Journal of Cloud Computing
a SpringerOpen Journal

RESEARCH Open Access

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

Nelson Gonzalez[1*], Charles Miers[1,4], Fernando Redígolo[1], Marcos Simplício[1], Tereza Carvalho[1], Mats Näslund[2] and Makan Pourzandi[3]

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.

Introduction

Security is considered a key requirement for cloud computing consolidation as a robust and feasible multipurpose solution [1]. This viewpoint is shared by many distinct groups, including academia researchers [2,3], business decision makers [4] and government organizations [5,6]. 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 [7]. These concerns have their origin not only on existing problems, directly inherited from the adopted technologies, but are also related to new issues derived from the composition of essential cloud computing features like scalability, resource sharing and virtualization (e.g., data leakage and hypervisor vulnerabilities) [8]. The distinction between these classes is more easily identifiable by analyzing the definition of the essential cloud computing characteristics proposed by the NIST (National Institute of Standards and Technology) in [9], 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 [10]. An authoritative reference in the area is the risk assessment developed by ENISA (European Network and Information Security Agency) [5]. 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) [6], 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.

*Correspondence: nmimura@larc.usp.br
[1] Escola Politécnica at the University of São Paulo (EPUSP), São Paulo, Brazil
Full list of author information is available at the end of the article

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 the concerns that remain unanswered. 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, without losing sight of important issues that also exist in other distributed systems. This article extends our previous work presented in [11], providing an enhanced review of the cloud computing security taxonomy previously presented, as well as a deeper analysis of the related work by discussing the main security frameworks currently available; in addition, we discuss further the security aspects related to virtualization in cloud computing, a fundamental yet still underserved field of research.

Cloud computing security

Key references such as CSA's security guidance [6] and top threats analysis [12], ENISA's security assessment [5] and the cloud computing definitions from NIST [9] highlight different security issues related to cloud computing that require further studies for being appropriately handled and, consequently, for enhancing technology acceptance and adoption. Emphasis is given to the distinction between services in the form of software (SaaS), platform (PaaS) and infrastructure (IaaS), which are commonly used as the fundamental basis for cloud service classification. However, no other methods are standardized or even employed to organize cloud computing security aspects apart from cloud deployment models, service types or traditional security models.

Aiming to concentrate and organize information related to cloud security and to facilitate future studies, in this section we identify the main problems in the area and group them into a model composed of seven categories, based on the aforementioned references . Namely, the categories are: network security, interfaces, data security, virtualization, governance, compliance and legal issues. Each category includes several potential security problems, resulting in a classification with subdivisions that highlights the main issues identified in the base references:

1. Network security: Problems associated with network communications and configurations regarding cloud computing infrastructures. The ideal network security solution is to have cloud services as an extension of customers' existing internal networks [13], adopting the same protection measures and security precautions that are locally implemented and allowing them to extend local strategies to any remote resource or process [14].
   (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 [15]. They also 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 similar security measures specific for cloud environments [16,17] reveal the urge for adapting existing solutions for this new computing paradigm.
   (c) Security configuration: Configuration of protocols, systems and technologies to provide the required levels of security and privacy without compromising performance or efficiency [18].
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) for accessing virtualized resources and systems must be protected in order to prevent malicious use [19-23].
   (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 [24-27].
   (d) Authentication: Mechanisms required to enable access to the cloud [28]. Most services rely on regular accounts [20,29,30] consequently being susceptible to a plethora of attacks [31-35] whose consequences are boosted by multi-tenancy 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 requiring basic security levels) [36].

(a) Cryptography: Most employed practice to secure sensitive data [37], thoroughly required by industry, state and federal regulations [38].
(b) Redundancy: Essential to avoid data loss. Most business models rely on information technology for its core functionalities and processes [39,40] and, thus, mission-critical data integrity and availability must be ensured.
(c) Disposal: Elementary data disposal techniques are insufficient and commonly referred as deletion [41].In the cloud, the complete destruction of data, including log references and hidden backup registries, is an important requirement [42].

4. Virtualization: Isolation between VMs, hypervisor vulnerabilities and other problems associated to the use of virtualization technologies [43].

(a) Isolation: Although logically isolated, all VMs share the same hardware and consequently the same resources, allowing malicious entities to exploit data leaks and cross-VM attacks [44]. 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.
(c) Data leakage: Exploit hypervisor vulnerabilities and lack of isolation controls in order to leak data from virtualized infrastructures, obtaining sensitive customer data and affecting confidentiality and integrity.
(d) VM identification: Lack of controls for identifying virtual machines that are being used for executing a specific process or for storing files.
(e) Cross-VM attacks: Includes attempts to estimate provider traffic rates in order to steal cryptographic keys and increase chances of VM placement attacks. One example consists in overlapping memory and storage regions initially dedicated to a single virtual machine, which also enables other isolation-related attacks.

5. Governance: Issues related to (losing) administrative and security controls in cloud computing solutions [45,46].

(a) Data control: Moving data to the cloud means losing control over redundancy, location, file systems and other relevant configurations.
(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: Includes requirements related to service availability and audit capabilities [47,48].

(a) Service Level Agreements (SLA): Mechanisms to ensure the required service availability and the basic security procedures to be adopted [49].
(b) Loss of service: Service outages are not exclusive to cloud environments but are more serious in this context due to the interconnections between services (e.g., a SaaS using virtualized infrastructures provided by an IaaS), as shown in many examples [50-52]. This leads to the need of strong disaster recovery policies and provider recommendations to implement customer-side redundancy if applicable.
(c) Audit: Allows 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 [53] 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 [54].
(d) Service conformity: Related to how contractual obligations and overall service requirements are respected and offered based

on the SLAs predefined and basic service and customer needs.

7. Legal issues: Aspects related to judicial requirements and law, such as multiple data locations and privilege management.

    (a) Data location: Customer data held in multiple jurisdictions depending on geographic location [55] are affected, directly or indirectly, by subpoena law-enforcement measures.
    (b) E-discovery: As a result of a law-enforcement measures, hardware might be confiscated for investigations related to a particular customer, affecting all customers whose data were stored in the same hardware [56-58]. 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 [59,60].
    (d) legislation: Juridical concerns related to new concepts introduced by cloud computing [61].

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.

The three first groups correspond to fundamental (and often related) security principles [7] (Chapters 3-8).

The *architecture* dimension is subdivided into network security, interfaces and virtualization issues, comprising both user and administrative interfaces to access the cloud. It also comprises security during transferences of data and virtual machines, as well as other virtualization related issues, such as isolation and cross-VM attacks. This organization is depicted in Figure 2. 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). This suggests that the security mechanisms used must be clearly stated before the service is contracted, defining which role is responsible for providing firewalling capabilities, access control features and technology-specific requirements (such as those related to virtualization).

The *compliance* dimension introduces responsibilities toward services and providers. The former includes SLA concerns, loss of service based on outages and chain failures, and auditing capabilities as well as transparency and security assessments. The latter refers to loss of control over data and security policies and configurations, and also lock-in issues resulting from lack of standards, migrations and service terminations. The complete scenario is presented in Figure 3.

The *privacy* dimension includes data security itself (from sensitive data, regulations and data loss to disposal and redundancy) and legal issues (related to multiple jurisdictions derived from different locations where data and services are hosted). The expansion of this group is represented in Figure 4. We note that the concerns in this dimension cover the complete information lifecycle (i.e., *generation, use, transfer, transformation, storage, archiving,* and *destruction*) inside the provider perimeter and in its immediate boundaries (or interfaces) to the users.

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 towards how the underlying elements (e.g., infrastructural hardware and software) are protected.

Current status of cloud security

A clear perspective of the main security problems regarding cloud computing and on how they can be organized

Figure 1 Cloud computing security taxonomy. Top level overview of the security taxonomy proposed, highlighting the three main categories: security related to privacy, architecture and compliance.

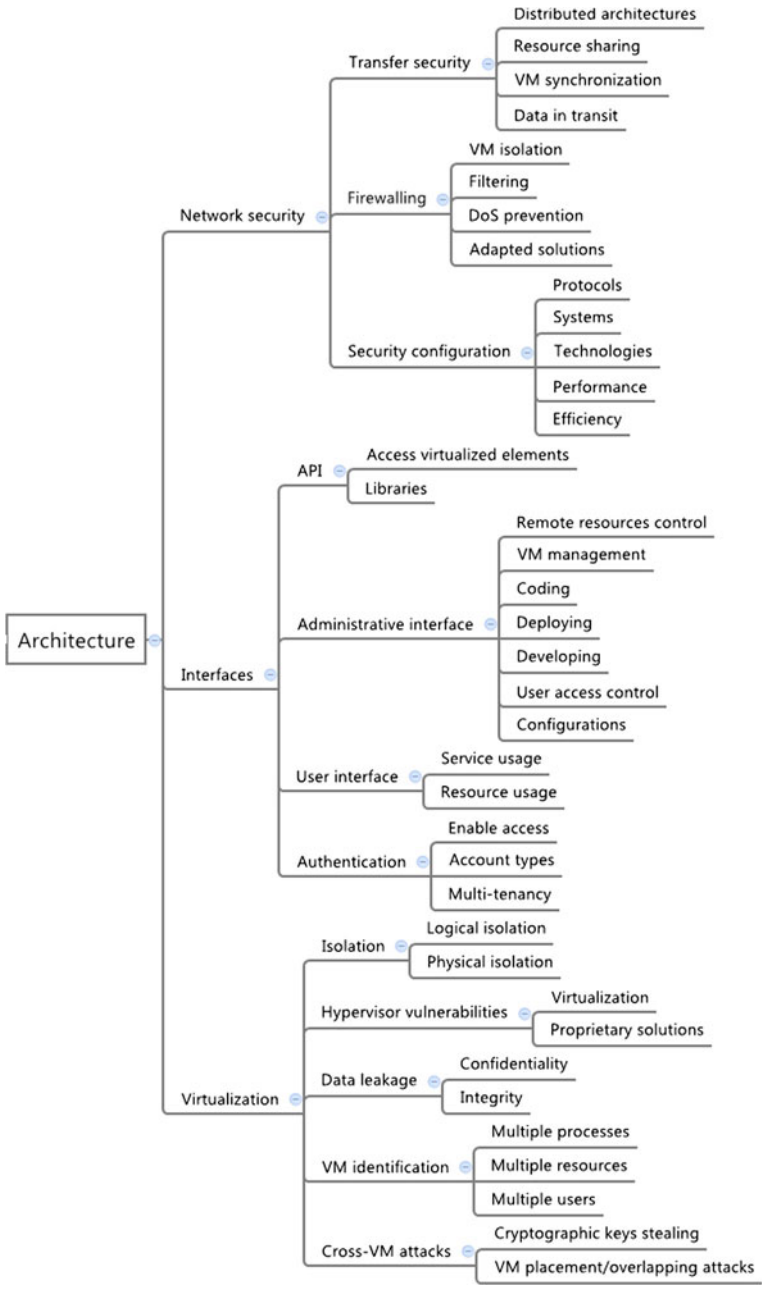

Figure 2 Security taxonomy - architecture. Details from architecture category, which is divided in network, host, application, data (security and storage), security management, and identity and access controls – all these elements are directly connected to the infrastructure and architecture adopted to implement or use a cloud solution.

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 an involved task. Nonetheless, we identify the number of references dealing with each concern, providing

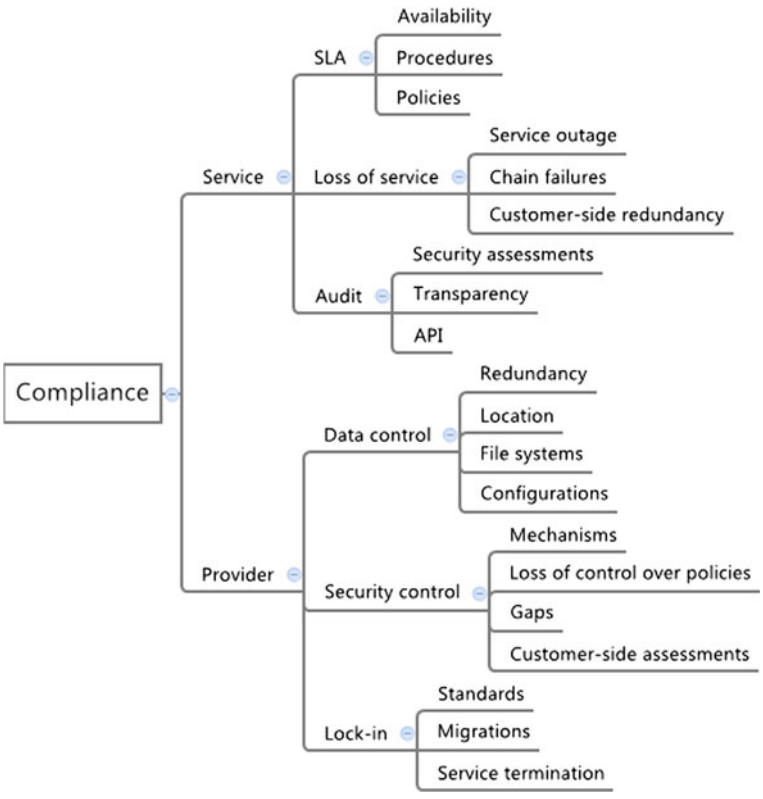

Figure 3 Security taxonomy - compliance. Details from compliance category, divided in lifecycle controls and governance, risk and other compliance related issues (such as continuous improvement policies).

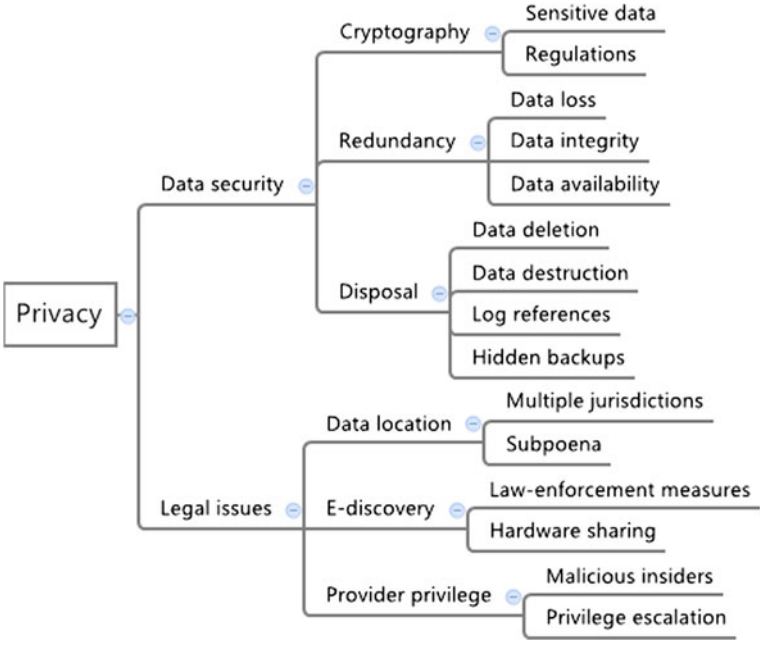

Figure 4 Security taxonomy - privacy. Details from privacy category, initially divided in concerns and principles. Concerns are related to the complete data lifecycle, from generation, use and transfer to transformation, storage, archival and destruction. Principles are guidelines related to privacy in the cloud.

some useful 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 came 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 aiming to identify all the mentioned concerns covered and solutions provided. Therefore, 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 sub-divided 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 references identified. The comparison between areas is presented using radar graphs to identify how many solutions address each concern category/group.

Security concerns

The results obtained for the number of citations on security issues is shown in Figure 5. The three major problems identified in these references are legal issues, compliance and loss of control over data. These legal- and governance-related concerns are 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 related to compliance, which is a major problem), firewalling and interfaces.

Grouping the concerns using the categories presented in section "Cloud computing security" leads to the

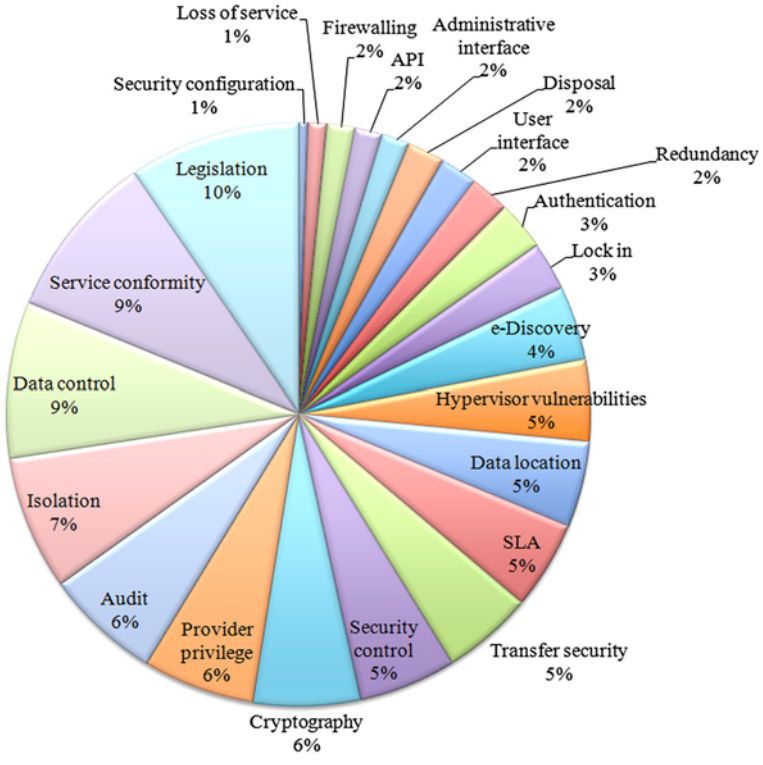

Figure 5 Security problems. Pie chart for security concerns.

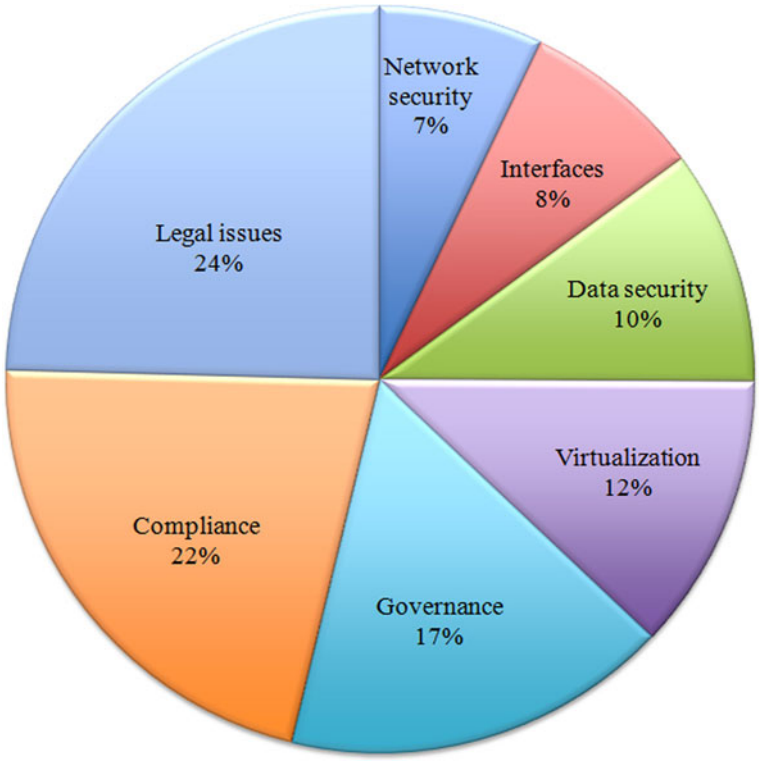

Figure 6 Security problems with grouped categories. Pie chart for security concerns with grouped categories (seven altogether: legal issues, compliance, governance, virtualization, data security, interfaces and network security).

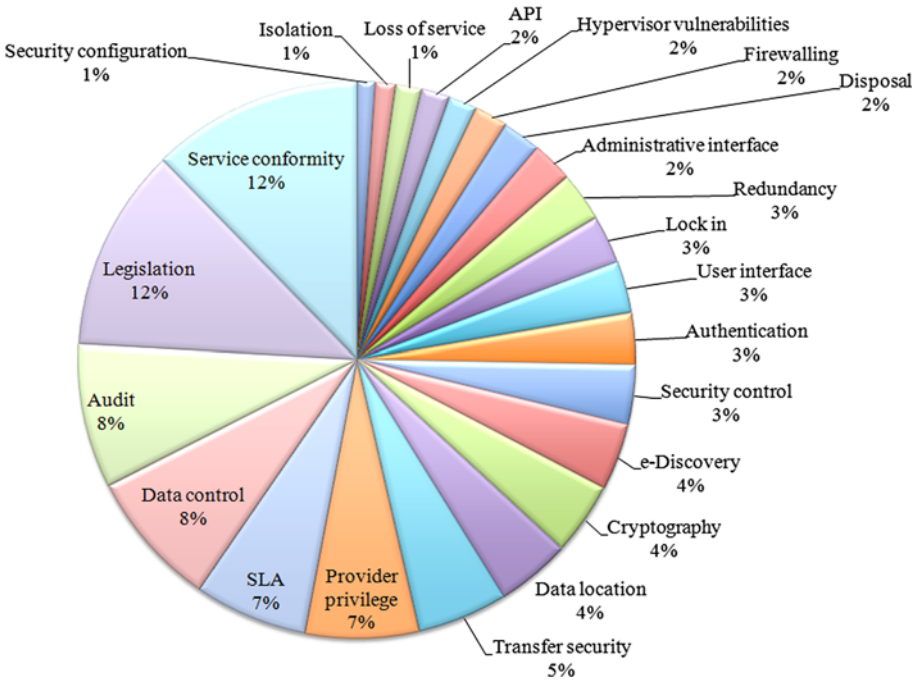

Figure 7 Security solutions with grouped categories. Pie chart for solutions with grouped categories, showing a clear lack for virtualization security mechanisms in comparison to its importance in terms of concerns citations.

construction of Figure 6. This figure shows that legal and governance issues represent a clear majority with 73% of concern citations, showing a deep consideration of legal issues such as data location and e-discovery, or governance ones like loss of control over security and data. The technical issue more intensively evaluated (12%) is virtualization, followed by data security, interfaces and network security.

Virtualization is one of the main novelties employed by cloud computing in terms of technologies employed, considering virtual infrastructures, scalability and resource sharing, and its related problems represent the first major technical concern.

Security solutions

When analyzing citations for solutions, we used the same approach described in the beginning of this section. The results are presented in Figure 7, which shows the percentage of solutions in each category defined in section "Cloud computing security", and also in Figure 8, which highlights the contribution of each individual sub-category.

When we compare Figures 6 and 7, it is easy to observe that the number of citations covering security problems related to legal issues, compliance and governance is high (respectively 24%, 22%, and 17%); however, the same also happens when we consider the number of references proposing solutions for those issues (which represent respectively 29%, 27%, and 14% of the total number of citations). In other words, these concerns are higly relevant but a large number solutions are already available for tackling them.

The situation is completely different when we analyze technical aspects such as virtualization, isolation and data leakage. Indeed, virtualization amounts for 12% of problem references and only 3% for solutions. Isolation is a perfect example of such discrepancy as the number of citations for such problems represents 7% in Figure 5, while solutions correspond to only 1% of the graph from Figure 8. 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. A conclusion that can be drawn from this situation is that such concerns are also significant but yet little is available in terms of solutions. This 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.

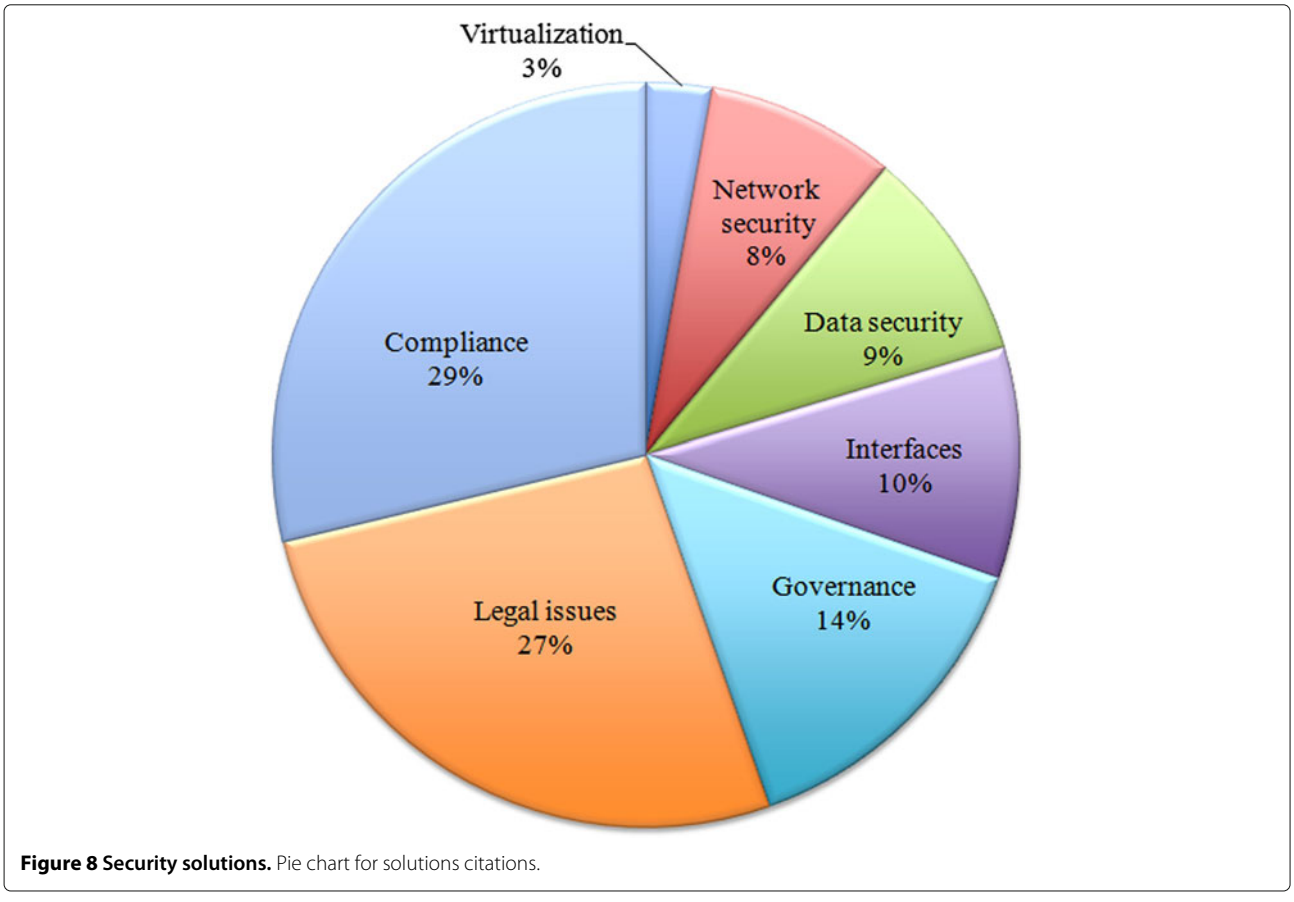

Figure 8 Security solutions. Pie chart for solutions citations.

Comparison

The differences between problem and solution citations presented in the previous sections can be observed in Figure 9.

Axis values correspond to the number of citations found among the references studied. Blue areas represent concern citations and lighter red indicates solutions, while darker red shows where those areas 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 4) are depicted in Figure 10.

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.

Finally, Considering virtualization as key element for future studies, Figure 11 presents a comparison focusing on five virtualization-related problems: isolation (of computational resources, such as memory and storage capabilities), hypervisor vulnerabilities, data leakage, cross-VM attacks and VM identification. The contrast related to isolation and cross-VM attacks is more evident than for the other issues. However, the number of solution citations for all issues is notably low if compared to any other security concern, reaffirming the need for further researches in those areas.

Related work

An abundant number of related works and publications exist in the literature, emphasizing the importance and demand of security solutions for cloud computing. However, we did not identify any full taxonomy that addresses directly the security aspects related to cloud computing. We only identified some simplified models that were developed to cover specific security aspects such as authentication. We were able to recognize two main types of works: (1) security frameworks, which aim to aggregate information about security and also to offer sets of best practices and guidelines when using cloud solutions, and (2) publications that identify future trends and propose solutions or areas of interest for research. Each category and corresponding references are further analyzed in the following subsections.

Security frameworks

Security frameworks concentrate information on security and privacy aiming to provide a compilation of risks, vulnerabilities and best practices to avoid or mitigate them. There are several entities that are constantly publishing material related to cloud computing security, including ENISA, CSA, NIST, CPNI (Centre for the Protection of

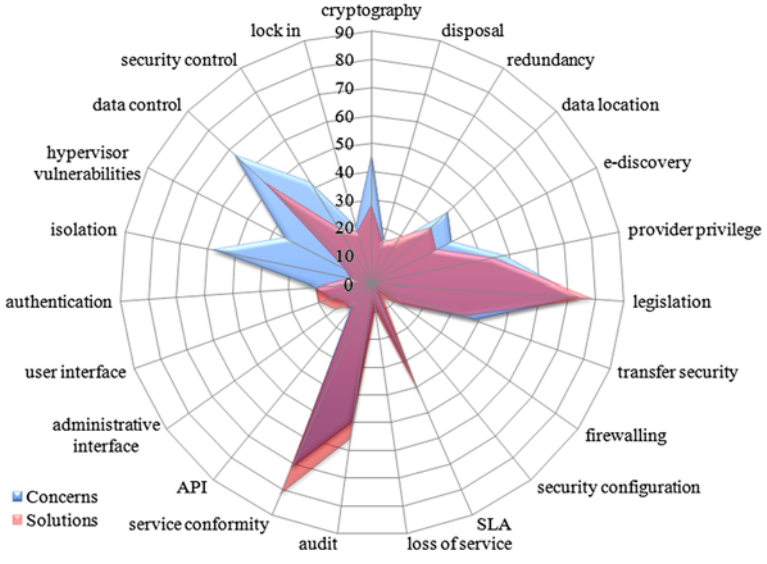

Figure 9 Comparison between citations. Radar chart comparing citations related to concerns and solutions, showing the disparities for each security category adopted.

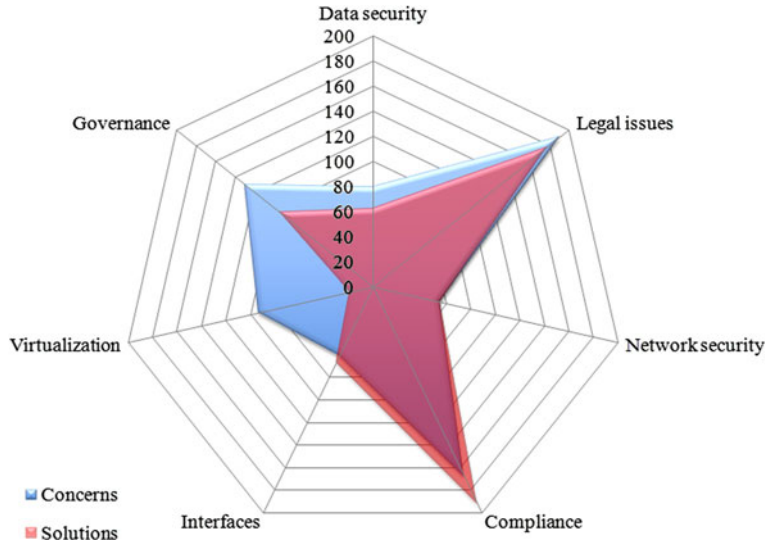

Figure 10 Comparison between citations with grouped categories. Radar chart grouping the categories, showing the difference between citations about concerns and solutions regarding each category.

National Infrastructure from UK government) and ISACA (the Information Systems Audit and Control Association). In this paper we focus on the first three entities, which by themselves provide a quite comprehensive overview of issues and solutions and, thus, allowing a broad understanding of the current status of cloud security.

ENISA

ENISA is an agency responsible for achieving high and effective level of network and information security within the European Union [62]. In the context of cloud computing, they published an extensive study covering benefits and risks related to its use [5]. In this study, the security risks are divided in four categories:

- Policy and organizational: issues related to governance, compliance and reputation;
- Technical: issues derived from technologies used to implement cloud services and infrastructures, such as isolation, data leakage and interception, denial of service attacks, encryption and disposal;
- Legal: risks regarding jurisdictions, subpoena and e-discovery;

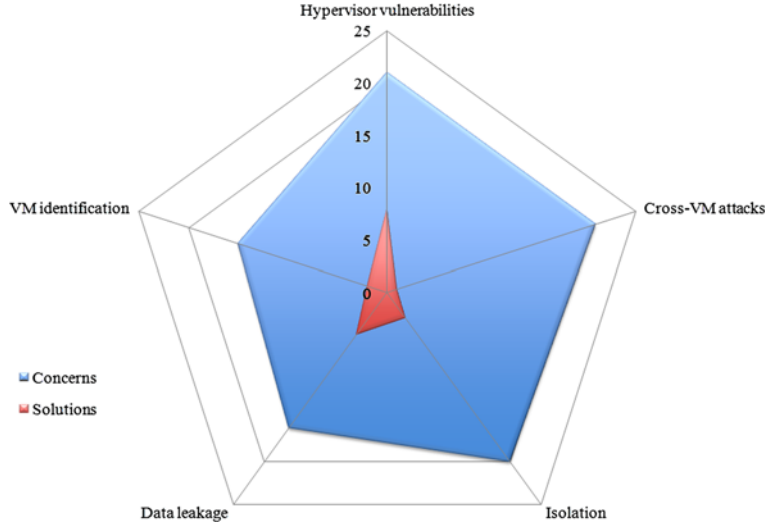

Figure 11 Comparison for virtualization. Radar chart only for virtualization issues.

- Not cloud specific: other risks that are not unique to cloud environments, such as network management, privilege escalation and logging;

As a top recommendation for security in cloud computing, ENISA suggests that providers must ensure some security practices to customers and also 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 encompass the isolation of virtual machines, resources and information. Their analysis is based not only on what is currently observed, but also on what can be improved through the adoption of existing best practices or by means of solutions that are already used in non-cloud environments. This article aims at taking one step further by transforming these observations into numbers – a quantitative approach.

CSA

CSA is an organization led by a coalition of industry practitioners, corporations, associations and other stakeholders [63], such as Dell, HP and eBay. One of its main goals is to promote the adoption of best practices for providing security within cloud computing environments.

Three CSA documents are analyzed in this paper – the security guidance [6], the top threats in cloud computing [12] and the Trusted Cloud Initiative (TCI) architecture [64] – as they comprise most of the concepts and guidelines researched and published by CSA.

The latest CSA security guidance (version 3.0 [65]) denotes multi-tenancy as the essential cloud characteristic while virtualization can be avoided when implementing cloud infrastructures – multi-tenancy only implies the use of shared resources by multiple consumers, possibly from different organizations or with different objectives. They discuss that, even if virtualization-related issues can be circumvented, segmentation and isolated policies for addressing proper management and privacy are still required. The document also establishes thirteen security domains:

1. Governance and risk management: ability to measure the risk introduced by adopting cloud computing solutions, such as legal issues, protection of sensitive data and their relation to international boundaries;
2. Legal issues: disclosure laws, shared infrastructures and interference between different users;
3. Compliance and audit: the relationship between cloud computing and internal security policies;
4. Information management and data security: identification and control of stored data, loss of physical control of data and related policies to minimize risks and possible damages;
5. Portability and interoperability: ability to change providers, services or bringing back data to local premises without major impacts;
6. Traditional security, business continuity and disaster recovery: the influence of cloud solutions on traditional processes applied for addressing security needs;
7. Data center operations: analyzing architecture and operations from data centers and identifying essential characteristics for ensuring stability;
8. Incident response, notification and remediation: policies for handling incidents;
9. Application security: aims to identify the possible security issues raised from migrating a specific solution to the cloud and which platform (among SPI model) is more adequate;
10. Encryption and key management: how higher scalability via infrastructure sharing affects encryption and other mechanisms used for protecting resources and data;
11. Identity and access management: enabling authentication for cloud solutions while maintaining security levels and availability for customers and organizations;
12. Virtualization: risks related to multi-tenancy, isolation, virtual machine co-residence and hypervisor vulnerabilities, all introduced by virtualization technologies;
13. Security as a service: third party security mechanisms, delegating security responsibilities to a trusted third party provider;

CSA also published a document focusing on identifying top threats, aiming to aid risk management strategies when cloud solutions are adopted [12]. As a complete list of threats and pertinent issues is countless, the document targets those that are specific or intensified by fundamental characteristics of the cloud, such as shared infrastructures and greater flexibility. As a result, seven threats were selected:

1. Abuse and nefarious used of cloud computing: while providing flexible and powerful resources and tools, IaaS and PaaS solutions also unveil critical exploitation possibilities built on anonymity. This leads to abuse and misuse of the provided infrastructure for conducting distributed denial of service attacks, hosting malicious data, controlling botnets or sending spam;
2. Insecure application programming interfaces: cloud services provide APIs for management, storage, virtual machine allocation and other service-specific operations. The interfaces provided must implement security methods to identify, authenticate and protect

against accidental or malicious use, which can introduce additional complexities to the system such as the need for third-party authorities and services;
3. Malicious insiders: although not specific to cloud computing, its effects are amplified by the concentration and interaction of services and management domains;
4. Shared technology vulnerabilities: scalability provided by cloud solutions are based on hardware and software components which are not originally designed to provide isolation. Even though hypervisors offer an extra granularity layer, they still exhibit flaws which are exploited for privilege escalation;
5. Data loss and leakage: insufficient controls concerning user access and data security (including privacy and integrity), as well as disposal and even legal issues;
6. Account, service and traffic hijacking: phishing and related frauds are not a novelty to computing security. However, not only an attacker is able to manipulate data and transactions, but also to use stolen credentials to perform other attacks that compromise customer and provider reputation.
7. Unknown risk profile: delegation of control over data and infrastructure allows companies to better concentrate on their core business, possibly maximizing profit and efficiency. On the other hand, the consequent loss of governance leads to obscurity [66]: information about other customers sharing the same infrastructure or regarding patching and updating policies is limited. This situation creates uncertainty concerning the exact risk levels that are inherent to the cloud solution;

It is interesting to notice the choice for cloud-specific issues as it allows the identification of central points for further development. Moreover, this compilation of threats is closely related to CSA security guidance, composing a solid framework for security and risk analysis assessments while providing recommendations and best practices to achieve acceptable security levels.

Another approach adopted by CSA for organizing information related to cloud security and governance is the TCI Reference Architecture Model [64]. This document focuses on defining guidelines for enabling trust in the cloud while establishing open standards and capabilities for all cloud-based operations. The architecture defines different organization levels by combining frameworks like the SPI model, ISO 27002, COBIT, PCI, SOX and architectures such as SABSA, TOGAF, ITIL and Jericho. A wide range of aspects are then covered: SABSA defines business operation support services, such as compliance, data governance, operational risk management, human resources security, security monitoring services, legal services and internal investigations; TOGAF defines the types of services covered (presentation, application, information and infrastructure; ITIL is used for information technology operation and support, from IT operation to service delivery, support and management of incidents, changes and resources; finally, Jericho covers security and risk management, including information security management, authorization, threat and vulnerability management, policies and standards. The result is a tri-dimensional relationship between cloud delivery, trust and operation that aims to be easily consumed and applied in a security-oriented design.

NIST

NIST has recently published a taxonomy for security in cloud computing [67] that is comparable to the taxonomy introduced in section "Cloud computing security taxonomy". This taxonomy's first level encompass typical roles in the cloud environment: cloud service provider, responsible for making the service itself available; cloud service consumer, who uses the service and maintains a business relationship with the provider; cloud carrier, which provides communication interfaces between providers and consumers; cloud broker, that manages use, performance and delivery of services and intermediates negotiations between providers and consumers; and cloud auditor, which performs assessment of services, operations and security. Each role is associated to their respective activities and decomposed on their components and subcomponents. The clearest difference from our taxonomy is the hierarchy adopted, as our proposal primarily focuses on security principles in its higher level perspective, while the cloud roles are explored in deeper levels. The concepts presented here extend NIST's initial definition for cloud computing [9], incorporating a division of roles and responsibilities that can be directly applied to security assessments. On the other hand, NIST's taxonomy incorporates concepts such as deployment models, service types and activities related to cloud management (portability, interoperability, provisioning), most of them largely employed in publications related to cloud computing – including this one.

Frameworks summary

Tables 1 and 2 summarize the information about each framework.

Books, papers and other publications

Rimal, Choi and Lumb [3] present a cloud taxonomy created from the perspective of the academia, developers and researchers, instead of the usual point of view related to vendors. Whilst they do provide definitions and concepts such as cloud architecture (based on SPI model),

Table 1 Summary of CSA security frameworks

Framework	Objectives	Structure and comments
CSA Guidance		
	• Recommendations for reducing risks • No restrictions regarding specific solutions or service types • Guidelines not necessarily applicable for all deployment models • Provide initial structure to divide efforts for researches	• One architectural domain • Governance domains: risk management, legal concerns, compliance, auditing, information management, interoperability and portability • Operational domains: traditional and business security, disaster recovery, data center operations, encryption, application security, identification, authorization, virtualization, security outsourcing • Emphasis on the fact that cloud is not bound to virtualization technologies, though cloud services heavily depend on virtualized infrastructures to provide flexibility and scalability
CSA Top Threats		
	• Provide context for risk management decisions and strategies • Focus on issues which are unique or highly influenced by cloud computing characteristics	• Seven main threats: – Abuse and malicious use of cloud resources – Insecure APIs – Malicious insiders – Shared technology vulnerabilities – Data loss and leakage – Hijacking of accounts, services and traffic – Unknown risk profile (security obscurity) • Summarizes information on top threats and provide examples, remediation guidelines, impact caused and which service types (based on SPI model) are affected
CSA Architecture		
	• Enable trust in the cloud based on well-known standards and certifications allied to security frameworks and other open references • Use widely adopted frameworks in order to achieve standardization of policies and best practices based on already accepted security principles	• Four sets of frameworks (security, NIST SPI, IT audit and legislative) and four architectural domains (SABSA business architecture, ITIL for services management, Jericho for security and TOGAF for IT reference) • Tridimensional structure based on premises of cloud delivery, trust and operations • Concentrates a plethora of concepts and information related to services operation and security

Table summarizing information related to CSA security frameworks (guidance, top threats and TCI architecture).

virtualization management, service types, fault tolerance policies and security, no further studies are developed focusing on cloud specific security aspects. This characteristic is also observed in other cloud taxonomies [68-70] whose efforts converge to the definition of service models and types rather than to more technical aspects such as security, privacy or compliance concerns – which are the focus of this paper.

In [7], Mather, Kumaraswamy and Latif discuss the current status of cloud security and what is predicted for the future. The result is a compilation of security-related subjects to be developed in topics like infrastructure, data security and storage, identity and access management, security management, privacy, audit and compliance. They also explore the unquestionable urge for more transparency regarding which party (customer or cloud provider) provides each security capability, as well as the need for standardization and for the creation of legal agreements reflecting operational SLAs. Other issues discussed are the inadequate encryption and key management capabilities currently offered, as well as the need for multi-entity key management.

Many publications also state the need for better security mechanisms for cloud environments. Doelitzscher *et al.* [71] emphasize security as a major research area in cloud computing. They also highlight the lack of flexibility of classic intrusion detection mechanisms to handle virtualized environments, suggesting the use of special security audit tools associated to business flow modeling through security SLAs. In addition, they identify abuse of cloud resources, lack of security monitoring in cloud infrastructure and defective isolation of shared resources as focal points to be managed. Their analysis of top security concerns is also based on publications from CSA, ENISA and others, but after a quick evaluation of issues their focus switch to their security auditing solution, without offering a deeper quantitative compilation of security risks and areas of concern.

Table 2 Summary of ENISA and NIST security frameworks

Framework	Objectives	Structure and comments
ENISA Report		
	• Study on benefits and risks when adopting cloud solutions for business operations • Provide information for security assessments and decision making	• Three main categories of cloud specific risks (policy and organizational, technical, legal) plus one extra category for not specific ones • Offers basic guidelines and best practices for avoiding or mitigating their effects • Presents recommendations for further studies related to trust building (certifications, metrics and transparency), large scale data protection (privacy, integrity, incident handling and regulations) and technical aspects (isolation, portability and resilience) • Highlights the duality of scalability (fast, flexible and accessible resources versus concentrations of data attracting attackers and also providing infrastructure for aiding their operations) • Extensive study on risks considering their impact and probability
NIST Taxonomy		
	• Define what cloud services should provide rather than how to design and implement solutions • Ease the understanding of cloud internal operations and mechanisms	• Taxonomy levels: – First level: cloud roles (service provider, consumer, cloud broker, cloud carrier and cloud auditor) – Second level: activities performed by each role (cloud management, service deployment, cloud access and service consumption) – Third and following levels: elements which compose each activity (deployment models, service types and auditing elements) • Based on publication SP 500-292, highlighting the importance of security, privacy and levels of confidence and trust to increase technology acceptance • Concentrates many useful concepts, such as models for deploying or classifying services

Table summarizing information on ENISA and NIST security frameworks.

Associations such as the Enterprise Strategy Group [72] emphasize the need for hypervisor security, shrinking hypervisor footprints, defining the security perimeter virtualization, and linking security and VM provisioning for better resource management. Aiming to address these requirements, they suggest the use of increased automation for security controls, VM identity management (built on top of Public Key Infrastructure and Open Virtualization Format) and data encryption (tightly connected to state-of-art key management practices). Wallom *et al.* [73] emphasize the need of guaranteeing virtual machines' trustworthiness (regarding origin and identity) to perform security-critical computations and to handle sensitive data, therefore presenting a solution which integrates Trusted Computing technologies and available cloud infrastructures. Dabrowski and Mills [74] used simulation to demonstrate virtual machine leakage and resource exhaustion scenarios leading to degraded performance and crashes; they also propose the addition of orphan controls to enable the virtualized cloud environment to offer higher availability levels while keeping overhead costs under control. Ristenpart *et al.* [44] also explore virtual machine exploitation focusing on information leakage, specially sensitive data at rest or in transit. Finally, Chadwick and Casenove [75] describe a security API for federated access to cloud resources and authority delegation while setting fine-grained controls and guaranteeing the required levels of assurance inside cloud environments. These publications highlight the need of security improvements related to virtual machines and virtualization techniques, concern that this paper demonstrates to be valid and urgent.

Discussion

Considering the points raised 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 (in which the cloud must be strategically and financially considered as a decisive factor).

Another point observed is that, even though adopting a cloud service or provider may be easy, migrating to another is not [76]. After moving local data and processes to the cloud, the lack of standards for protocols and formats directly affects attempts to migrate to a different provider even if this is motivated by legitimate reasons such as non-fulfillment of SLAs, outages or provider bankruptcy [77]. Consequently, the first choice must be carefully made, as SLAs are not perfect and services outages happen at the same pace that resource sharing, multi-tenancy and scalability are not fail proof. After a decision 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 them into 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.

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 such a context with high distribution of complex services and web-based applications, thus requiring more sophisticated approaches. At the same time, our quantitative analysis indicates that virtualization remains an underserved area regarding the number of solutions provided to identified concerns.

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 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 there 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 a focus of future work in the area. We are also working on a testbed based on OpenStack for researches related to identity and credentials management in the cloud environment. This work should address basic needs for better security mechanisms in virtualized and distributed architectures, guiding other future researches in the security area.

Competing interests

The authors declare that they have no competing interests.

Author's contributions

NG carried out the security research, including the prospecting for information and references, categorization, results analysis, taxonomy creation and analysis of related work. CM participated in the drafting of the manuscript as well as in the analysis of references, creation of the taxonomy and revisions of the text. MS, FR, MN and MP participated in the critical and technical revisions of the paper including the final one, also helping with the details for preparing the paper to be published. TC coordinated the project related to the paper and also gave the final approval of the version to be published. All authors read and approved the final manuscript.

Acknowledgements

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

Author details

[1]Escola Politécnica at the University of São Paulo (EPUSP), São Paulo, Brazil. [2]Ericsson Research, Stockholm, Sweden. [3]Ericsson Research, Ville Mont-Royal, Canada. [4]State University of Santa Catarina, Joinville, Brazil.

Received: 30 January 2012 Accepted: 5 June 2012
Published: 12 July 2012

References

1. IDC (2009) Cloud Computing 2010 – An IDC Update. slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update
2. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson DA, Rabkin A, Stoica I, Zaharia M (2009) Above the Clouds:

A Berkeley View of Cloud Computing. Technical Report UCB/EECS-2009-28, University of California at Berkeley, eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html
3. Rimal BP, Choi E, Lumb I (2009) A Taxonomy and, Survey of Cloud Computing Systems. In: Fifth International Joint Conference on INC, IMS and IDC, NCM '09, CPS. pp 44–51
4. Shankland S (2009) HP's Hurd dings cloud computing, IBM. CNET News
5. Catteddu D, Hogben G (2009) Benefits, risks and recommendations for information security. Tech. rep., European Network and Information Security Agency, enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
6. CSA (2009) Security Guidance for Critical Areas of Focus in Cloud Computing. Tech. rep., Cloud Security Alliance
7. Mather T, Kumaraswamy S (2009) Cloud Security and privacy: An Enterprise Perspective on Risks and Compliance. 1st edition. O'Reilly Media
8. Chen Y, Paxson V, Katz RH (2010) What's New About Cloud Computing Security? Technical Report UCB/EECS-2010-5, University of California at Berkeley, eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html
9. Mell P, Grance T (2009) The NIST Definition of Cloud Computing. Technical Report 15, National Institute of Standards and Technology, www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf
10. Ibrahim AS, Hamlyn-Harris J, Grundy J (2010) Emerging Security Challenges of Cloud Virtual Infrastructure. In: Proceedings of APSEC 2010 Cloud Workshop, APSEC '10
11. Gonzalez N, Miers C, Redígolo F, Carvalho T, Simplício M, Naslund M, Pourzandi M (2011) A quantitative analysis of current security concerns and solutions for cloud computing. In: Proceedings of 3rd IEEE CloudCom. Athens/Greece: IEEE Computer Society
12. Hubbard D, Jr LJH, Sutton M (2010) Top Threats to Cloud Computing. Tech. rep., Cloud Security Alliance. cloudsecurityalliance.org/research/projects/top-threats-to-cloud-computing/
13. Tompkins D (2009) Security for Cloud-based Enterprise Applications. http://blog.dt.org/index.php/2009/02/security-for-cloud-based-enterprise-applications/
14. Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On Technical Security Issues in Cloud Computing. In: IEEE Internation Conference on Cloud Computing. pp 109–116
15. TrendMicro (2010) Cloud Computing Security - Making Virtual Machines Cloud-Ready. Trend Micro White Paper
16. Genovese S (2009) Akamai Introduces Cloud-Based Firewall. http://cloudcomputing.sys-con.com/node/1219023
17. Hulme GV (2011) CloudPassage aims to ease cloud server security management. http://www.csoonline.com/article/658121/cloudpassage-aims-to-ease-cloud-server-security-management
18. Oleshchuk VA, Køien GM (2011) Security and Privacy in the Cloud - A Long-Term View. In: 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology (Wireless VITAE), WIRELESS VITAE '11. pp 1–5, http://dx.doi.org/10.1109/WIRELESSVITAE.2011.5940876
19. Google (2011) Google App Engine. code.google.com/appengine/
20. Google (2011) Google Query Language (GQL). code.google.com/intl/en/appengine/docs/python/overview.html
21. StackOverflow (2011) Does using non-SQL databases obviate the need for guarding against SQL injection? stackoverflow.com/questions/1823536/does-using-non-sql-databases-obvia
te-the-need-for-guarding-against-sql-injection
22. Rose J (2011) 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
23. Balkan A (2011) Why Google App Engine is broken and what Google must do to fix it. aralbalkan.com/1504
24. Salesforce (2011) Salesforce Security Statement. salesforce.com/company/privacy/security.jsp
25. Espiner T (2007) Salesforce tight-lipped after phishing attack. zdnet.co.uk/news/security-threats/2007/11/07/salesforce-tight-lipped-after-phishing-attack-39290616/
26. Yee A (2007) Implications of Salesforce Phishing Incident. ebizq.net/blogs/security_insider/2007/11/-implications_of_salesforce_phi.php
27. Salesforce (2011) Security Implementation Guide. login.salesforce.com/help/doc/en/salesforce_security_impl_guide.pdf
28. Li H, Dai Y, Tian L, Yang H (2009) Identity-Based Authentication for Cloud Computing. In: Proceedings of the 1st International Conference on Cloud Computing, CloudCom '09
29. Amazon (2011) Elastic Compute Cloud (EC2). aws.amazon.com/ec2/
30. Kaufman C, Venkatapathy R (2010) Windows Azure Security Overview. go.microsoft.com/?linkid=9740388, [August]
31. McMillan R (2010) Google Attack Part of Widespread Spying Effort. PCWorld
32. Mills E (2010) Behind the China attacks on Google. CNET News
33. Arrington M (2010) Google Defends Against Large Scale Chinese Cyber Attack: May Cease Chinese Operations. TechCrunch
34. Bosch J (2009) Google Accounts Attacked by Phishing Scam. BrickHouse Security Blog
35. Telegraph T (2009) Facebook Users Targeted By Phishing Attack. The Telegraph
36. Pearson S (2009) Taking account of privacy when designing cloud computing services. In: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, CLOUD '09
37. Musthaler L (2009) Cost-effective data encryption in the cloud. Network World
38. Yan L, Rong C, Zhao G (2009) Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography. In: Proceedings of the 1st International Conference on Cloud Computing, CloudCom '09
39. Tech C (2010) Examining Redundancy in the Data Center Powered by the Cloud and Disaster Recovery. Consonus Tech
40. Lyle M (2011) Redundancy in Data Storage. Define the Cloud
41. Dorion P (2010) Data destruction services: When data deletion is not enough. SearchDataBackup.com
42. Mogull R (2009) Cloud Data Security: Archive and Delete (Rough Cut). securosis.com/blog/cloud-data-security-archive-and-delete-rough-cut/
43. Messmer E (2011) Gartner: New security demands arising for virtualization, cloud computing. http://www.networkworld.com/news/2011/062311-security-summit.html
44. Ristenpart T, Tromer E, Shacham H, Savage S (2009) Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM conference on Computer and communications security, CCS '09. New York, NY, USA, ACM, pp 199–212, doi.acm.org/10.1145/1653662.1653687
45. Chow R, Golle P, Jakobsson M, Shi E, Staddon J, Masuoka R, Molina J (2009) Controlling data in the cloud: outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM workshop on, Cloud computing security, CCSW '09. New York, NY, USA, ACM, pp 85–90, http://doi.acm.org/10.1145/1655008.1655020
46. Sadeghi AR, Schneider T, Winandy M (2010) Token-Based Cloud Computing - Secure Outsourcing of Data and Arbitrary Computations with Lower Latency. In: Proceedings of the 3rd international conference on Trust and trustworthy computing, TRUST '10
47. Brandic I, Dustdar S, Anstett T, Schumm D, Leymann F (2010) Compliant Cloud Computing (C3): Architecture and Language Support for User-driven Compliance Management in Clouds. In: 2010 IEEE 3rd International Conference on Cloud Computing. pp 244–251, http://dx.doi.org/10.1109/CLOUD.2010.42
48. Brodkin J (2008) Gartner: Seven cloud computing security risks. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853
49. Kandukuri BR, Paturi R, Rakshit A (2009) Cloud Security Issues. In: Proceedings of the 2009 IEEE International Conference on Services Computing, SCC '09
50. Winterford B (2011) Amazon EC2 suffers huge outage. http://www.crn.com.au/News/255586,amazon-ec2-suffers-huge-outage.aspx
51. Clarke G (2011) Microsoft BPOS cloud outage burns Exchange converts. http://www.theregister.co.uk/2011/05/13/
52. Shankland S (2011) Amazon cloud outage derails Reddit, Quora
53. Young E (2009) Cloud Computing - The role of internal audit
54. CloudAudit (2011) A6 - The automated audit, assertion, assessment and assurance API. http://cloudaudit.org/
55. Anand N (2010) The legal issues around cloud computing. http://www.labnol.org/internet/cloud-computing-legal-issues/14120/

56. Hunter S (2011) 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/
57. Sharon D, Nelson JWS (2011) 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/
58. Bentley L (2009) 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
59. Zierick J (2011) The special case of privileged users in the sloud. http://blog.beyondtrust.com/bid/63894/The-Special-Case-of-Privileged-Users-in-the-Cloud
60. Dinoor S (2010) Got Privilege? Ten Steps to Securing a Cloud-Based Enterprise. http://cloudcomputing.sys-con.com/node/1571649
61. Pavolotsky J (2010) Top five legal issues for the cloud. http://www.forbes.com/2010/04/12/cloud-computing-enterprise-technology-cio-network-legal.html
62. ENISA (2011) About ENISA. http://www.enisa.europa.eu/about-enisa
63. CSA (2011) About. https://cloudsecurityalliance.org/about/
64. CSA (2011) CSA TCI Reference Architecture. https://cloudsecurityalliance.org/wp-content/uploads/2011/11/TCI-Reference-Architecture-1.1.pdf
65. CSA (2011) Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. Tech. rep., Cloud Security Alliance. [Http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf]
66. Ramireddy S, Chakraborthy R, Raghu TS, Rao HR (2010) Privacy and Security Practices in the Arena of Cloud Computing - A Research in Progress. In: AMCIS 2010 Proceedings, AMCIS '10. http://aisel.aisnet.org/amcis2010/574
67. NIST (2011) NIST Cloud Computing Reference Architecture: SP 500-292. http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf
68. Youseff L, Butrico M, Silva DD (2008) Toward a Unified Ontology of Cloud Computing. In: Grid Computing Environments Workshop, 2008. GCE '08. pp 10, 1, http://dx.doi.org/10.1109/GCE.2008.4738443
69. Johnston S (2008) Sam Johnston: taxonomy: the 6 layer cloud computing stack. http://samj.net/2008/09/taxonomy-6-layer-cloud-computing-stack.html]
70. Linthicum D (2009) Defining the cloud computing framework. http://cloudcomputing.sys-con.com/node/811519
71. Doelitzscher F, Reich C, Knahl M, Clarke N (2011) An autonomous agent based incident detection system for cloud environments. In: Third IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2011, CPS. pp 197–204, http://dx.doi.org/10.1109/CloudCom.2011.35
72. Oltsik J (2010) Information security, virtualization, and the journey to the cloud. Tech. rep., Cloud Security Alliance
73. Wallom D, Turilli M, Taylor G, Hargreaves N, Martin A, Raun A, McMoran A (2011) myTrustedCloud: Trusted Cloud Infrastructure for Security-critical Computation and Data Managment. In: Third IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2011, CPS. pp 247–254
74. Dabrowski C, Mills K (2011) VM Leakage and Orphan Control in Open-Source Clouds. In: Third IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2011, CPS. pp 554–559
75. Chadwick DW, Casenove M (2011) Security APIs for My Private Cloud. In: Third IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2011, CPS. pp 792–798
76. Claybrook B (2011) How providers affect cloud application migration. http://searchcloudcomputing.techtarget.com/tutorial/How-providers-affect-cloud-application-migration
77. CSA (2011) Interoperability and portability

doi:10.1186/2192-113X-1-11
Cite this article as: Gonzalez *et al.*: **A quantitative analysis of current security concerns and solutions for cloud computing.** *Journal of Cloud Computing: Advances, Systems and Applications* 2012 **1**:11.