed.

Security metrics and a more quantitative approach to security, in both the definition of requirements and their monitoring, remain an important open research topic.

There are other important security metrics that are related to the security processes of the CSP, such as employee training, physical security and contingency plans. These were not taken into account in this work because they cannot be automatically gathered and monitored.

B. Design and Implementation

The design of a software project and related architectural decisions may consume a great time before the implementation is even started. Building an extension over a previous architecture, as was our case, may greatly reduce this time.

Nevertheless, many important decisions have to be made to achieve a final functioning software. The major decisions in this case were related to the security metrics and the software used to provide the necessary security data.

As already stated in this paper, defining and quantifying security is no easy task, therefore it was the most time consuming aspect of the project. Trying to come up with a simple set of metrics that represent the state of security of a whole cloud not only seems, but definitely is a daunting task.

Something that became clear with this implementation is that no single set of metrics can embrace every security need, and so to define the metrics we based our approach on the common security issues described in the literature, as well as issues that are consistently cited as the most critical by industry users. It is also important to note that the definition and monitoring of metrics must be flexible enough to accommodate different potential uses of the software.

After defining what is going to be measured it is necessary

 ISBN: 978-1-61208-376-6

oneadmin i-322 stratus	AVAILABILITY	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	99.93%
	CIPHER	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	AES
	SSH_VALID	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	25
	IS_ENCRYPTED	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	yes
	LAST_BACKUP	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	2014-08-14 18:30:48
	LAST_INTEGRITY	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	2014-08-14 10:23:50
	LAST_MALWARE_SCAN	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	2014-08-14 10:02:42
	VULNERABILITIES	CRITICAL	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	111
	MALWARE_FOUND	CRITICAL	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	5
	PASSWORD_INTERVAL	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	180 days
	SSH_FAIL	WARNING	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	545

Figure 2. Nagios simplified interface of the monitored cloud services

to focus on how to do it. The idea of analyzing logs to obtain security data is classical in information security and it seemed like a natural approach to our challenge.

To read, parse and present the data we chose to use the Python programming language because it already formed the base of PCMONS and it fits very well these kinds of tasks.

An important aspect of the proposed solution is its modularity. Because of this feature we were able to introduce the new metrics and adapt it to our needs without changing anything that was already done in terms of basic monitoring. We believe the same can be achieved anytime it becomes necessary to adapt the software to new particular monitoring needs.

Modularity and extensibility are necessary approaches when you deal with such dynamic and highly scalable environments, because you have to be certain that you will be able to adjust the software to your future needs, which may be very different from current ones. The most challenging metrics in terms of implementation were those that gathered data from non-standard security software, such as tripwire, because we had to understand the data they generated to interface them with PCMONS. The analysis of our results shows that PCMONS was able to comply with our defined set of metrics, since their implementation relied on established security software, and that the definition and implementation of new metrics may be done in the future without the need for a great architectural redesign.

C. Testing Environment

Setting up a reliable testing environment was also extremely important to the success of the project. Setting up a private cloud is often advertised as being simple and convenient, but that is not always true when we have to deal with specificities of architectures, operating systems and hypervisors.

Our private cloud has been evolving for some years and through the realization of other projects we were able to gather experience on deploying, managing and monitoring it, which allowed us to choose tools we already knew would work well together.

Since the whole cloud infrastructure is built upon a piece of software, it is important to know that it is stable, reliable, well documented and provides available support. Our choice for the OpenNebula platform came from previous experience with it and its widespread use by many big players in the industry, such as Telefonica, Akamai and IBM.

An important feature of this extension of PCMONS is that it can run over Eucalyptus, OpenNebula and OpenStack, monitoring virtual machines in every platform. The support for different cloud platforms reflects the evolution of cloud tools and a greater effort being made in terms of standardization, interoperability and portability, all of which are big issues in cloud computing.

The use of scripting languages in the development process, such as Python and Bash Script allowed us to define the metrics, implement and test them on the fly on the testing environment, without needing to stop services, compile software, test it, compile it again and so on. This approach required less intensive use of the testing environment during development and accelerated the whole process.

IX. Conclusion and Future Work

This paper described a few of our previous works in the field of Cloud Computing and how to bring them all together in order to develop a cloud security monitoring architecture.

The use of cloud computing is a great option for telecommunications companies that want to reduce OPEX and CAPEX costs and still improve their service provisioning. Security, nevertheless, must be accurately planned and monitored to ensure that the transition to the cloud runs smoothly.

The paper described the design and implementation of a cloud security monitoring tool, and how it can gather data from many security sources inside VMs and the network in which the physical machines are to give administrators a clear view of the security of their systems and allow Cloud Service Providers to give users guarantees about the security of their machines and data.

Currently, there are not many solutions to cloud security monitoring, and this paper shows it is possible to build such a system based on previous work.

As future work, we can point to the definition and implementation of new metrics and a better integration with existing Security SLAs, planning to include a new module to treat possible actions to be taken in response to metric violations, such as locking a virtual machine or shutting it down.

Also, it would be important to study the integration of the

 ISBN: 978-1-61208-376-6

security monitoring model with other active research fields in cloud security, such as Identity and Access Management and Intrusion Detection Systems.

ACKNOWLEDGEMENT

We would like to thank Salvatore Loreto, Saverio Niccolini and Vijay Gurbani for their prior review and for their help in improving the paper.

REFERENCES

[1] P. Mell and T. Grance, The nist definition of cloud computing. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (2011) [retrieved: Sept, 2014]

[2] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," Internet Computing, IEEE, vol. 16, no. 1, jan.-feb. 2012, pp. 69 –73.

[3] F. Shaikh and S. Haider, "Security threats in cloud computing," in Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, 2011, pp. 214–219.

[4] R. B. Uriarte and C. B. Westphall, "Panoptes: A monitoring architecture and framework for supporting autonomic clouds," in Network Operations and Management Symposium (NOMS), 2014 IEEE. IEEE, 2014, pp. 1–5.

[5] D. Fernandes, L. Soares, J. Gomes, M. Freire, and P. Incio, "Security issues in cloud environments: a survey," International Journal of Information Security, vol. 13, no. 2, 2014, pp. 113–170. [Online]. Available: http://dx.doi.org/10.1007/s10207-013-0208-7 [retrieved: Sept, 2014]

[6] T. T. W. Group et al., "The notorious nine: cloud computing top threats in 2013," Cloud Security Alliance, 2013.

[7] M. Mukhtarov, N. Miloslavskaya, and A. Tolstoy, "Cloud network security monitoring and response system," vol. 8, no. Special Issue on Cloud Computing and Services. sai: itssa.0008.2012.020 ITSSA, 2012, pp. 71–83.

[8] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," Security Privacy, IEEE, vol. 9, no. 2, march-april 2011, pp. 50 –57.

[9] X. Tan and B. Ai, "The issues of cloud computing security in high-speed railway," in Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on, vol. 8, 2011, pp. 4358–4363.

[10] F. Sabahi, "Cloud computing security threats and responses," in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, 2011, pp. 245–249.

[11] K. Vieira, A. Schulter, C. Westphall, and C. Westphall, "Intrusion detection for grid and cloud computing," IT Professional, vol. 12, no. 4, 2010, pp. 38–43.

[12] L. Kaufman, "Data security in the world of cloud computing," Security Privacy, IEEE, vol. 7, no. 4, 2009, pp. 61–64.

[13] S. Chaves, C. Westphall, C. Westphall, and G. Geronimo, "Customer security concerns in cloud computing," in ICN 2011, The Tenth International Conference on Networks, 2011, pp. 7–11.

[14] S. De Chaves, R. Uriarte, and C. Westphall, "Toward an architecture for monitoring private clouds," Communications Magazine, IEEE, vol. 49, no. 12, 2011, pp. 130–137.

[15] S. de Chaves, C. Westphall, and F. Lamin, "Sla perspective in security management for cloud computing," in Networking and Services (ICNS), 2010 Sixth International Conference on, 2010, pp. 212–217.

[16] R. M. Ryan MacDonald, Linux malware detect. [Online]. Available: https://www.rfxn.com/projects/linux-malware-detect/ (2014) [retrieved: Sept, 2014]

[17] R. Deraison, Open vulnerability assessment system. [Online]. Available: http://http://www.openvas.org/ (2014) [retrieved: Sept, 2014]

[18] E. Gerbier, Another file integrity checker. [Online]. Available: http://afick.sourceforge.net/ (2014) [retrieved: Sept, 2014]

[19] J. da Silva, Advanced maryland automatic network disk archiver. [Online]. Available: http://http://www.amanda.org/ (2014) [retrieved: Sept, 2014]

[20] D. dos Santos, C. Merkle Westphall, and C. Becker Westphall, "A dynamic risk-based access control architecture for cloud computing," in Network Operations and Management Symposium (NOMS), 2014 IEEE, May 2014, pp. 1–9.

[21] P. Silva, C. Westphall, C. Westphall, M. Mattos, and D. Santos, "An architecture for risk analysis in cloud," in ICNS 2014, The Tenth International Conference on Networking and Services, 2014, pp. 29–33.

 ISBN: 978-1-61208-376-6