2011 Third IEEE International Conference on Coud Computing Technology and Science

A quantitative analysis of current security concerns and solutions for cloud computing

Nelson Gonzalez*, Charles Miers*‡, Fernando Redígolo*, Tereza Carvalho*, Marcos Simplicio*,
Mats Näslund† and Makan Pourzandi†
*Escola Politécnica at the University of São Paulo (EPUSP), São Paulo, Brazil
e-mail: {nmimura,cmiers,fernando, mjunior, carvalho}@larc.usp.br
‡University of Santa Catarina – Joinville, Brazil
†Ericsson Research – Stockholm, Sweden / Ville Mont-Royal, Canada
e-mail: {mats.naslund,makan.pourzandi}@ericsson.com

***Abstract*—The development of cloud computing services is speeding up the rate in which the organizations outsource their computational services or sell their idle computational resources. Even though migrating to the cloud remains a tempting trend from a financial perspective, there are several other aspects that must be taken into account by companies before they decide to do so. One of the most important aspect refers to security: while some cloud computing security issues are inherited from the solutions adopted to create such services, many new security questions that are particular to these solutions also arise, including those related to how the services are organized and which kind of service/data can be placed in the cloud. Aiming to give a better understanding of this complex scenario, in this article we identify and classify the main security concerns and solutions in cloud computing, and propose a taxonomy of security in cloud computing, giving an overview of the current status of security in this emerging technology.**

I. Introduction

Security is considered a key feature for cloud computing consolidation as a robust and feasible multi-purpose solution [1]. This viewpoint is shared by many distinct groups, such as academia researchers [2], business decision makers [3] and government organizations [4], [5]. The many similarities in these perspectives indicate a grave concern on crucial security and legal obstacles for cloud computing, including service availability, data confidentiality, provider lock-in and reputation fate sharing [6]. These concerns include not only existing problems, directly inherited from the adopted technologies, but also new issues derived from the composition of essential cloud computing features like scalability, resource sharing and virtualization (e.g., data leakage and hypervisor vulnerabilities) [7]. The distinction between these classes is more easily identifiable by analyzing the definition of the essential cloud computing characteristics proposed by the NIST in [8], which also introduces the SPI model for services (SaaS, PaaS, and IaaS) and deployment (private, public, community and hybrid).

Due to the ever growing interest in cloud computing, there is an explicit and constant effort to evaluate the current trends in security for such technology, considering both problems already identified and possible solutions. An authoritative reference in the area is the risk assessment developed by ENISA (European Network and Information Security Agency) [4]. Not only does it list risks and vulnerabilities, but it also offers a survey of related works and research recommendations. A similarly work is the security guidance provided by the Cloud Security Alliance (CSA) [5], which defines security domains congregating specific functional aspects, from governance and compliance to virtualization and identity management. Both documents present a plethora of security concerns, best practices and recommendations regarding all types of services in NIST's SPI model, as well as possible problems related to cloud computing, encompassing from data privacy to infrastructural configuration. Albeit valuable, these studies do not focus on quantifying their observations, something important for developing a comprehensive understanding of the challenges still undermining the potential of cloud computing.

The main goal of this article is to identify, classify, organize and quantify the main security concerns and solutions associated to cloud computing, helping in the task of pinpointing secure concerns that still lack a solution. Aiming to organize this information into a useful tool for comparing, relating and classifying already identified concerns and solutions, as well as future ones, we also present a taxonomy proposal for cloud computing security. We focus on issues that are specific to cloud computing, but without losing sight of important concerns that also exist in other distributed systems.

The rest of this document is organized as follows. Section II builds on several references to describe and group key aspects related to cloud computing security. The groups built in this manner are used in section III for the construction of the proposed taxonomy of cloud computing security. Section IV then leverages on these concepts for identifying and organizing the relationships between concerns and solutions in cloud security. Section V discusses how some representative cloud computing scenarios could benefit from the adoption of security solutions. Section VI covers the related work. Finally, section VII presents our considerations and future work.

II. Cloud computing security

Aiming to organize the data related to cloud security and to facilitate further studies, in this section we identify the main problems in the area and group them into a model composed of seven categories: network security, interfaces, data security, virtualization, governance, compliance and legal issues.

978-0-7695-4622-3/11 $26.00 © 2011 IEEE
DOI 10.1109/CloudCom.2011.39

IEEE computer society

Several key references were employed to gather the information required for building these categories, including CSA's security guidance [5] and top threats analysis [9], ENISA's security assessment [4] and the cloud computing definitions from NIST [8]. Emphasis is given on the distinction between services in software (SaaS), platform (PaaS) and infrastructure (IaaS), which are commonly used as the fundamental basis for cloud service classification.

Each category includes several potential security problems, resulting in the classification with subdivisions that highlight the main issues identified by the aforementioned references:

1) Network security: Problems associated with network communications and configurations regarding cloud computing infrastructures. The ideal network security solution is having cloud services as an extension of customer's existing internal networks [10], adopting the same protection measures and security precautions that are locally implemented and allowing to extend local strategies to any remote resources or processes.
    a) Transfer security: Distributed architectures, massive resource sharing and virtual machine (VM) instances synchronization imply more data in transit in the cloud, thus requiring VPN mechanisms for protecting the system against sniffing, spoofing, man-in-the-middle and side-channel attacks.
    b) Firewalling: Firewalls protect the provider's internal cloud infrastructure against insiders and outsiders [11] and enable VM isolation, fine-grained filtering for addresses and ports, prevention of Denial-of-Service (DoS) and detection of external security assessment procedures. Efforts for developing consistent firewall and other security measures specific for cloud environments [12], [13] reveals the urge for adapting existing solutions for this new computing paradigm.
    c) Security configuration: Configuration of protocols, systems and technologies to provide required levels of security and privacy without compromising performance or efficiency.
2) Interfaces: Concentrates all issues related to user, administrative and programming interfaces for using and controlling clouds.
    a) API: Programming interfaces (essential to IaaS and PaaS) to access virtualized resources and systems must be protected in order to prevent malicious use [14], [15], [16], [17], [18].
    b) Administrative interface: Enables remote control of resources in an IaaS (VM management), development for PaaS (coding, deploying, testing) and application tools for SaaS (user access control, configurations).
    c) User interface: End-user interface for exploring provided resources and tools (the service itself), implying the need of adopting measures for securing the environment [19], [20], [21], [22].
    d) Authentication: Mechanisms required to enable access to the cloud. Most services rely on regular accounts [15], [23], [24] consequently being susceptible to a plethora of attacks [25], [26], [27], [28], [29]. The consequences are boosted by multitenancy and resource sharing.
3) Data security: Protection of data in terms of confidentiality, availability and integrity (which can be applied not only to cloud environments, but any solution which requires basic security levels).
    a) Cryptography: Most employed practice to secure sensitive data [30], thoroughly required by industry, state and federal regulations.
    b) Redundancy: Essential to avoid data loss. Most business models rely on information technology for its core functionalities and processes [31], [32] and, thus, mission-critical data integrity and availability must be ensured.
    c) Disposal: Elementary data disposal techniques are insufficient and commonly referred as deletion [33].In the cloud, the complete destruction of data, including log references and hidden backup registries, is an important requirement [34].
4) Virtualization: Isolation between VMs, hypervisor vulnerabilities and other problems associated to the use of virtualization technologies [35].
    a) Isolation: Even though logically isolated, all VMs share the same hardware and consequently the same resources, allowing the exploit of data leaks and cross-VM attacks. The concept of isolation can also be applied to more fine-grained assets, such as computational resources, storage and memory.
    b) Hypervisor vulnerabilities: The hypervisor is the main software component of virtualization. Even though there are known security vulnerabilities for hypervisors, solutions are still scarce and often proprietary, demanding further studies to harden these security aspects.
5) Governance: Issues related to (losing) administrative and security controls in cloud computing solutions.
    a) Data control: Moving data to the cloud means losing control over redundancy, location, file systems and other relevant configurations [36].
    b) Security control: Loss of governance over security mechanisms and policies, as terms of use prohibit customer-side vulnerability assessment and penetration tests while insufficient Service Level Agreements (SLA) lead to security gaps.
    c) Lock-in: User potential dependency on a particular service provider due to lack of well-established standards (protocols and data formats), consequently becoming particularly vulnerable to migrations and service termination.
6) Compliance: Category which includes requirements related to service availability and audit capabilities [37].

a) Service Level Agreements (SLA): Mechanisms to ensure the required service availability and the basic security procedures to be adopted.
b) Loss of service: Service outages are not exclusive to cloud environments but are more serious in this context due to interconnections between services (a SaaS using virtualized infrastructures provided by an IaaS), as shown in many examples [38], [39], [40]. Thus it is required strong disaster recovery policies and provider recommendations to implement customer-side redundancy if applicable.
c) Audit: Enables security and availability assessments to be performed by customers, providers and third-party participants. Transparent and efficient methodologies are necessary for continuously analyzing service conditions [41] and are usually required by contracts or legal regulations. There are solutions being developed to address this problem by offering a transparent API for automated auditing and other useful functionalities [42].

7) Legal issues: Juridical concerns related to new concepts introduced by cloud computing [43], such as multiple data locations and privilege management.
a) Data location: Customer data held in multiple jurisdictions depending on geographic location [44], therefore being affected, directly or indirectly, by subpoena law-enforcement measures.
b) E-discovery: As a result of a law-enforcement measure, hardware might be confiscated for investigations related to a particular customer, affecting all customers whose data were stored in the same hardware [45], [46], [47]. Data disclosure is critical in this case.
c) Provider privilege: Malicious activities of provider insiders are potential threats to confidentiality, availability and integrity of customers' data and processes' information [48], [49].

III. Cloud computing security taxonomy

The analysis of security concerns in the context of cloud computing solutions shows that each issue brings different impacts on distinct assets. Aiming to create a security model both for studying security aspects in this context and for supporting decision making, in this section we consider the risks and vulnerabilities previously presented and arrange them in hierarchical categories, thus creating a cloud security taxonomy. The main structure of the proposed taxonomy, along with its first classification levels, are depicted in figure 1.

Figure 1. Cloud computing security taxonomy

The three first groups correspond to fundamental (and often related) security principles [6, Chapters 3-8].

The *architecture* dimension is subdivided into network configuration, hosts and virtualization issues, as well as dedicated applications and services, data security and storage concerns (whether it is in transit, at rest, being processed or being disposed), and management of security, identities and access. This organization is depicted in figure 2.

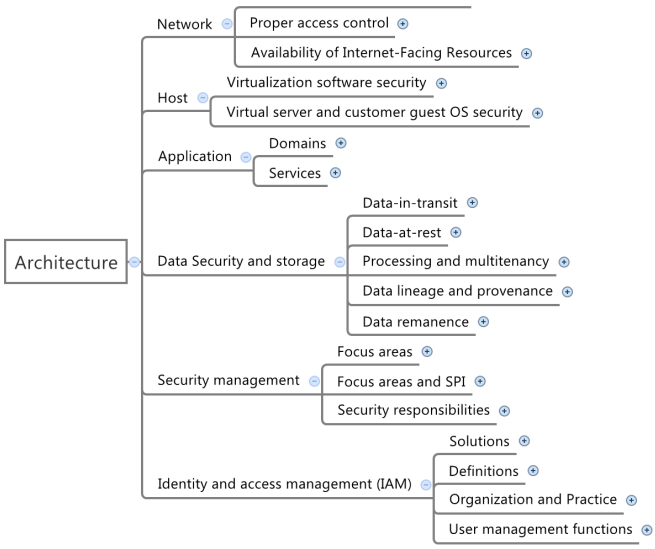

Figure 2. Security taxonomy - architecture

The architecture group allows a clearer division of responsibilities between providers and customers, and also an analysis of their security roles depending on the type of service offered (Software, Platform or Infrastructure).

The *compliance* dimension introduces administrative and legal responsibilities of the provider toward the offering of cloud services. In this case the categories proposed are based on the service lifecycle (from its definition to its operation and monitoring) and on governance, risk and compliance directives (e.g., how risk is assessed and which are the key controls for monitoring and reporting). The complete scenario is presented in figure 3.

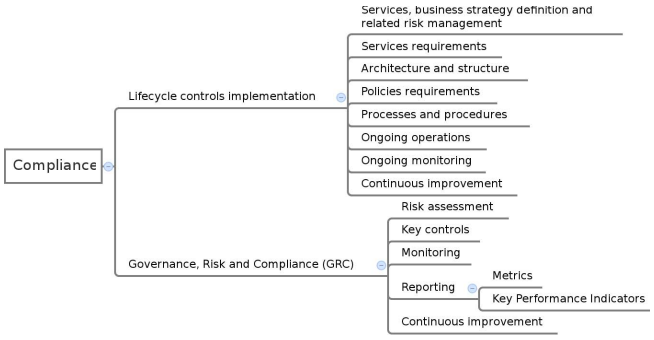

Figure 3. Security taxonomy - compliance

The *privacy* dimension is initially divided into concerns and principles. The former congregates issues related to privacy while generating, using, transferring, transforming, storing, archiving, destroying and auditing data. The latter covers best practices and common principles to ensure data privacy, including any personally identifiable information (PII). The expansion of this group is represented in figure 4.

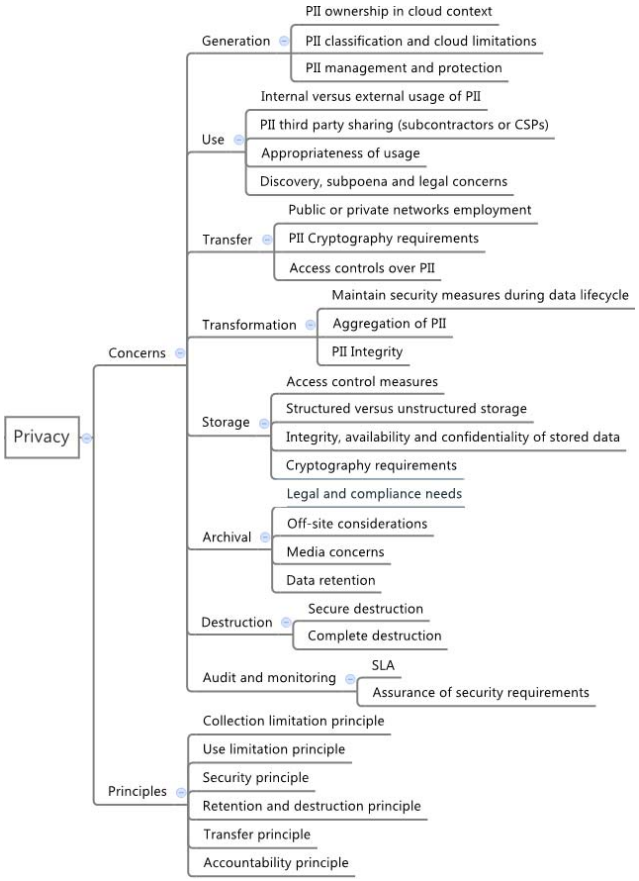

Figure 4. Security taxonomy - privacy

Figure 4 displays an evident attention to PII as it represents customer sensitive information. We note that the concerns in this dimension cover the complete information lifecycle (i.e., *generation, use, transfer, transformation, storage, archival,* and *destruction*) inside the provider perimeter and in its immediate boundaries (or interfaces) to the users. *Audit and monitoring* are also important aspects due to the requirements that cloud provider should ensure in order to fulfill service agreements with its customers.

A common point between all groups is the intrinsic connection to data and service lifecycles. Both privacy and compliance must be ensured through all states of data, including application information or customer assets, while security in this case is more oriented to how the underlying elements such as infrastructural hardware and software are protected.

IV. Current status of cloud security

A clear perspective of the main security problems regarding cloud computing and on how they can be organized to ease decision making is the primary step for having a comprehensive overview of the current status of cloud security. In this section, we analyze industry and academia viewpoints focusing on strategic study areas that need to be further developed. This study is based on more than two hundred different references including white papers, technical reports, scientific papers and other relevant publications. They were analyzed in terms of security problems and solutions by evaluating the number of citations for each case.

We used a quantitative approach to identify the amount of references related to each category of concerns or solutions. Our goal is not to determine if the presented solutions completely solve an identified concern, since most of the referenced authors agree that this is a hard task. Nonetheless, we identify the number of references dealing with each concern, providing some insight on which are the concerns that have received more attention from the research community and which have not been so extensively analyzed. Some observations about the analysis method:

1) The references consulted come from different research segments, including academia, organizations, and companies. Due to the article's length limitations, we did not include all the consulted references in the References Section. In the following we present some of the main sources of consultation:
   a) Academia: conference papers and journals published by IEEE, ACM, Springer, Webscience, and Scipress.
   b) Organizations: reports, white papers, and interviews from SANS Institute, CSA, NIST, ENISA, Gartner Group, KVM.org, OpenGrid, OpenStack, and OpenNebula.
   c) Companies: white papers, manuals, interviews, and web content from ERICSSON, IBM, XEROX, Cisco, VMWare, XEN, CITRIX, EMC, Microsoft, and Salesforce.
2) Each reference was analyzed to identify all the mentioned concerns covered and solutions provided. Thus, one reference can produce more than one entry on each specified category.
3) Some security perspectives were not covered in this paper, as each security/concern category can be subdivided in finer-grained aspects such as: authentication, integrity, network communications, etc.

We present the security concerns and solutions using pie charts in order to show the representativeness of each category/group in the total amount of identified references. The comparison is presented using radar graphs to identify how many solutions address each concern category/group.

A. Security concerns

The results obtained for citations on security issues is shown in figure 5.

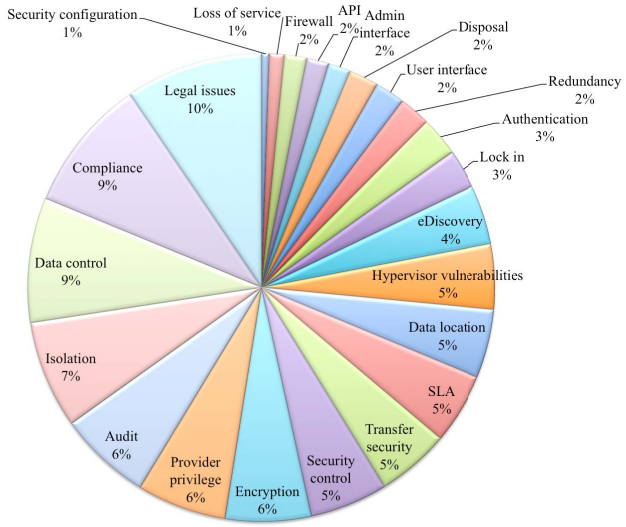

Figure 5. Security problems

Legal and administrative issues represent a clear majority with over half of the citations. The three first major problems are legal issues, compliance and loss of control over data, followed by the first technical issue, isolation, with 7% of citations. The least cited problems are related to security configuration concerns, loss of service (albeit this is also referenced by compliance, which is a major problem), firewalling and interfaces. Grouping the problems using the categories presented in section II reveals the results presented in figure 6.

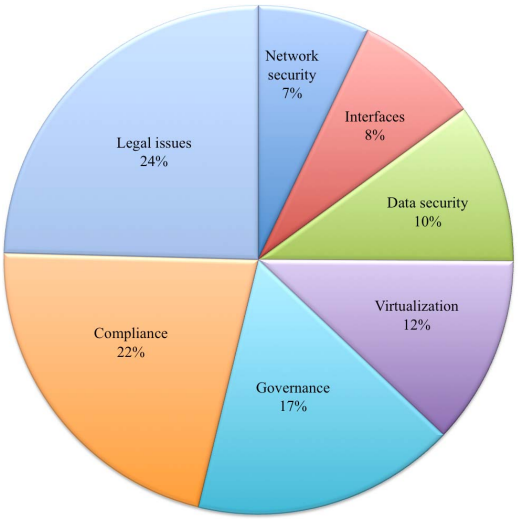

Figure 6. Security problems with grouped categories

Legal and administrative issues represent 73% of concern citations, showing a clear consideration of legal issues such as data location and e-discovery, or administrative ones like loss of governance over security and data. The technical issue more intensively evaluated (12%) is virtualization, followed by data security, interfaces and network security.

Virtualization represents the novelty of cloud computing in terms of technologies employed, considering virtual infrastructures, scalability and resource sharing, and its related problems represent the first major technical concern.

B. Security solutions

The number of citations for security problems related to legal issues, compliance and other administrative aspects (governance) is high: as shown in figure 6, they correspond to 73% (respectively: 24%, 22%, and 17%). However, the references to solutions is also notable: figure 7 shows a total of 32% (respectively: 12%, 12%, and 8%). In other words, the concern is relevant but a large number solutions are already available.

When analyzing citations for solutions, we used the same approach described in the beginning of this section. The results are presented in figure 7.

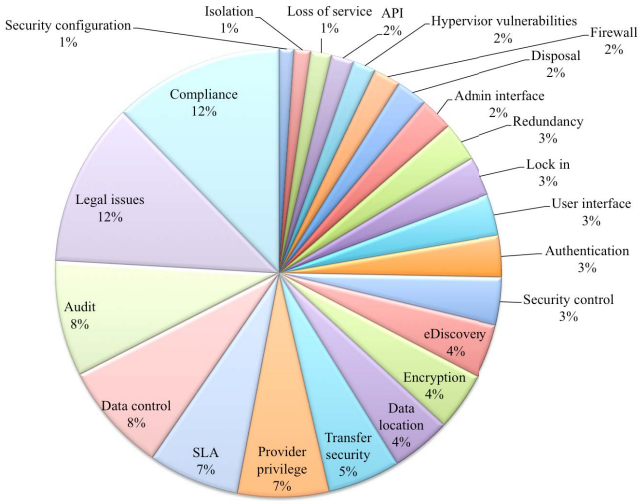

Figure 7. Security solutions

The situation is completely different when analyzing technical aspects such as virtualization, isolation and data leakage. Isolation is a perfect example as the number of citations for problems represents 7% while solutions amounts for only 1%. A conclusion that can be drawn from this situation is that the concern is also significant but yet little is available in terms of solutions. We note that, for this specific issue, special care has been taken when assessing the most popular virtual machine solution providers (e.g., XEN, VMWARE, and KVM), aiming to verify their concerns and available solutions.

Grouping the security issues and analyzing the solution citations results in figure 8.

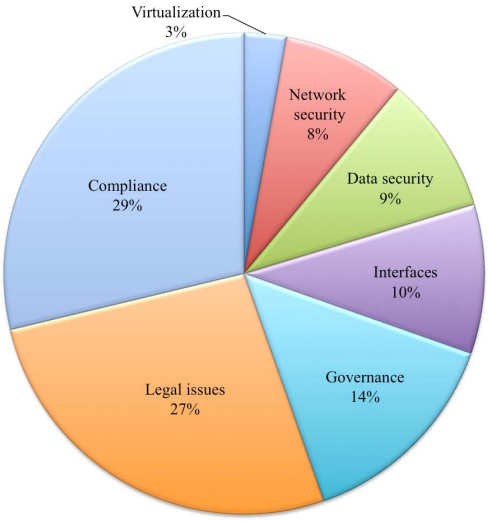

Figure 8. Security solutions with grouped categories

While compliance, legal issues and governance all have a high number of citations for problems and solutions, virtualization amounts for 12% of problem references and only 3% for solutions. This discrepancy indicates the need of evaluating potential areas still to be developed in order to provide better security conditions when migrating data and processes in the cloud.

C. Comparison

The differences between problem and solution citations presented in the previous sections are observed in figure 9.

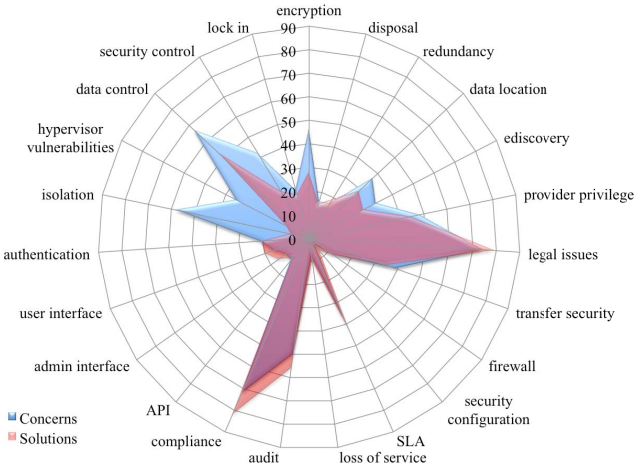

Figure 9. Comparison between citations

The blue areas represent concern citations, lighter red for solutions and darker red where they overlap. In other words, light red areas are problems with more citations for solutions than problems – they might be meaningful problems, but there are many solutions already addressing them – while blue areas represent potential subjects that have received little attention so far, indicating the need for further studies.

Figure 9 clearly shows the lack of development regarding data control mechanisms, hypervisor vulnerabilities assessment and isolation solutions for virtualized environments. On the other hand, areas such as legal concerns, SLAs, compliance and audit policies have a quite satisfactory coverage. The results for grouped categories (presented in section II) are depicted in figure 10.

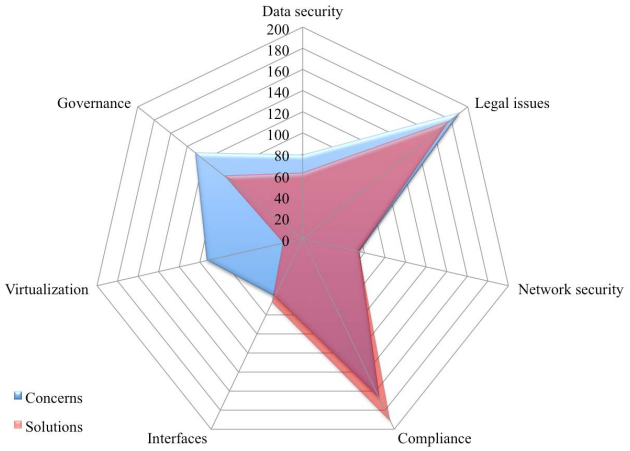

Figure 10. Comparison between citations with grouped categories

Figure 10 shows that virtualization problems represent an area that requires studies for addressing issues such as isolation, data leakage and cross-VM attacks; on the other hand, areas such as compliance and network security encompass concerns for which there are already a considerable number of solutions or that are not considered highly relevant.

V. Discussion

Considering the discussion in the previous section, a straightforward conclusion is that cloud security includes old and well-known issues – such as network and other infrastructural vulnerabilities, user access, authentication and privacy – and also novel concerns derived from new technologies adopted to offer the adequate resources (mainly virtualized ones), services and auxiliary tools. These problems are summarized by isolation and hypervisor vulnerabilities (the main technical concerns according to the studies and graphics presented), data location and e-discovery (legal aspects), and loss of governance over data, security and even decision making, where the cloud must be strategically and financially considered as a decisive factor.

Another point observed is that, while adopting a cloud service or provider is easy, migrating to another is not [50]. After moving local data and processes to the cloud, the lack of standards for protocols and formats directly affect an attempt to migrate to a different provider, even if this is motivated by legitimate reasons such as non-fulfillment of SLAs, outages or provider bankruptcy [51]. Consequently, the first choice must be carefully made, as SLAs are not perfect and services outages happen at the same pace that resource sharing, multitenancy and scalability are not fail proof. After that is made,

future migrations between services can be extremely onerous in terms of time and costs; most likely, this task will require an extensive work for bringing all data and resources to a local infrastructure before redeploying to the cloud.

Finally, the analysis of current trends for cloud computing reveals that there is a considerable number of well-studied security concerns, for which plenty solutions and best practices have been developed, such as those related to legal and administrative concerns. On the other hand, many issues still require further research effort, especially those related to secure virtualization.

VI. Related work

Regarding opinions on the current status of cloud security and what is predicted for the future, Mather, Kumaraswamy and Latif [6] created a compilation of security points to be developed based on topics like infrastructure, data security and storage, identity and access management, security management, privacy, audit and compliance. There is an unquestionable need for greater transparency regarding which party (customer or cloud provider) provides each security capability, along with standardization and legal agreements to be created reflecting operational SLAs. Other problems discussed are the inadequate encryption and key management capabilities currently offered, and the need for multi-entity key management.

As a top recommendation for security in cloud computing, ENISA [4] suggests that providers must ensure some security practices to customers, and also provide a clear contract to avoid legal problems. Key points to be developed include breach reporting, better logging mechanisms and engineering of large scale computer systems, which includes the isolation of virtual machines and also of resources and information. Their analysis is based on what is currently observed and can be improved by adopting available best practices or by applying solutions to cloud computing that are already used in other environments. This article aims at taking one step further by transforming these observations into numbers – a quantitative approach.

NIST has been developing a taxonomy [52] identifying key roles in the cloud environment, which includes service providers, cloud carriers (which participate on distributing or accessing services in order to provide value-adding functionalities), consumers, brokers (which deal with consumption and provisioning of services) and auditors (which perform audits on security, privacy-impact and performance). The concepts presented here extend NIST's initial definition for cloud computing [8], incorporating a division of roles and responsibilities that can be directly applied to security assessments.

Concerning future developments, there is a clear claim for a solid solutions when protecting virtual environments. Associations such as the Enterprise Strategy Group [53] emphasize the need for hypervisor security, shrinking hypervisor footprints, defining the security perimeter virtualization, and linking security and VM provisioning for better resource management. This implies increased automation for security controls, greater use of VM identity management (built on top of Public Key Infrastructure and Open Virtualization Format) and data encryption (tightly connected to smarter key management practices).

VII. Considerations and future work

Security is a crucial aspect for providing a reliable environment and then enable the use of applications in the cloud and for moving data and business processes to virtualized infrastructures. Many of the security issues identified are observed in other computing environments: authentication, network security and legal requirements, for example, are not a novelty. However, the impact of such issues is intensified in cloud computing due to characteristics such as multi-tenancy and resource sharing, since actions from a single customer can affect all other users that inevitably share the same resources and interfaces. On the other hand, efficient and secure virtualization represents a new challenge in this context with high distribution of complex services and web-based applications, thus requiring more sophisticated approaches.

It is strategic to develop new mechanisms that provide the required security level by isolating virtual machines and the associated resources while following best practices in terms of legal regulations and compliance to SLAs. Among other requirements, such solutions should employ virtual machine identification, provide an adequate separation of dedicated resources combined with a constant observation of shared ones, and examine any attempt of exploiting cross-VM and data leakage.

A secure cloud computing environment depends on several security solutions working harmoniously together. However, in our studies we did not identify any security solutions' provider owning all the facilities necessary to get high levels of security conformity for clouds. Thus, cloud providers need to orchestrate / harmonize security solutions from different places in order to achieve the desired security level.

In order to verify these conclusions in practice, we deployed testbeds using OpenNebula (based on KVM and XEN) and analyzed its security aspects; we also analyzed virtualized servers based on VMWARE using our testbed networks. This investigation lead to a wide research of PaaS solutions, and allowed us to verify that most of them use virtual machines based on virtualization technologies such as VMWARE, XEN, and KVM, which often lack security aspects We also learned that Amazon changed the XEN source code in order to include security features, but unfortunately the modified code is not publicly available and it appears to be no article detailing the changes introduced. Given these limitations, a deeper study on current security solutions to manage cloud computing virtual machines inside the cloud providers should be the focus of future work in the area.

Acknowledgments

This work was supported by the Innovation Center, Ericsson Telecomunicações S.A., Brazil.

REFERENCES

[1] IDC, "Cloud computing 2010 – an IDC update," slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update, September 2009.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California at Berkeley, eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html, Tech. Rep. UCB/EECS-2009-28, February 2009.

[3] S. Shankland, "HP's Hurd dings cloud computing, IBM," CNET News, October 2009.

[4] D. Catteddu and G. Hogben, "Benefits, risks and recommendations for information security," European Network and Information Security Agency, enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment, Tech. Rep., November 2009.

[5] CSA, "Security guidance for critical areas of focus in cloud computing," Cloud Security Alliance, Tech. Rep., December 2009.

[6] T. Mather and S. Kumaraswamy, *Cloud Security and privacy: An Enterprise Perspective on Risks and Compliance*, 1st ed. O'Reilly Media, October 2009.

[7] Y. Chen, V. Paxson, and R. H. Katz, "What's new about cloud computing security?" University of California at Berkeley, eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html, Tech. Rep. UCB/EECS-2010-5, January 2010.

[8] P. Mell and T. Grance, "The nist definition of cloud computing," National Institute of Standards and Technology, www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, Tech. Rep. 15, July 2009.

[9] D. Hubbard, L. J. H. Jr, and M. Sutton, "Top threats to cloud computing," Cloud Security Alliance, Tech. Rep., March 2010. [Online]. Available: cloudsecurityalliance.org/research/projects/top-threats-to-cloud-computing/

[10] D. Tompkins, "Security for cloud-based enterprise applications," http://blog.dt.org/index.php/2009/02/security-for-cloud-based-enterprise-applications/, February 2009.

[11] TrendMicro, "Cloud Computing Security - Making Virtual Machines Cloud-Ready," Trend Micro White Paper, May 2010.

[12] S. Genovese, "Akamai introduces cloud-based firewall," http://cloudcomputing.sys-con.com/node/1219023, December 2009.

[13] G. V. Hulme, "Cloudpassage aims to ease cloud server security management," http://www.csoonline.com/article/658121/cloudpassage-aims-to-ease-cloud-server-security-management, January 2011.

[14] Google, "Google App Engine," code.google.com/appengine/, 2011.

[15] ——, "Google query language (gql)," code.google.com/intl/en/appengine/docs/python/overview.html, 2011.

[16] StackOverflow, "Does using non-sql databases obviate the need for guarding against sql injection?" stackoverflow.com/questions/1823536/does-using-non-sql-databases-obviate-the-need-for-guarding-against-sql-injection, 2011.

[17] J. Rose, "Cloudy with a chance of zero day," www.owasp.org/images/1/12/Cloudy_with_a_chance_of_0_day_-_Jon_Rose-Tom_Leavey.pdf, 2011.

[18] A. Balkan, "Why Google App Engine is broken and what Google must do to fix it," aralbalkan.com/1504, 2011.

[19] Salesforce, "Salesforce security statement," salesforce.com/company/privacy/security.jsp, 2011.

[20] T. Espiner, "Salesforce tight-lipped after phishing attack," zdnet.co.uk/news/security-threats/2007/11/07/salesforce-tight-lipped-after-phishing-attack-39290616/, November 2007.

[21] A. Yee, "Implications of salesforce phishing incident," ebizq.net/blogs/security_insider/2007/11/-implications_of_salesforce_phi.php, November 2007.

[22] Salesforce, "Security Implementation Guide," login.salesforce.com/help/doc/en/salesforce_security_impl_guide.pdf, April 2011.

[23] Amazon, "Elastic compute cloud (ec2)," aws.amazon.com/ec2/, 2011.

[24] C. Kaufman and R. Venkatapathy, "Windows azure security overview," go.microsoft.com/?linkid=9740388, 2010, august.

[25] R. McMillan, "Google attack part of widespread spying effort," PCWorld, January 2010.

[26] E. Mills, "Behind the china attacks on google," CNET News, January 2010.

[27] M. Arrington, "Google defends against large scale chinese cyber attack: May cease chinese operations," TechCrunch, January 2010.

[28] J. Bosch, "Google accounts attacked by phishing scam," BrickHouse Security Blog, October 2009.

[29] T. Telegraph, "Facebook users targeted by phishing attack," The Telegraph, May 2009.

[30] L. Musthaler, "Cost-effective data encryption in the cloud," Network World, December 2009.

[31] C. Tech, "Examining redundancy in the data center powered by the cloud and disaster recovery," Consonus Tech, 2010.

[32] M. Lyle, "Redundancy in data storage," Define the Cloud, February 2011.

[33] P. Dorion, "Data destruction services: When data deletion is not enough," SearchDataBackup.com, 2010.

[34] R. Mogull, "Cloud data security: Archive and delete (rough cut)," securosis.com/blog/cloud-data-security-archive-and-delete-rough-cut/, September 2009.

[35] E. Messmer, "Gartner: New security demands arising for virtualization, cloud computing," http://www.networkworld.com/news/2011/062311-security-summit.html, June 2011.

[36] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, ser. CCSW '09. New York, NY, USA: ACM, 2009, pp. 85–90. [Online]. Available: http://doi.acm.org/10.1145/1655008.1655020

[37] J. Brodkin, "Gartner: Seven cloud computing security risks," http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853, July 2008.

[38] B. Winterford, "Amazon ec2 suffers huge outage," http://www.crn.com.au/News/255586,amazon-ec2-suffers-huge-outage.aspx, April 2011.

[39] G. Clarke, "Microsoft bpos cloud outage burns exchange converts," http://www.theregister.co.uk/2011/05/13/, May 2011.

[40] S. Shankland, "Amazon cloud outage derails reddit, quora," April 2011.

[41] E. . Young, "Cloud computing - the role of internal audit," October 2009.

[42] CloudAudit, "A6 - the automated audit, assertion, assessment and assurance api," http://cloudaudit.org/.

[43] J. Pavolotsky, "Top five legal issues for the cloud," http://www.forbes.com/2010/04/12/cloud-computing-enterprise-technology-cio-network-legal.html, April 2010.

[44] N. Anand, "The legal issues around cloud computing," http://www.labnol.org/internet/cloud-computing-legal-issues/14120/, July 2010.

[45] S. Hunter, "Ascending to the cloud creates negligible e-discovery risk," http://ediscovery.quarles.com/2011/07/articles/information-technology/ascending-to-the-cloud-creates-negligible-ediscovery-risk/, July 2011.

[46] J. W. S. Sharon D. Nelson, "Virtualization and cloud computing: benefits and e-discovery implications," http://www.slaw.ca/2011/07/19/virtualization-and-cloud-computing-benefits-and-e-discovery-implications/, July 2011.

[47] L. Bentley, "E-discovery in the cloud presents promise and problems," http://www.itbusinessedge.com/cm/community/features/interviews/blog/e-discovery-in-the-cloud-presents-promise-and-problems/?cs=31698, April 2009.

[48] J. Zierick, "The special case of privileged users in the cloud," http://blog.beyondtrust.com/bid/63894/The-Special-Case-of-Privileged-Users-in-the-Cloud, June 2011.

[49] S. Dinoor, "Got privilege? ten steps to securing a cloud-based enterprise," http://cloudcomputing.sys-con.com/node/1571649, October 2010.

[50] B. Claybrook, "How providers affect cloud application migration," http://searchcloudcomputing.techtarget.com/tutorial/How-providers-affect-cloud-application-migration, June 2011.

[51] CSA, "Interoperability and portability," July 2011.

[52] NIST, "Draft cloud taxonomy," http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/ReferenceArchitectureTaxonomy, March 2011.

[53] J. Oltsik, "Information security, virtualization, and the journey to the cloud," Cloud Security Alliance, Tech. Rep., August 2010.