Cloud Security: State of the Art

Liliana F. B. Soares, Diogo A. B. Fernandes, João V. Gomes, Mário M. Freire and Pedro R. M. Inácio

1 Introduction

Throughout the end of the first half and during the second half of the past century, advances in technology allowed scientists to develop computer systems. In the beginning, mostly between the forties and the sixties, single computers would fill large rooms with electronics that would consume as much power as several hundreds of modern desktop computers. However, a diversity of revolutionary approaches were invented throughout the time, gradually replacing those large, and expensive, computer rooms with smaller, more powerful computers, being able to hold many of them. This allowed computer systems and networks to emerge, like standard Ethernet networks that still persist today. Distributed systems, one of those approaches, arose as a means to aggregate computational assets with the main goal of supporting highly intensive and hardware-demanding tasks, which can consume several processing resources simultaneously and last for a long time. Examples of such tasks include molecular modeling, scientific simulations and weather forecasts.

L. F. B. Soares (✉) · D. A. B. Fernandes · J. V. Gomes ·
M. M. Freire · P. R. M. Inácio
Instituto de Telecomunicações, Department of Computer Science,
University of Beira Interior Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal
e-mail: lsoares@penhas.di.ubi.pt

D. A. B. Fernandes
e-mail: dfernandes@penhas.di.ubi.pt

J. V. Gomes
e-mail: jgomes@di.ubi.pt

M. M. Freire
e-mail: mario@di.ubi.pt

P. R. M. Inácio
e-mail: inacio@di.ubi.pt

S. Nepal and M. Pathan (eds.), *Security, Privacy and Trust in Cloud Systems*,
DOI: 10.1007/978-3-642-38586-5_1,

1.1 Computer Clusters, Grids and Clouds

Two of the most typical distributed systems are computer clusters and computer grids. As the name suggests, computer clusters consist of coupled hardware resources that can function standalone. These resources are put on a centralized point, usually a large, cooled, well protected room, leading to expensive approaches. Clusters enhance computational, memory and storage capabilities of computer systems, therefore requiring specially designed middleware to support communications between each hardware node. In addition, this type of architecture for computer systems requires bandwidth-wise network links to support large amounts of intracommunications network traffic. However, nowadays, open-source software enables the use of processing units and memory from desktop computers to dispatch distributed, potentially parallel tasks by nominating a master node that manages the cluster. This approach can reduce implementation costs to companies rather than spending big on supercomputers or expensive clusters. Grid systems, on the other hand, are not as coupled as clusters and dwell over large scattered and heterogeneous networks in a decentralized fashion. The most prominent example is the Internet, over which grids are deployed as overlay networks. In fact, the most well-known form of grids is the one of using typical desktop and home computers as end slave computation nodes. This approach, however, brings obstacles, such as increased management complexity, task assignment, and results collecting and gathering.

Based on the cluster and grid computing paradigms [35, 90], cloud computing has emerged in the last few years as the latest approach with the purpose of computing as utility. In fact, grid computing provides the backbone and supporting infrastructure for clouds [35]. It was around 2008 that the cloud computing subject started gaining serious interest among the industry and the academia. Additionally, to provide a better perspective, the *utility computing* term was first invoked as early as 1965 [23]. It refers to computational resources efficiently wrapped as services, being more a business model rather than a computing paradigm today, and matching the cloud business model. Analogously to clusters, clouds are composed of umpteen servers placed in large, cooled, well protected rooms under the same subnet. Facilities that host clouds are nowadays called data centers, which require being physically and logically segregated from malicious intrusions because clouds usually hold large amounts of sensitive data belonging to customers. The main innovative side of clouds is how Information Technologies (IT) are put together along with virtualization techniques, providing web service-based and on-demand capabilities accessible over the Internet. To this end, a pay-per-use business model is implemented, meaning that computational, storage or networking resources rented by customers are strictly billed according to their needs, that is, time of usage, assets required, load and security measures. Cloud systems are both centralized and decentralized, allowing public access to their resources via web technologies. Hence, a centralized and distributed resource handling approach is applied, providing multi-tenant and Service-Oriented Architecture (SOA) capabilities, similarly to grids.

1.2 Cloud Security

The National Institute of Standards and Technology (NIST) view of cloud is summarized in version 3 of the security guidance entitled as *Security Guidance for Critical Areas of Focus in Cloud Computing* [24], published by the Cloud Security Alliance (CSA), an organization aiming at promoting the use of best practices in cloud security. In the document, the cloud deployment models, the cloud service delivery models or service models, and the five essential characteristics of clouds are described. The cloud deployment models include public, private, hybrid, and community clouds, and Virtual Private Clouds (VPCs). The service models are divided into Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Finally, the characteristics are broad network access, rapid elasticity, measured service, on-demand self-service, and resource pooling.

The NIST [74] mentions security, interoperability and portability as major barriers for a broader adoption of cloud solutions. There are just a few standards supporting clouds, which translates into the *lock-in* issue faced by customers. In other words, when a customer decides for a certain cloud provider, the data stored on the cloud cannot yet migrate to clouds of other providers. Nonetheless, *interclouds* [11, 88], a term referring to a network of clouds, a place of cloud computing, interoperability, ubiquitous and utility computing, and data storage, would overcome this issue and free data movement among clouds belonging to different providers. Clouds increased the complexity of many previous security issues and introduced new ones, being yet a risky business. To demonstrate how security is one of the most mind changing factor (if not the most important), in 2009, the International Data Corporation (IDC), a market research and analysis firm, has harvested opinions among company Chief Information Officers (CIOs) on the most concerning cloud obstacles. The survey [46] was concluded with the security topic ranking first with 87.5 % of the votes, 12.9 % more than the study on the previous year [47], in which security also led with 74.6 %. The results of the 2009 study are illustrated in Fig. 1. This perspective concerning cloud security is shared with the *Top predictions for IT Organizations and Users for 2012 and Beyond* report [38], property of Gartner, a technology research and advisory company. Because of security, people hesitate to fully move their business into clouds, slowing down their propagation, as the research and the industry are focused on patching security issues, rather than exploring their potentialities. In addition, *"my sensitive corporate data will never be in the cloud"* is a statement that has been heard multiple times [3], further pointing out how critical security is. Because clouds outsource businesses of many customers, which includes potentially sensitive data and applications, they pose as attractive attack targets for cybernetic pirates or *malicious insiders*. Thus, there is much at stake in the cloud business, being *data disclosure*, *data loss* and *financial loss* major risk scenarios. Clouds offer many appealing features and advantages, but until some of its risks are better understood, major players might hold back [106]. This means that cloud systems are a risky business, not only to customers, but also to the providers investments.

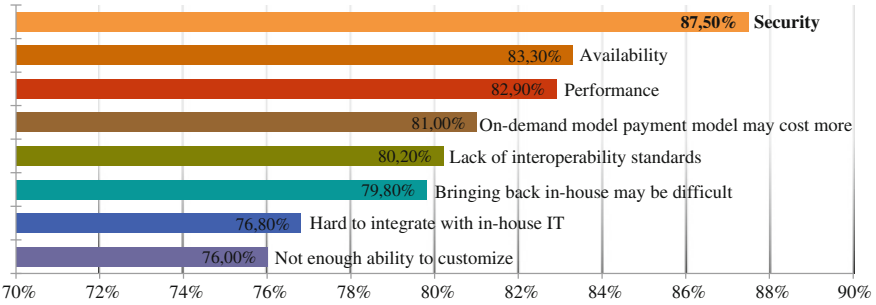

Fig. 1 Challenges and issues of the cloud model according to IDC and corresponding results from the cloud user survey (adapted from [46])

1.3 Organization

The previous paragraphs enlightened on the differences between the cloud, the cluster and the grid computing paradigms, highlighting the most prominent characteristics of these distributed systems. Essentially, the importance of the cloud security topic is highlighted in the discussion, underlining how critical it is to address security issues. To this end, this chapter discusses the most prominent security issues tackled in the literature, surveying vulnerabilities, gaps, threats, attacks, and risks on cloud environments. Such terms are emphasized throughout the text as to better distinguish each issue. Additionally, concepts of both cloud and cloud security subjects are described in order to facilitate the understanding of this chapter. Foremost, the chapter presents a comprehensive analysis of the state-of-the-art on cloud security issues.

The remaining of this chapter is organized as follows. Section 2 delivers an insight on the works that are most similar to the one presented herein. Section 3 overviews some general features of clouds and key concepts of cloud security. Subsequently, in Sect. 4, a discussion of the published literature on security issues in cloud environments is presented. A synthesis of the chapter containing a timeframe overview of what was discussed is included in Sect. 5. The chapter ends with the main conclusions in Sect. 6.

2 Related Work

Cloud security has been in vogue on the literature and industry for a while now. Various international conferences have focused on this subject alone, such as the Association for Computer Machinery (ACM) *Workshop on Cloud ComputingSecurity*, the *International Conference on Cloud Security Management* and the only European conference on the subject, *SecureCloud*, which already numbers up to three editions. As a result, several scientific contributions have been published, not only

in conferences proceedings, but also in international journals and magazines. Thus, there are a few works surveying this area of knowledge that are worthy to describe herein.

The study in [115] surveyed security and privacy concerns of cloud providers. Firstly, the security topic was discussed while having in mind availability, confidentiality, data integrity, control and audit properties, concluding that these do not meet current concerns. Secondly, the privacy topic was discussed with focus on out-of-date privacy acts that fail to protect information from being disclosed to the government and third-parties. In addition, the multi-location issue of clouds is also included in the study, stating that knowing in which country the data will be kept is a prerequisite for customers, in order to find by which laws the data is governed. It was claimed that new strategies should be put forward to achieve the five aforementioned properties and that privacy acts should be changed accordingly.

Again, in [116], the confidentiality, privacy, integrity and availability aspects in clouds were placed under observation. Various issues were discussed so as to present a synthesis of security requirements and threats with respect to the service models. The study ended with the proposal of a trusted third-party solution to eradicate security threats of confidentiality, integrity, authenticity and availability. The solution combined Public Key Infrastructures (PKIs), the Lightweight Directory Access Protocol (LDAP) and Single Sign-On (SSO) with a top-down fashion of the trust tree. The study was concluded with the premise that cloud benefits will outnumber its shortcomings.

Another survey targeting security issues on the cloud service models was presented in [95]. Each model was singularly studied, pointing out some of the most significant security vulnerabilities, threats and risks. It should be noted that the SaaS model was the one with the majority of the issues. An overview of current solutions discussed in the literature is presented afterwards. Yet again, the study was concluded saying that proper solutions should be designed and deployed to allow the cloud industry expand further.

The security and privacy topics were again discussed in [111]. A comprehensive and technical review of security issues was included in the study, in which confidentiality, integrity, availability, accountability and privacy-preservability were identified as the most significant attributes. To each property, a few security issues are described, followed by the corresponding defense solutions. In the end, it was claimed that the study might help shaping the future research directions in the security and privacy contexts in terms of clouds.

In [88], various security challenges were enumerated as key topics in cloud security. Those challenges related with resource allocation, system monitoring and logging, computer forensics, virtualization, multi-tenancy, authentication and authorization, availability, and cloud standards. The study particularly focused afterwards on introducing the Service Level Agreements (SLAs), trust, and accountability topics with regard to cloud security. Issues and solutions were dually discussed throughout the study.

The previous works defined the basis of this chapter by providing materials to review the state-of-the-art on the subject. Nonetheless, the review presented in

this chapter contains a wider analysis when compared to those studies, allowing to construct a broader taxonomy for cloud security issues, leaving aside a deeper analysis of solutions for such issues. As commonly seen in other works, including the ones above, the chapter also discusses basic cloud and cloud security concepts in order to ease its understanding.

3 Security-Related Concepts in Cloud Environments

This section defines and describes some basic concepts on cloud and cloud computing, together with key notions on cloud security. The discussion complements some ideas already included in the Introduction section. Thus, it prepares the reader for the remaining part of the chapter.

3.1 Cloud Service Models

The increasing connection demands of the population have triggered the development of Web 2.0 and a new class of services. Cloud systems have adopted a standard three-model architecture, each one containing fundamental parts to support the cloud unique operation. The architecture is composed of IaaS, PaaS and SaaS, sorted upwardly.

The bottom model, IaaS, revolutionized how businessmen invest in IT infrastructures. Instead of spending large amounts of budget in hardware and technical crews to assemble and manage the materials, IaaS providers offer reliable virtual servers on the minute. Amazon Web Services (AWS) is a real example of such providers. A pay-per-use approach is employed in this model, meaning that customers only pay for what they require. Additionally, it abstracts businesses from the scalability, management and provisioning of the infrastructure, allowing them to focus on promoting their applications. The IaaS model provides basic security, including perimeter firewall and load balancing, as long as the VMM is not compromised. The provider should, at least, ensure security up to the VMM, which includes environmental, physical and virtualization security. IaaS ultimately suffers from the *data locality* and *co-location* issues.

The middleware model, PaaS, delivers abilities for customers to develop their own cloud applications by providing platforms and frameworks. Consequently, this model becomes more extensible than SaaS by providing a set of customer-ready features, therefore administrating greater flexibility in security. Thus, *unsafe* Integrated Development Environments (IDEs) and Application Programming Interfaces (APIs) may constitute vulnerability points. Furthermore, because the underlying elements of SOA applications are obscured by the architecture, cybernetic pirates are most likely to attack visible code written by users. A set of coding metrics should be put forward to evaluate the quality of code written by those users.

The top model, SaaS, allows applications to be remotely deployed and hosted on clouds, delivering on-demand capabilities in the form of services that can be accessed via the Internet. This model improves operational efficiency and also reduces costs to customers, similarly to IaaS. It is rapidly becoming prevalent in the cloud business as it is rapidly meeting the requirements of IT companies. However, several security issues are raised by this model, mostly related with data storage, thus making customers uncomfortable in adopting SaaS solutions. Cloud providers must assure data isolation, confidentiality and privacy, meaning that users should not access nor understand data from other users. Nonetheless, from the customer viewpoint, it is hard to tell whether or not the data is well secured, and that applications are available at all times. Furthermore, it is harder to preserve or enhance security that was formerly provided by previous systems.

Although the three service models make up the foundations for the cloud operation, the IT industry is assisting to a mutation; it is converging to Anything-as-a-Service (XaaS). Because clouds are virtually infinite and can, therefore, support anything, or everything, in the form of services, the XaaS approach is able to deliver a wide range of services, including large resources and specific requirements.

3.2 Data Center Facilities Security

As previously said, clouds are computer systems put on specially designed rooms to hold a massive number of servers and network links. Cooling is an active research area in which many approaches are proposed and implemented with the purpose of producing efficient facilities. Protection is other topic of concern when mentioning such facilities. Rooms in such infrastructures hold many expensive network, computation and storage devices, and private data, therefore requiring proper security. In fact, entrepreneurs build data centers while having in mind many geological and environmental aspects, such as location, temperature, humidity, and earthquakes. Other political, governmental, and energy-saving aspects are also taken into consideration. For instance, grid redundancy [22] is a technique used to assure power continuity to devices, by tolerating loss of any power supply or a single alternating current power source. The goal is to provide the most possible reliable facilities to achieve high availability [19], reaching 99.99 % uptime in many cases, and being fully fault-tolerant. Hence, many data centers achieve the tier 4 level, which is the highest level defining the quality of data centers, being the lowest tier 1.

Physical security is established on-site in the data center facilities. If this prerequisite would not be fulfilled, other security measures would be unnecessary. For example, a security center managing video cameras, security sensors, personnel entrances and access to resources may be the most adopted approach. All this to prevent break-ins and other physical violations. Nonetheless, physical access to the rooms holding equipments should be restricted and only exclusive personnel with security clearances should go in to perform managing operations.

Flooding attacks, *hardware interruption*, *theft*, *modification*, *infrastructure misuse* and *natural disasters* are amongst the main issues of data center facilities [116].

Clouds contain service-driven networks, Storage Area Networks (SANs), and computational and storage-related hardware, which should be dully protected by resorting to firewalls and Intrusion Detection Systems (IDSes), like in standard networks. This approach would enable the analysis of network traffic and the detection or prevention of malicious intrusion attempts [62, 67]. Various IDS solutions have been provided [27, 61, 84]. It is recommended to deploy both IDS and Intrusion Prevention System (IPS) in clouds in order to achieve the desired security level [70]. Honeypots should also be considered, so as to divert attackers attentions [93]. Nonetheless, it should be paid some attention to the trade-off between security and performance [78], because too many security deployments may cause disruptions. Amazon Elastic Compute Cloud (EC2), for example, provides a firewall solution to each customer. By default, it is configured in deny mode, and customers must configure ports to allow incoming traffic for hosted services. The firewall has the ability of restricting traffic by protocol, port, and Internet Protocol (IP) address [1, 8].

3.3 Cloud Stakeholders

The players intervening in the cloud business define how the infrastructure is used and managed. In a simplified way, clouds have virtualized platforms that abstract the underlying hardware, and have services running on top of those platforms. Cloud providers own data center facilities and, therefore, have the responsibility of managing the facilities and the hardware resources in them. Service providers are another, but optional, stakeholder that can rent cloud resources to a cloud provider. In turn, service providers can deliver computational, storage and networking capabilities in the form of services to cloud customers. At all times, SLAs are negotiated in order to define the terms of service and what the cloud customer requires. Ideally, the optimal SLA should cover all critical security requirements. Traditionally, however, the extent of SLAs implemented in the industry does not fully include confidentiality and integrity aspects [88], mainly due to the challenges related with storage outsourcing. End users, which are also part of the model, are the ones that ultimately enjoy the services. This model is schematized in Fig. 2, where two distinct service providers

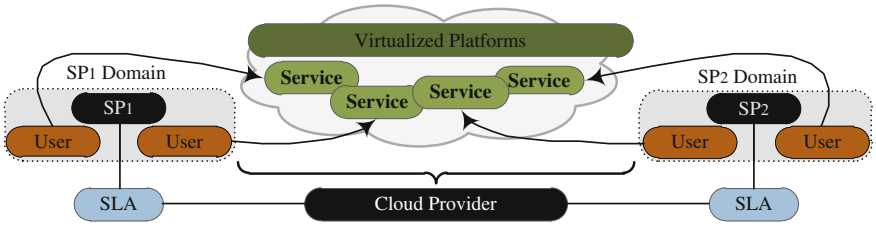

Fig. 2 Cloud stakeholders model adapted from [64, 115]. SP stands for service provider

hosting their services on the same cloud are illustrated. A noteworthy aspect is that, while cloud customers are responsible for application-level security, providers are responsible for physical and logical security. Intermediate layers of the cloud stack are shared between one another. Cloud customers may outsource their responsibility in security aspects to third-parties, who sell specialized security services.

3.4 Important Concepts in Cloud Security

As clouds rely on virtualization techniques, it is important to identify and describe which elements provide the backbone for virtualization. Thanks to it, a multi-tenant ability is implemented in clouds, meaning that users access applications specially designed to run on cloud platforms. Therefore, it is also important to discuss cloud software with focus on security. Moreover, clouds hold massive amounts of data from cloud customers, which is the main reason why data outsourcing and data storage are critical concepts to discuss. Consequently, standardization is also an issue relevant to include in cloud storage discussions. Finally, trust is briefly discussed from the outsourcing business model standpoint. These concepts are analyzed below, providing the means to clarify and identify the source of some cloud vulnerabilities and threats.

3.4.1 Virtualization Elements

Virtualization itself, or Virtual Machine (VM), is the process of abstracting computer applications, services and Operating Systems (OSes) from the hardware on which they run [93]. Virtualization technologies are placed within the IaaS model. Virtualized OSes are called guest OSes or just guests. The benefits of virtualization include costs and downtime reduction, ease of management and administration, and scalability [14]. Notwithstanding, it brought many new problems intrinsic to its nature, which researchers and entrepreneurs have tried to patch. A VM image is a pre-built copy of the memory and storage contents of a particular VM. VM images can be easily cloned or moved to another location while keeping the integrity of its contents. This allows clouds to deliver highly available services, that is, it keeps VMs running on other physical resources if the previous resources were compromised or allocated for other operations or VMs. Hence, it is perceivable that VMs require a middleware layer to support such operations, which is done by the help of Virtual Machine Monitors (VMMs), usually called hypervisors, and cloud computing OSes. Examples of popular hypervisors are VMware Player, VirtualBox and Xen. Cloud computing OSes are similar to traditional OSes, but provide an additional set of virtualization functionalities, such as allocation and deallocation of VMs, dispatching and migration of processes, and setup interprocess communications, in order to support autonomous scaling and opportunistic deployment of SaaS applications [81]. This would all be great if no security issues arose. However, virtualization brings

abstraction in *data locality*, which means that cloud users cannot pin-point the exact physical location of their data, as VMs can be moved from one machine to another autonomously by the underlying layers. Furthermore, data leakage by exploring VM or hypervisor vulnerabilities is the main virtualization risk.

3.4.2 Multi-Tenancy

Multi-tenancy is a virtualization feature that, apart from clouds, it is also present in grid systems. It consists of multiple users, called tenants, sharing a common platform or a single instance of an application. In a public cloud scenario, various customers may share the same VMMs and physical resources, but each one accesses its own VM with inherent SLAs, different security configurations and billing policies.

3.4.3 Cloud Software

Although virtualization brings many new issues, issues already prevalent in software developing are transported to clouds. These type of issues scatter over the PaaS and SaaS models, bringing up vulnerabilities in APIs and IDEs, and web technologies, respectively. For instance, bad programming approaches in deploying cloud applications or common Cross-Site Scripting (XSS) attacks can exploit vulnerabilities in these models. Therefore, each service model contains its own problems, raising concerns in the cloud business model.

3.4.4 Data Outsourcing

Outsourcing is the process of contracting services from third-party entities. In the context of cloud systems, data outsourcing consists in renting storage services off of cloud providers to store data from the customer on-premises. This approach brings both capital expenditure (CapEx) and operational expenditure (OpEx) to customers. However, more importantly, brings physical separation between the customers and their data, an issue called *loss of control* [111]. This has been one of the main motivations feeding customers contingency about moving their businesses into clouds. To overcome this, providers must be trustworthy and guarantee secure computing and data storage.

3.4.5 Data Storage Security and Standardization

Mechanisms to ensure information security must be applied to data stored in cloud systems. Cryptography approaches must be employed to ensure classical security properties, that is, confidentiality and privacy, integrity, authentication and availability. To this end, cloud providers should provide trusted encryption schemas

and application-level protocols, as well as authentication mechanisms and integrity checking techniques to ensure that data was not tampered with. This implies the use of secure communication protocols and standards. Nonetheless, the latest, standardization, poses as one of the cloud main barriers, complicating interoperability and the development of *interclouds*. Furthermore, applying classical security techniques may be impractical in cloud systems due to the great amount of data stored in their servers. Thinking on hashing entire data sets provides a good example on the issue, since it would require abnormal computational and communication overhead. New mechanisms are nonetheless expected to be developed, such as homomorphic encryption [92] that enables processing encrypted data without being decrypted, ideal for public clouds. Data backups and restores are also essential for the correct functioning of clouds. To this end, providers usually supply geographic redundancy to data, meaning that data is copied to different geographical locations, usually to another data center of the same cloud provider.

3.4.6 Trust

Trust is a critical barrier that must be surpassed in the cloud business model. Firstly, cloud customers must trust in the cloud systems of providers that are going to store their data. Secondly, providers must trust customers with access to the services, that is, access to clouds, which translates into one of the cloud main security issues. Malicious users can conceal attacks by perpetuating them as apparently legitimate users, like the *co-location* attack. Consequently, SLAs must be well detailed in order to legally cover all possible atypical scenarios in case of unexpected consequences of misusing the cloud infrastructure for both the client or for third-parties. Another important aspect in the trust topic is the pro-activity of cloud users in terms of security. Consider that users use low secure passwords to authenticate in the cloud via web, such as the passwords most used throughout the cybernetic world as shown by SplashData, a company dedicated to address password concerns in IT, in the Worst Passwords of 2012 [94]. The study was compiled by using millions of passwords posted online by hackers and it was concluded that the word *password* is the most common password. Several distinct characters should be used in order to assemble enough entropy. Moreover, most employees share their passwords with a coworker, a friend, or a friend of a coworker even after receiving password training [101]. This is a major problem, not only in clouds, but to all Internet systems, as unnoticed intrusions can happen.

3.5 General and Cloud-Specific Issues

A *security issue* is a general term that includes several problems. Vulnerabilities, gaps, threats, attacks, and risks are adequate sub-terms that derive from the issue term. It is important to distinguish the difference in these commonly used terms in

the security field [26]. *Threat* is a situation that may exploit a *vulnerability*, which is a flaw or weakness of a system, as in *gap*. *Attack* is the act of exploiting a threat, while *risk* is the likelihood of a threat agent taking advantage of a vulnerability and corresponding business impact. Moreover, people on the cloud security field tend to misunderstand the difference between general and cloud-specific issues, as that difference is not crisp enough [41]. Cloud computing heavily builds on capabilities available through several core technologies, which include web applications, the cloud service models, virtualization IaaS offerings, and cryptography mechanisms. A cloud-specific security issue must be intrinsic to or prevalent in a core technology. It has to have its root cause in one of the five essential characteristics proposed by the NIST, it is provoked when innovations make tried-and-tested security controls difficult or impossible to implement, or it is prevalent in established state-of-the-art cloud offerings. Only cloud-specific issues are included in the chapter.

3.6 Categorization of Cloud Security Issues

Researchers tend to define their own taxonomy on cloud security issues as there is not yet a *de facto* standard to follow. The study described in [92] mentions four categories, namely *cloud infrastructure*, *platform and hosted code*, *data*, *access*, and *compliance*. Another study [59] organized security issues into a model with three main sections, named security categories, security dimensions and security in the service models. Security categories span from *cloud customers* to *providers*, which can also be complemented with government entities [15], while security dimensions include *domains*, *risks* and *threats*. For instance, the *isolation failure* threat is due to virtualization vulnerabilities, therefore being placed on the IaaS model, posing as an issue to both customers and providers. In this chapter, the assessment of existing security issues in cloud security is done with basis on the previously discussed studies. This chapter considers *software-related*; *data storage and computation*; *virtualization*; *networking, web and hardware resources*; *access*; and *trust* as the most direct, in terms of threat identification, and embracing security issues set of categories in the cloud context.

4 Main Cloud Security Issues

Due to the growth of the cloud in the industry, entrepreneurs have decided to adopt cloud services, in spite of being aware of its security issues. Thus, clouds attract attention from a potential dangerous community and other parties aiming to exploit security vulnerabilities, and to perhaps publicly disclose private information. Malicious activities are motivated by a wide panoply of reasons, namely personal benefit, glory or vendetta. Therefore, it is important to address such security issues, which

are thoroughly reviewed in this section. This review is supported by a comprehensive study of the state-of-the-art on the subject.

4.1 Security Issues Identified by Organizations

The cloud security topic concerns not only the research community, but also the industry. Various documents have been published with the intent of aiding the development of trustworthy cloud systems. Nonetheless, customers should get a security assessment from third-parties before committing to a cloud provider. The following works, described in chronological order, are considered pioneering works on the subject [59].

The Gartner published the security document entitled *Assessing the Security Risks of Cloud Computing* [37]. In this document, seven security risks are identified as critical aspects to be considered by cloud customers before committing to a provider. They are privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, and long-term viability.

The European Network and Information Security Agency (ENISA), an organization responsible for responding to cyber security issues in the European Union, provided the document entitled *Cloud Computing:Benefits, Risks and Recommendations* [33]. Eight cloud specific risks are considered as top risks also from the customer viewpoint. They are loss of governance, *lock-in*, *isolation failure*, compliance risks, management interface compromise, data protection, insecure of incomplete data deletion, and malicious insider.

The CSA published version 1 of the document *Top Threatsto Cloud Computing* [25]. Besides describing each top threat, real life examples and remediation directions are provided. In addition, to each threat, references to the domains of the following document are included, along with the service models affected, which are summarized in Table 1 except for the domains. As can be concluded from the analysis of the table, all threats affect the three service models, except for two threats, illustrating

Table 1 Top threats to cloud computing as described in CSA [25], plus the domains in which they are included and the service models they affect. A check mark ✓ means the threat affects the underlying model. A cross × means otherwise

Threat #	Name	IaaS	PaaS	SaaS
1	Abuse and Nefarious use of cloud computing	✓	✓	×
2	Insecure interfaces and APIs	✓	✓	✓
3	Malicious insiders	✓	✓	✓
4	Shared technology issues	✓	×	×
5	Data loss or leakage	✓	✓	✓
6	Account of service Hijacking	✓	✓	✓
7	Unknown risk profile	✓	✓	✓

Table 2 Summary of the main characteristics of the cloud deployment models, regarding Ownership (Organization (O), Third-Party (TP), or Both (B)), Management (O, TP, or B), Location (Off-site, On-site, or B), Cost (Low, Medium, or High), and Security (Low, Medium, or High)

Model	Ownership	Management	Location	Cost	Security
Public	TP	TP	Off-site	Low	Low
Private and community	O or TP	O or TP	On-site	High	High
Hybrid	O and TP	O and TP	On-site and Off-site	Medium	Medium
VPC	B	B	B	B	High

how important it is to address security issues. Threat #4 only affects IaaS because it is where shared virtualization resources are located.

The CSA also published version 3 of the report *Security Guidance for Critical Areas of Focus in Cloud Computing* [24]. Fourteen domains are identified in report, namely cloud computing architectural framework (domain #1), governance and enterprise risk management (domain #2), legal and electronic discovery (domain #3), compliance and audit (domain #4), information lifecycle management (domain #5), portability and interoperability (domain #6), traditional security, business continuity and disaster recovery (domain #7), data center operations (domain #8), incident response (domain #9), application security (domain #10), encryption and key management (domain #11), identity and access management (domain #12), virtualization (domain #13), and security as a service (domain #14).

4.2 Deployment Models and Service Delivery Models Security

The cloud provides different deployment models that have their own characteristics, advantages and disadvantages. Table 2 summarizes the characteristics of the public, private, community, hybrid, and VPC deployment models. While public clouds are cheaper, located on-site, owned and managed by third-party entities, private clouds are more expensive, as they require specialized technicians and hardware, are located on-site, usually behind corporate firewalls, and can be owned and managed either by the organizations itself or a third-party. Private clouds are therefore more secure than public clouds. Community clouds are a particular case of private approaches, has they are setup to support a common interest between several distinct owners. Hybrid clouds mix up both public and private models. Moreover, VPCs are also a particular case of private models, resembling Virtual Private Networks (VPNs) in the sense of a network that is built on top of another network, removing the concerns related with operating in shared or public environments.

A cloud customer should deliberate the security state of each model before committing to a specific one, in order to conduct a strategic evaluation and be aware of current issues. More specifically, an assessment from the business perceptive should be performed in terms of security requirements. To this end, Table 3 intersects the

Table 3 Service models versus the public, private and hybrid deployment models with respect to security requirements as described by [83]

Security requirements	Cloud deployment models								
	Public cloud			Private cloud			Hybrid cloud		
Identification & Authentication	✓	∗	✓	✓	∗	✓	∗	∗	✓
Authorization	✓	✓	✓	∗	∗	✓	∗	∗	✓
Confidentiality	∗	∗	✓	∗	✓	✓	∗	∗	✓
Integrity	✓	∗	✓	∗	✓	✓	✓	✓	✓
Non-repudiation	∗	∗	✓	∗	∗	✓	∗	∗	∗
Availability	✓	✓	∗	✓	✓	✓	∗	∗	∗
	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS
	Cloud service models								

A check mark (✓) means an obligatory requirement in that specific service model and in the underlying deployment model, while an asterisk (∗) means optional

cloud deployment and service models with respect to six security requirements [83]. As can be concluded from the analysis of the table, authorization requirements on the three service models are mandatory in public clouds, so as to prevent unauthorized access to assets. The hybrid model is less demanding in terms of security requirements than both public and private models, as it is more secure. Amongst the three deployment models, integrity properties are much desired, pointing out the interest in checking data correctness and if it was tampered with or corrupted. Moreover, SaaS is the service model with more security requirements throughout all underlying deployment models. The study in [95] corroborates this trend, showing that a great deal of security issues is included in the SaaS, when compared to the remaining models. Particular issues arise in public clouds as specific pieces of data may be amongst other types of data potentially unrelated due to the SaaS model. The next sub-subsections discuss the cloud service models with more detail.

Subsequent subsections perform an extensive review of the state-of-the-art security issues in cloud environments, looking into vulnerabilities, gaps, threats, attacks, risks, and general problems that affect the cloud business. Naturally, those issues can relate to specific deployment or service models, thereupon complementing previous discussions. The review is conducted with basis on the taxonomy defined in Sect. 3.6.

4.3 Software-Related Security Issues

Software security is and has been a vital part of computer systems. Normally, large applications with thousands of lines of code, or even millions, are written by several different people with distinct programming skills and ideals. Managing such applications is a hard task and gives rise to software holes that can be exploited by malicious users. Additionally, programmers find it more attractive to provide functional, fancy software, sometimes caring more about the interface and functionality, than security

and reliability. Moreover, open-source software is free and its code is exposed to analysis, easing the search for bugs to be explored. Software security is a system-wide issue that takes into account both security mechanisms and design with security purposes, and ends up in robust programming approaches to harden software and hamper attacks [12]. Hence, software security should be part of a full design and development lifecycle, and should start being considered in all software engineering phases [68, 77]. In the cloud context, software security is intrinsic to the PaaS and SaaS models. The following subsections cover security issues related with *multi-tenancy*, *platforms and frameworks*, *user frontend*, and *control*.

4.3.1 Multi-Tenancy

The multi-tenancy feature stems from the virtualization layer and allows storing information from multiple customers at the same physical hardware. This scenario promotes attackers to exploit this configuration in the form of *co-location*, *co-residence*, or *co-tenancy attacks*, wherein an attacker is able to disguise as a regular and legitimate customer to infiltrate neighbor VMs belonging to other real legitimate customers. Several aftermaths are possible, including compromising integrity, confidentiality and privacy. Hacking trough *loopholes or injecting client code* into the SaaS model are two possible ways to achieve that purpose [95]. Another series of issues are implied by multi-tenancy, such as *data breach* [85, 105], *computation breach* [105], *data loss* and *data leakage* [12]. The *object reusability* issue is mentioned in [116]. It can be a result of *data remanence* in multi-tenant scenarios. To tackle these issues, data must be well segregated, meaning that SaaS systems have to assure clear boundaries between customers data.

4.3.2 Platforms and Frameworks

Given that clouds follow a SOA approach, the problem of data integrity gets magnified when compared to other distributed systems [95]. Moreover, web services normally rely on eXtensible Markup Language (XML), SOAP and REpresentational State Transfer (REST), and APIs. Most vendors deliver their APIs without transactions support, which further complicates the management of data integrity across multiple SaaS applications. Additionally, the PaaS model supplies platform and frameworks to develop cloud applications. During the applications development lifecycle, programmers should deploy rigorous security measures focusing on authentication, access control and encryption [12]. Nonetheless, *unsafe* APIs and IDEs (may allow hosting *botnets* and *trojan horses*) with *insecure systems calls or deficient memory isolation* [72] may comprise points of entrance to attackers [113].

4.3.3 User Frontend

Besides the particular issues derived from insecure platforms and frameworks, other problems arise from the user frontend to services. In other words, because clouds provide on-demand self-service capabilities, services subscribed by customers require a management interface with fine-grained configurations of those services [41]. Usually, those interfaces are accessible via the Internet, therefore being at peril because of web related security issues [102]. Moreover, there is a higher probability of exploiting those administrative interfaces in clouds than in other systems where management functionalities are only accessible to a few administrators.

4.3.4 Control

Control refers to regulating the use of a system composed of an infrastructure, data, applications and services [115]. While a customer may be concerned about *malicious usage* and *malicious computation*, a provider may be worried about monitoring and logging events within the cloud systems, because standards and control mechanisms are scarce [41]. Log files record all tenant events. Thus, *insufficient logging and monitoring capabilities* may hamper or prevent pruning for a single tenant.

Software spans across almost all elements of a system. This subsection discussed specific security issues of this topic. Nonetheless, the following subsections present a more detailed description of issues that may recall software-related components.

4.4 Data Storage and Computational Security Issues

Data storage security also comprises an important aspect of Quality of Service (QoS) [108]. Clouds, however, complicated QoS requirements and raised new issues. As customers do not have their data locally stored, techniques and mechanisms to efficiently and reliably check the data are required. Auditing approaches are adequate for such task, but it would not be fair to let the provider or the customer execute the auditing, because neither of them can guarantee to provide unbiased and honest results [107]. In addition, customers may not have the time, willingness, resources, or feasibility to monitor their data. In such case, they may delegate such responsibility to an optional trusted third-party auditor. Storage outsourcing hardens the task of efficiently and securely verify that a server, or a group of servers, is faithfully storing outsourced data [4]. Following is a discussion of security issues related with *abstraction*, *integrity*, *confidentiality and privacy*, *availability*, *sanitization*, and *cryptography*.

4.4.1 Abstraction

Clouds raised the *loss of control* issue [111], in which the customer is physically separated from the servers storing or computing the data, having no possible control over them whatsoever. In addition to being physically away, the data is somewhere within the server pool, at an unknown location, disabling the possibility of pinpointing the storage partition, network port, and switches involved in the handling of the data [92]. This issue is due to virtualization abstracting the VM location. Additionally, it is hard to isolate particular resources that have been compromised. *Multi-location* [115] is a term used to refer data being held in multiple locations. In the case of a service provider, as a means to provide high availability, data is backed up to other clouds of the same provider, usually in other data centers. However, big players, like Google and Amazon, have data centers all over the world, rising compliance and legal issues as data travels across borders, which are further discussed in Sect. 4.8. Nonetheless, a trustworthy SaaS model must be capable of offering *data locality* reliability.

4.4.2 Integrity

Integrity refers not only to data integrity but also to computational integrity. Data integrity points out that data should be honestly and correctly stored, detecting corruptness, modification or unauthorized deletion. Computational integrity stands for authentic computation of programs and reliable results output without being distorted by *malicious agents*, and *downtimes* and *slowdowns*, respectively. Attacks threatening these properties are usually known by *data loss*, *data manipulation* and *dishonest computation* [111]. *Administrative errors* in data backups, restoration, migration, or other operational tasks may lead to data loss, while *malfunctioning* Central Processing Units (CPUs), *transmissions buses*, *vulnerable code*, *misconfigured policies*, or rootkit attacks may lead to *dishonest computation*. For example, MapReduce, a computing framework for processing large datasets in distributed systems, may be dishonestly executed by misconfigured or malicious machines, resulting in inaccurate computational results. Additionally, finding out which machines are compromised is a difficult task. On the other hand, Atomicity, Consistency, Isolation and Durability (ACID) properties are nowadays assured and preserved in standalone database systems; but distributed systems, such as clouds, created a challenge in transactions between data sources, which must be handled in a fail-safe manner [95].

4.4.3 Confidentiality and Privacy

Confidentiality is fundamentally related with privacy, both emphasizing that confidential or private resources are not to be accessed nor seen by unauthorized parties. Confidentiality refers to data confidentiality and computational confidentiality. In the cloud context, however, questions related with these properties arise when an

individual, a businessman, or a government agency shares information in the cloud [95]. Nonetheless, the risks vary significantly with the terms of service and privacy policies established in SLAs. Laws may oblige cloud providers to look for criminal activity evidence or other government security matters in data contents. As previously said, assessing if the confidentiality agreement is being fulfilled is hard for both the customer and third-party hired auditors because the cloud provider may not be willing to allow examining metadata files. *Malicious insiders*, governed by personal motivations such as low salaries, and by exploring defective personnel management or insufficient security clearances in the data center, may access and *disclose data* private to customers. A single incident can expose a huge amount of information. Pooling and elasticity of cloud systems determine that resources allocated to one user will be reallocated to a different user a later time. Thus, it might be possible for a user to read data written by previous users in terms of memory and storage, an issue named *data recovery* [41]. A similar problem occurs due to VM mobility, further discussed in the next subsection.

4.4.4 Availability

Cloud services need to be guaranteed that they are up and running around the clock and accessible on-demand. IaaS physical and virtual resources, like databases and processing servers, need to be available to support data fetch operations and computational tasks of programs. To this end, a multi-tier architecture is deployed in cloud systems [95], supported by a load-balanced farm of application instances running on many servers. This approach enables resiliency against Denial of Service (DoS) attacks by building software and hardware failure measures in all tiers. *Weak authentication mechanisms* and *weak session management* are possible exploitable threats to provoke a DoS in data and computational availability. For instance, a supposedly legitimate user can have servers processing highly demanding tasks, occupying resources that might be denied to other users.

4.4.5 Sanitization

Data deletion has been a concern in distributed systems, to which monitoring, marking and tracking mechanisms have been employed for data discovery [71]. In clouds, data sanitization is of extreme importance, useful to properly dispose of sensitive data belonging to customers. In fact, data centers, like the ones belonging to Google, have destruction policies that physically wreck hard drives, even though media sanitization is hard or impossible due to resource pooling and elasticity [41]. Nonetheless, de *deficient destruction policies* may result in *data loss* [12] and *data disclosure* [16]. Examples include discarding disks without being wiped out [2] or the impossibility of destruction because disks might still be being used by other tenants [41].

4.4.6 Cryptography

The main issues concerning application of cryptographic techniques are the use of *insecure or obsolete cryptography mechanisms* and *poor key management* [41]. One particular issue stems from the abstraction layer imposed by virtualization between VMs and hardware, which can weaken Pseudo-Random Number Generators (PRNGs), resulting in the production of poor cryptographic material. The usage of not up-to-date and faulty cryptographic algorithms might expose pertinent and encrypted data [113]. Furthermore, given that nowadays most computers have multi-core CPUs with high clock rates, *brute force* attacks are easier to perform. Hence, programmers should pay particular attention to the cryptographic mechanisms embedded on their applications.

4.5 Virtualization Security Issues

Virtualization technology is placed in the SaaS model of the cloud stack. It is one of the main innovative sides of clouds. While constituting a defense and fault-tolerant mechanism, virtualization also poses many security issues, as not all virtualized environments are *bug-free* [2]. A multi-tenant approach seems promising to the cloud providers perspective, but increases the co-location attack surface as VM-to-VM attacks become more probable [9]. Regardless of the fact that virtualization security has been the subject of research even before the emergence of clouds, achieving logical and virtual isolation has not yet been completely met. The following discussion addresses security issues related with *managing images*, *monitoring virtual machines*, *networking*, *integrity*, *confidentiality and privacy*, and *availability*.

4.5.1 Managing Images

VMMs allow VMs to be easily turned on, off, or suspended by saving its current state in images. At the next boot, the state is loaded and applications can run or rerun as normally. VMs images contain information of files, processes, and memory blocks of the guest OS, therefore being potentially large-sized. This may pose performance challenges to cryptographic techniques [104]. Images are usually kept offline at an image repository. Even in offline state, they are vulnerable to *theft* and *code injection* [72]. One possible workaround is to concatenate various images, given that is harder to copy larger files than smaller ones. The administrator of an image repository risks *hosting and distributing malicious images*. Security properties of dormant images are not constant and degrade over time because an unknown threat may appear after the time of publishing images [110]. Moreover, images should converge to a steady state by performing scans for worms and other viruses, otherwise *infected* VMs can sporadically disseminate malware, an issue named *transience* [36]. This also applies to software licenses, security patches and updates, wherein administrators

tend to overlook long-lived inactive images because of high *maintenance costs*. Other issue is known as VM *sprawl* [65], referring to the possibility of having the number of VMs continuously growing while most of them are idle or never back from sleep, in turn wasting resources and complicating VMs management. A cloud provider risks leaking data due to unwittingly making files public. A cloud user risks running *vulnerable*, *malicious*, *out-of-date or unlicensed images* stored at an insecure, wrongly administrated repository [110]. The danger of compromising images lies in bypassing firewalls or IDSes by running an apparently legitimate VM, and place it in the cloud. VMs encapsulate software dependencies, allowing easy propagation of *trojan horses*.

4.5.2 Monitoring Virtual Machines

VMMs do not offer perfect isolation, inspection and interposition [95]. For example, Virtual PC and Virtual Server from Microsoft may allow *running code* on the host system or on another VM, or *elevating privileges*. Because of an input validation error, *Xen* allowed the *execution of commands* in Domain0 by a root user of a guest OS. Such problems are due to VMM vulnerabilities. VM *escape* refers to the case of gaining access to the VMM through a VM [50], therein being capable of attacking other VMs monitored by the same VMM. Well-known VM *escape* attacks include SubVirt [60], BLUEPILL [89] and Direct Kernel Structure Manipulation (DKSM) [7]. *Zero-day* vulnerabilities consist of vulnerabilities that are exploited before the developers know about them [70]. In the virtualization context, one could be capable of gaining access to VMMs or VMs. HyperVM was once exploited without the knowledge of the provider, resulting in the destruction of many web sites [40]. Furthermore, monitoring all VMs in a data center may massively increase the *computational overhead* due to the wide range of OSes that can be deployed in seconds, an issue named VM diversity [36, 103]. The ease of cloning and distributing VMs throughout cloud servers can also *propagate errors* and make arise to other vulnerabilities. Thus, more work is needed to enhance behavioral and introspection VM techniques while having in mind operational cost.

4.5.3 Networking

IaaS provides the means to resource pooling, therefore enabling customers to share physical resources and, most likely, networking equipments. Vulnerabilities originated in communication protocols also affect clouds, such as in Domain Name Service (DNS) servers [41, 72]. In virtualized networks, *administrative access* and *tailoring* is limited, potentially leaving uncovered holes [41]. *Incorrect network virtualization* may allow user code to access sensitive portions of the underlying infrastructure, disclosing sensitive knowledge of the real network or resources from other users [2]. *Packet sniffing* and *spoofing* also applies here. Virtualization software, such as virtual switches, may contain vulnerabilities that enable *network-based*

VM attacks [72]. Another important aspect in virtualized networking is the traffic produced, which is twofold. It occurs not only in real, physical, standard Ethernet networks, but also within virtualized environments. It can be defying to control both kinds of traffic because tried-and-tested network-level security might not work in the virtualization layer [41]. For instance, Virtual Local Area Networks (VLANs) and firewalls prove *less effective* when moved to such environments [104]. Moreover, securing dynamic establishment of *virtualized communication channels* is aggravated when VMs dwell across various IaaS platforms [80]. VM *mobility* [36, 103] is an issue arising from the resource pooling feature. VMs are likely to be copied or moved to other servers via network links, enabling quick deployment, but also quick *spread of vulnerable configurations* [50] and *image theft*. VM *moving*, also called *live migration* [114], is susceptible to many attacks. *Man-in-the-middle* attacks [75], Time of Check to Time of Use (TOCTTOU) vulnerabilities and *replay* attacks [114] are examples of such attacks. Copying images is also known as VM *cloning* or *template image cloning* [31, 41]. An image can be manipulated to provide backdoor access in the future, when instanced. Also, a template image might retain the original owner data which, when copied, may leak sensitive information like secret keys and cryptographic salt values. Moreover, various copies of the same VM may exist, and an attacker may access one and read its contents unnoticed, while trying to break the administrator password. Computer forensics techniques can be applied to obtain complete history of the VM, including usernames, passwords, applications and services, Internet browsing history, and IP addresses.

4.5.4 Integrity, Confidentiality and Privacy

Previously described issues can have impact on integrity, confidentiality and privacy properties. Nonetheless, more specific issues that compromise those properties are described herein. VM *hopping* is a term referring to maliciously gaining access to another VM belonging to a different cloud user [50], which can happen due to VMM *isolation failure*, as discussed earlier. Also known as cross-VM attacks [111], they require that two VMs are running on the same physical host and the knowledge of the IP address of the victim. According to [85], such requirements are easily met, highlighting the crucial importance of addressing these issues. Moreover, a single VMM is most likely to place many VMs co-resident on the same machine. In a successful attack, it is possible to monitor resources, modify configurations and files. Amazon EC2 was successfully exploited in 2009 [85] and 2011 [13] through *cross*-VM *side-channel* and *covert-channel* attacks. *Side-channel* attacks passively observe data flowing on the server, while *covert-channels* monitor and send data [17]. Variations of these attacks are being researched, such as using CPU load as a *covert-channel* [76], and L2 *cache covert-channel* to leak small useful information, such as private keys. *Timing side-channels* are regarded as an insidious security challenge because they are hard to control, enable stealing data, only the cloud provider can detect them, and can undermine efficiency [5]. Virtualization technologies may use a memory deduplication technique that allows reducing physical memory usage.

Attacks to this technique have been described in the literature [96, 97], and have the purpose of detecting applications or files on a co-residing VM. Furthermore, a series of attacks conducted by a *malicious insider* have been demonstrated in [87] and used to get plaintext passwords in memory dumps of a VM, extract a private key out of a key pair using memory snapshots, execute arbitrary commands in a backup copy of a VM by exploiting Domain0, and compromise data by exploiting VM relocation. The aforementioned attacks exploit the very nature of multi-tenancy, making it possible to access data belonging to other tenants. Thus, integrity, confidentiality and privacy properties are compromised by such attacks. Availability is also compromised because the attacker can stop services or ruin boot configurations so that VMs need fixing. Virtualization issues are key issues in clouds.

4.5.5 Availability

To compromise availability in virtualized environments, it is possible to take one VM, or more, under the control of an attacker, occupy all available resources so that the VMM cannot handle more VMs [103]. In such case, support to other VMs would be denied. However, a threshold for resource allocation should be deployed to mitigate this issue.

4.6 Networking, Web and Hardware Resources Security Issues

Cloud infrastructures are not only composed by the hardware where the data is stored and processed, but also by the path connecting to the point it gets transmitted. In a typical cloud scenario, data is split into a vast number of packets that are transmitted from source to destination through umpteen number of third-party infrastructure devices and links [85, 113]. The Internet is the most prominent example to use here. It is already known to suffer from *man-in-the-middle*, IP *spoofing*, *port scanning*, *packet sniffing*, *botnets*, *phishing*, and *spam* attacks. Consequently, the cloud inherits such issues from the Internet, even though *botnets* in clouds are easier to shutdown than traditional ones [17]. So, even if large amounts of security measures are put in the service models, the data is still transmitted through common Internet technology. Additionally, technologies to access the cloud vary from service enabled fat clients to web browser-based thin clients [55], being the latest the most common nowadays [45]. In fact, SaaS applications are required to be accessed over the web, by which a browser is most suitable. Thus, clouds also inherit web security issues, such as the ones mentioned in *The Ten Most Critical Web Application Security Risks* [77], a document containing the top ten web security issues, which was elaborated by Open Web Application Security Project (OWASP), a non-profit organization dedicated to the widespread of good application security practices. For example, *injection* tops the list, while XSS stands second. Web services play an important role in clouds, therefore deserving a special attention in this subsection. Below, a discussion of security issues

related with *communication protocols and standards*, *integrity*, *confidentiality and privacy*, *availability*, and *accountability* is thus included.

4.6.1 Communication Protocols and Standards

By design, the HyperText Transport Protocol (HTTP) is stateless and does not guarantee delivery nor supports transactions. To address this, web applications usually implement session handling techniques, many times being vulnerable to *session riding or session hijacking* [41]. As mentioned before, Dynamic Host Configuration Protocol (DHCP), DNS, and IP are among known vulnerable protocols that might enable *network-based cross-tenant attacks* in IaaS. Distinct technologies are used to access cloud resources [70], such as HTTP and HTTP Secure (HTTPS) for SaaS applications; SOAP, REST and Remote Procedure Call (RPC) technologies for PaaS web services and APIs; and remote connections, VPNs and File Transfer Protocol (FTP) for IaaS storage and computational services. Thus, web security and known protocol-related security issues are also relevant to clouds.

4.6.2 Integrity

Database systems require transaction support in order to guarantee data integrity. As HTTP fails to do so, *transaction management* comprises an obstacle that should be handled at the software API to enhance transactions in SaaS applications. An attack named *metadata spoofing* consists in reengineering metadata descriptions of, for example, Web Service Definition Language (WSDL) documents by establishing a *man-in-the-middle* [51]. Using such attack, it is possible to specify operations different from the ones in the document, allowing to create user logins, for instance. Besides compromising integrity, it also compromises authentication, posing as a different threat. However, if sound techniques are used, the attack is easily detected. Nonetheless, one has to take into consideration that, in clouds, WSDL documents are more dynamically accessed than on other systems, drastically raising the potential spread of malicious files and, thereupon, the probability of a successful attack.

4.6.3 Confidentiality and Privacy

In the network and web context, compromising confidentiality and privacy may imply compromising authentication mechanisms firstly. Network penetration and packet analysis; session management weaknesses; and incorrect Secure Sockets Layer (SSL) configurations can lead to *active session hijacking* and *credentials access* [95]. Concerns regarding web services existed before the emergence of clouds. For example, *wrapping* attacks [55, 69, 82], also known as *rewriting* attacks, consist in rewriting SOAP messages by adding a wrapper and forged XML field to access the target web resource. A valid SOAP envelope signature of the original message is maintained,

to validate the execution of the modified request. In 2009, Amazon EC2 was found to be vulnerable to a variation of a *wrapping attack* [42], which allowed performing an arbitrary number of EC2 operations. Moreover, an attack named *SOAPAction spoofing*, which consists in modifying HTTP headers after intersecting them to also invoke other operations, was perpetuated in a .NET web service in 2009, as well as an XML *injection attack* [51]. Another attack, entitled WSDL *scanning* attack, has been addressed in various studies [30, 51]. It consists in discovering and fingerprinting web services to find omitted, confidential operations, supposedly available only to administrators. *Data leakage* is a possible aftermath of all these attacks. Note that the aforementioned attacks raise confidential and privacy concerns, as executing arbitrary operations may output sensitive information or allow the attackers to access unauthorized resources.

4.6.4 Availability

Data centers require bandwidth-wise networking links to support large amounts of network traffic. However, in 2007, Cisco stated [21] that large server cluster designs are usually under-provisioned in terms of network capacity with a factor of 2.5:1 up to 8:1, meaning that the network capacity of data centers is less than the aggregate capacity of the hosts inside the same subnet. This *bandwidth under-provisioning* [111] vulnerability worsens the impact of *flooding* attacks, raising availability and QoS concerns. DoS attacks by *flooding* are some of the most concerning in computer systems. For example, a botnet can be used to send millions of Transmission Control Protocol (TCP) SYN messages to the target server in a small period of time, creating a Distributed DoS (DDoS) which can overload the server processing all the requests. DoS attacks are often termed as direct or indirect attacks. A direct DoS attack implies pre-determining the target service, which potentially gives in to the overload. A possible side effect of direct approaches is that adjacent services running on the same hosting machine can also be denied, creating collateral damage—an indirect DoS attack. A condition known as *race in power* [52] is the worst case scenario of DoS attacks. As cloud systems may aid overloaded machines by relocating services to other machines, the workload can be propagated throughout the system. At some point, the system aiding may also host the *flooding*, placing both cloud systems off against each other, both aiding one another with resources until the point where one, finally, gives in and reaches a full loss of availability state. A new form of particular cloud DoS has been discovered in 2010 [63]. The objective is to starve an exploitable bottleneck uplink found in the topology. To perform such attack, it is required to gain access to enough hosts within the target subnet and to produce, preferably, User Datagram Protocol (UDP) traffic upwardly through the uplink, in order to consume its bandwidth, having the side effect of starving other TCP connections, who back off during congestion. *Resource exhaustion* [51], a particular case of DoS, is characterized by a large attack surface. The *oversize payload* attack on web services consists in increasing memory usage when Document Object Model (DOM) parsing is employed to transform XML documents into memory objects. A

raise of memory consumption with a factor of 2:30 has been observed for common web service frameworks, such as the Axis web service, which resulted in an out-of-memory exception. Another attack named coercive parsing exploits namespace vulnerabilities in XML parsing with the purpose of overusing the CPU. Axis2 web service was exploited, causing CPU usage of 100 %. Moreover, the *obfuscation* attack aims at overloading the CPU and increasing memory usage. With the same objectives, the *oversized cryptography* attack exploits buffer vulnerabilities and encrypted key chains in web services. Other related issues include WS-Addressing spoofing attack [53], in the Business Process Execution Language (BPEL) [51] and flooding by using XML messages [18].

4.6.5 Accountability

Clouds follow a pay-as-you-go business model. In terms of networking, bandwidth rented by customers is also billed according to their needs and usage. *Flooding* also impacts accountability, raising costs for cloud customers. SLAs must, therefore, cover determination of liability in case of abnormal large bills, meaning that the responsible party must be determined [111]. Fraudulent Resource Consumption (FRC) [48, 49], a more subtle and evasive attack than DoS, has the goal of exploring the cloud pricing model to cause *financial loss* to the victim. It consists in sending requests to consume bandwidth continuously and for a long period of time, but not intensively enough to cause DoS. It is hard to analyze and classify traffic belonging to a Fraudulent Resource Consumption (FRC) attack, which is representative of an Economic Denial of Sustainability (EDoS). Also, in order to achieve maximum profitability, cloud providers choose to multiplex applications of different customers in the resources pool, in order to achieve high utilization. However, this may cause incorrect resource consumption metering, resulting in additional costs for the customers and leading to *inaccurate billing* [111].

4.7 Access Security Issues

Access to cloud resources concerns the security policies deployed by an organization to its employees, according to their role in the company. For instance, personnel with lower security clearance should not have access to certain datasets of higher security clearance. Thus, SaaS applications should be capable of being customized and configurable to incorporate specific access security policies. To this end, authorization and authentication mechanisms are put in place, which commonly resort to a combination of username and password, called credentials, which are private to each user. A discussion of security issues related with *data centralization*, *credentials*, *authentication*, *authorization*, *identity management*, and *anonymization* is included subsequently.

4.7.1 Data Centralization

Data centers condense in a single centralized point massive amounts of data and resources. They pose as appealing attack points, which may be even a more severe issue if *malicious insiders* and *malicious outsiders* infiltrate the facility and the cloud. The vulnerability might lie on the deployed security procedures for physical and logical access controls. Unpleasant or former employees, customers, hobbyist hackers, espionage agents, or other cybernetic intruders portray a possible malicious community, ready to exploit the right opportunity. Outside threats pose greater impact on clouds, not only in terms of system damage, but also to the provider reputation and business, due to the long term loss of leaving customers [9]. Nevertheless, monitoring of privileged administrators should be carried out, because they can turn into malicious sysadmins—administrators with *malicious intents* [57]. Henceforth, deploying firewalls, Access Control Lists (ACLs) and IDSes or IPSes is mandatory.

4.7.2 Credentials

Usually, LDAP or Active Directory (AD) servers are used to manage credentials in larger systems. In the cloud computing paradigm, those servers can be placed inside the company network, behind a firewall, or outsourced to the cloud provider system. The option mentioned in last increases IT *management overhead* if multiple SaaS services are rented by the customer, because one has to add, modify, disable, or remove accounts, as personnel leaves or enters the company. Furthermore, the loss of control issue applies here also, as the customer is deprived of configurations and security of LDAP or AD servers [92]. In the past, weak password-recovery mechanisms resulted in *weak credential-reset* vulnerabilities when access responsibilities are outsourced [41]. Credentials have long been an issue of remote access mechanisms. If they are stolen by means of *phishing*, *fraud*, *keyloggers*, *buffer overflows*, or other software security holes, *service hijacking* becomes the most probable menace [9]. In such case, monitoring or manipulating data and transactions is possible, along with performing *malicious redirects* or launching DoS attacks by using the compromised account as an attacking concealed base. *Replay sessions* are most likely to happen. Moreover, it is possible to perform User to Root (U2R), in which the attacker gains root level access to VMs or hosts after gaining access to a valid user account [70]. Either way, *service disruptions* can cause a business halt or lose valuable customers, ultimately leading to *financial loss*.

4.7.3 Authentication

A centralized service system approach is advantageous in SaaS authentication because of centered monitoring, making software piracy more difficult [19]. Remote authentication mechanisms rely mostly on regular accounts, nevertheless being susceptible to a plethora of attacks [39]. *Dictionary* and *brute-force* attacks are amongst

the most prominent examples. Various approaches for authentication exist, such as simple text passwords, third-party authentication, graphical passwords, biometric scans, and 3D password objects [28]. Simple text passwords are usually static, long-living approaches. Nevertheless, *archaic static password*—one-tier login—is simply not good enough, constituting actually one of the biggest security risks [44]. For small cloud deployments, third-party authentication is not usually preferred. While graphical password schemes require a long time, biometric technologies, like fingerprinting, palm printing, and iris or retina recognition, may violate the user personal space. Moreover, they require physical presence, thereupon being not applicable in remote systems, but suitable for physical data center security. Finally, 3D passwords do not support multi-level authentication. Still on authentication topic, it is important to mention that customers are most likely to subscribe multiple services to a provider, resulting in several login requirements. Besides Hart [44] claiming one-tier login not being enough and while Tripathi [102] also acknowledges the difficulty in deploy strong user-level authentication, multi-level authentication mechanisms for several services is a hard task to achieve, because their management and reliability are hard to deploy. SSO is perhaps the most used technique. Google, for instance, was once vulnerable in their SSO implementation that allowed users to switch between services, like Gmail and Calendar, without re-authenticating [66]. The Security Assertion Markup Language (SAML) would be used to carry *impersonation* attacks and access a target Google account. Many authentication mechanisms have a threshold for authentication attempts to fight *brute-force* attacks. However, an availability issue arises in the form of DoS via *account lockout*, meaning that an attacker can repeatedly, and in quick succession, try to authenticate with a valid username until the threshold is surpassed [41].

4.7.4 Authorization

Due to the growth of cloud storage systems, services performing mashups of data are likely to be common in the future [19]. It was previously said that centralized access control would be advantageous but, in this scenario, it may not be, however, possible or desirable. The development of data mashups have security implications in terms of *data leakage* and on the number of resources a user retrieves data from. The latter places access authorization requirements for reasons of usability. For instance, Facebook does not typically verify third-party appliances, which use data uploaded to its servers. *Malicious applications* can, therefore, perform malicious activities. Other social sites are also endangered [109]. *Insufficient or faulty authorization checks* are possible attack vectors, like an *insecure direct object reference*, also called Uniform Resource Locator (URL)-*guessing* attacks [41], an issue with rank four in the top ten web application security issues of OWASP. Service management interfaces are also prone to offering *coarse authorization control models*, making impossible to implement duty separation capabilities.

4.7.5 Identity Management

Identity Management (idM) is a broad administrative area that deals with identifying entities and cloud objects, controlling access to resources according to pre-established policies [72]. Three idM perspectives are often considered [95]. The first perspective, pure identity, manages identities with no regards to access or entitlements. The second perspective, log-on, uses traditional approaches by using physical tokens, such as smartcards. The third perspective, service paradigms, delivers online, on-demand, presence-based services with respect to roles, appropriate to cloud services. Three idM models were also identified in [95]. The first, independent idM stack, is maintained at the provider end, keeping usernames, passwords, and all related information per SaaS application. This model should be highly configurable to comply with the customer security policies. The second, synchronized credentials, consist in replicating account information stored at the customer end in the provider, giving access control abilities to the provider. It is in this model that an issue known as *account information leakage* is mentioned. The third, federated idM, provides the means for linking account information storage across multiple idM sources, being SSO one good example of such mechanisms. Authentication occurs at the customer side, while users identity and other attributes are propagated on-demand through federation to the provider. *Trust* and *validation* issues appear in this model. Apart from that, large PaaS and SaaS platforms have complex hierarchies and fine-grained access policies, therefore raising logistic and transport issues in synchronizing data [92]. Moreover, using different identity tokens and identity negotiation protocols in general idM might present interoperability drawbacks also [98].

4.7.6 Anonymization

Some systems implement anonymous access to enhance security, aiming to prevent disclosure of the identity information of users. Notwithstanding, full anonymization brings the *hidden identity of adversaries* issue [111]. *Malicious users* can jeopardize security if they acquire access to an anonymized account, hiding exploitation tracks and becoming undetectable.

4.8 Trust Security Issues

Outsourcing services brings several trust issues. Firstly, cloud customers must heavily trust providers with their data, losing control over it. Secondly, providers must trust and provide access for customers to access cloud resources. Trust is not only related with the relationship between cloud stakeholders, but also with the assets in the cloud, relying on remote data storage mechanisms, computational algorithms, hardware, virtualization techniques, and web-based access [56]. Nonetheless, sometimes trust cannot be established or, even if it can, it may not be enough to make the

customer comfortable. Hence, additional means are expected to be developed in order to increase security confidence in the cloud business. In fact, trust is also important in other distributed systems, such as Peer-to-Peer (P2P) and sensor networks [34]. This section contains a discussion on security issues related with *reputation*, *compliance and legal issues*, *auditability*, *computer forensics*, *confidentiality and privacy*, and *anonymization*.

4.8.1 Reputation

The cloud operation mandates sharing assets among several users. Hence, activities and behaviors of cloud stakeholders affect each others reputation, an issue known as *reputation isolation* [33, 71] or *fate-sharing* [17, 86]. For example, a user may subvert a system, in turn disrupting services to other users. Moreover, all of them benefit from the security expertise concentration that cloud computing offers, depending on the signed SLAs, consequently sharing the same infrastructure and fate. In 2009, Amazon EC2 was subverted by spammers who caused blacklisting of many internal IP addresses, which resulted in major service disruptions [17]. A second noteworthy incident occurred in the same year, in which federal agents seized data centers suspicious of facilitating cyber-crime. Many cloud customers, namely companies, without knowledge of the suspicions, had business disruptions, halts, or even complete closures. Therefore, hardware confiscation, a result from applying law-enforcement, is an issue named *e-discovery*, by which data *disclosure* and *data loss* are major risks [39].

4.8.2 Compliance and Legal Issues

The most clear legal issue stems from the abstraction and multi-location properties of clouds. Several cloud providers have data centers spread all over the world for providing geographic redundancy. However, many countries do not allow data to leave country boundaries. If such happens, to which country jurisdiction does the data falls under when an incident takes place? Or who has jurisdiction over data as it flows across borders? Moreover, can government agencies access the information as it changes jurisdiction? Also, can a provider deliver trustable reports of the customers data health? If served a subpoena or other legal action under a limited time-frame, how can a customer compel the provider, if even possible, to gather potential required evidences within the time-frame? According to Refs. [19, 58, 71], such questions have fuzzy, unclear answers. Additionally, *dishonest computation*, *accidental resource allocation*, *availability issues*, and *data loss* constitute possible violations to SLAs. In any case, compliance issues are at cause. Thus, the risk of investing in certification, such as industry standards or regulatory requirements, is high to customers due to failure of providing compliance evidence by providers [33]. Anyhow, public clouds imply that certain kinds of compliance cannot be achieved, like the security requirement Payment Card Industry (PCI) Data Security Standard

(DSS) [79]. Other perspective on the compliance and legal topic is related with the possibility of different alignment interests between cloud stakeholders [19]. *Limited usability*, *implied*, and *obliged contractual* or *unclear terms* can pose issues in the customers service usage context. After the SLA is closed, the customer remains at the mercy of the provider. Consequently, customers may, or may not, trust particular providers with basis on the SLAs they offer. SLAs are normally not consistent amongst different providers, leading to a higher uncertainty in identifying the most trustworthy providers [43]. In some cases, providers might use subcontractors, to which costumers have even less control, influence, compliance certainty, and trust [19], raising a problem known as the *transitive nature* issue. In such case, who is to blame when an incident takes place? The provider or the subcontractor? Problems like this have happened in the past, resulting in *data loss*. More on the law side, issues arise when providers must obey government regulations for disclosing data of lawful interception, which may break the trust chain created with customers and originate conflicting points. For example, the USA PATRIOT Act (UPA) conflicts with the Personal Information Protection and Electronic Documents Act (PIPEDA) and Data Protection Directive in Canada and Europe, respectively. Law acts have nonetheless been published to protect individual privacy and business secrets; but some might not be in accordance with the newly cloud requirements. The Electronic Communications Privacy Act (ECPA) of 1986 and UPA of 2001 are examples of acts that fail to protect data being disclosed to government entities. The Fair Credit Reporting Act (FCRA) of 1970, the Cable Communications Act (CCA) of 1984, the Video Privacy Protection Act (VPPA) of 1988, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, and the Gramm-Leach-Bliley Act (GLBA) of 1999 are other examples of acts that fail to protect data being disclosed to private entities. Thus, such out-of-date acts are inapplicable to cloud scenarios, as of 2010 [115].

4.8.3 Auditability

The answer to the question of the *provability of data deletion* is very relevant to a company retention policy [19]. Moreover, how can a customer be assured that data was really deleted or that security mechanisms are really being applied? Is trusting the provided reports, if any, enough? Auditability enables assessing the security requirements by putting an additional layer above virtualized guest OSes [2]. To this end, methodologies are necessary to analyze service conditions, monitor intrusions, accesses, record logs with detailed descriptions of what happens, and other events [39]. Nevertheless, cloud providers may not be willing to allow conducting audit operations [33]. Mutual auditability may provide a collaborative approach to be sure of each others *trustworthiness*, improving incident response and recovery. Customers can delegate auditing to third-party entities, leaving those responsibilities in the hands of specialized personnel. Auditability hastens blame attribution in case of search or seizure incidents, which can be vital to the cloud stakeholders, so that law enforcement agencies do not overreach when carrying out their duties during

data collecting procedures in data centers [17]. In fact, data might be forced to be kept within jurisdictional bounds so as to be valid in court if necessary. Nonetheless, businesses may not often like the fact that agencies might try to get their data via the *court system*, overlooking some laws and potentially peeking into the company secrets [115]. In any case, auditability methods are hampered by the *abstraction* issue (data is not physically on a single or fixed set of servers), and some of those methods are not privacy-preserving capable, pointing out research interests in this area [112].

4.8.4 Computer Forensics

Computer forensics is a particular form of auditing that has emerged in recent years to fight against cyber-crime. The main goal is to determine digital evidence by means of analysis techniques [99]. But clouds push and spread data further back into the network and servers, rather than purely being on a physical computing device. Therefore, investigative services and mechanisms also face the *abstraction* issue. According to [44], it is possible to comply with forensics with adequate access to the data, but more difficult in clouds. Private clouds are surely easier to analyze than public ones, because servers, applications, databases and other resources are more easily enumerated [99]. From the user perspective, forensics raise concerns in terms of *data seizing* and *data disclosure*, compromising confidentiality and privacy, while for the party conducting the forensics activities, the cloud stack exhibits several challenges. Key evidence may reside in web browsers history and caches, and other artifacts [20], which are remote to the cloud and hard to get, posing difficulties in *collection*, *collation* and *verification* tasks. Finding out what a user did from the beginning to the end of a service disruption is hard [99]. Virtualized platforms may also give rise to *unsound forensic data* and encryption schemes employed by customers and providers, privacy protecting acts, and time-consuming procedures to gain legal authority, also make of cloud forensics a difficult task to achieve. Moreover, the *lack of validation for disk images* in a scenario demoted of cryptography techniques may pose as a potential problem. *Evidence acquisition* is, therefore, a forefront security issue in cloud forensics [32, 99]. Computer forensics requires solid trust layers, not only at the provider and customer sides, but also in the court. A jury or a judge of a legal action ultimately has to decide whether or not the evidence presented is believable, reliable and trustworthy enough.

4.8.5 Confidentiality and Privacy

From the customer standpoint, *malicious sysadmins* constitute one of the major threats in clouds because of their privileged access, raising trust barriers [91]. A sysadmin is able to install all sorts of software and access VMs. For example, XenAccess allows running a user level process in Domain0 that directly accesses VMs memory contents at runtime. Other more sophisticated security attacks, such as cold boot attacks and *hardware tampering*, can be carried out for the same outcome. A

malicious sysadmin can further remove security-specific kernel modules, like firewalls and anti-viruses, making cloud systems vulnerable [117].

4.8.6 Anonymization

Anonymization can cut semantic links of the data to their owners, to overcome trust issues, while preserving the provider capability of charging resource usage in a proper and reliable manner [54]. Enterprises have actually felt increased pressure to anonymize their data until proper, trustable privacy mechanisms are in place [19]. For example, in the search marketplace, Google modifies the last IP address byte of logged searches after 9 months, and deletes it after 18 months. It also anonymizes cookie information, a process called generalization, which can guarantee reasonable privacy protection [100]. Anonymized data is retained for internal purposes. Even though anonymization is a difficult task, efforts have been carried out to address it in clouds [10, 54]. Nonetheless, *de-anonymization* attacks have been designed too. A family of attacks targeting social networks includes the active, the passive, and the semi-passive attacks, which *breach edge privacy* of a group of individuals [6]. Another study proposed an algorithm with 12 % *de-anonymization* error rate on an online photo-sharing website by only using network topology information [73]. *De-anonymization* attacks on dynamic social networks have also been studied, which used correlation techniques [29] to derive information about users. A curious *de-anonymization* attack targeting health records resulted in identifying the governor, at the time, of the Massachusetts state in the USA. It was proved that *innocuous and neutral data injection*, such as gender and birth-date, on anonymized data can lead to *information leakage* [92].

4.9 Other Security Issues

This subsection discusses security issues that either are not classified according to the taxonomy defined in Sect. 3.6 or that may fall in various categories. A discussion of security issues related with *virtualization and web*, *governance*, and *unknown threats* is included below.

4.9.1 Virtualization and Web

This specific topic includes only the *cloud malware injection* attack [55]. It consists in injecting malicious services or VMs into the cloud, serving any particular purpose of the attacker. The attack is initiated by injecting a service into the SaaS or PaaS models; or a VM into the IaaS model. Secondly, the cloud system must be tricked to treat the service or VM validly. Ultimately, authentic user requests are redirected

to the malicious instance and the code written by the attacker is executed, which can compromise the overall security of the system.

4.9.2 Governance

Governance issues consist in losing administrative, operational and security controls. In cloud environments, the *lock-in* issue might end up in a governance problem. As discussed earlier in Sect. 3.4, interoperability between clouds still faces security and standardization issues, namely when it comes to protocols, data formats and APIs. As a result, customers might become hostages of the provider of their choosing with regard to their data, becoming vulnerable to a few issues, namely the impossibility of data migration, price increases, reliability and security problems, service termination, or even providers going out of business [2, 39]. Standardized APIs would allow customers to deploy SaaS applications and have copies of the same data across multiple providers, mitigating the problem of a cloud provider having all copies in case of going out of business. Having perfect interoperability could lead to a *race-to-the-bottom* condition in terms of cloud pricing, resulting in flattening the profit for providers [2]. Nonetheless, it is normally argued that, on the one hand, customers may not adopt low-cost services because QoS and security properties do matter for them and, on the other, new possibilities to integrate hybrid clouds both on-premises and on-premises would arise. Moreover, besides the *data locality* issue, customers also face losing control over redundancy, file systems, other configurations related with storage and computation and, more importantly, security, namely at the physical level in the IaaS model [19].

4.9.3 Unknown Threats

The CSA finds *unknown risk profile* as one of the top threats to cloud computing [25], resembling *zero-day* vulnerabilities, earlier discussed in Sect. 4.5. Many companies might overlook security issues if the outcome benefits outweigh the risks taken. In this scenario, unknown risks arise when security matters are posted in background or in hold, or are low prioritized. Furthermore, the CSA finds information about who is sharing a cloud infrastructure to be pertinent to assess security risks, in addition to network intrusion logs, redirection attempts, and other types of logs. This is a prime example of why security within cloud environments must be upheld as high priority, for there is always the possibility of an unknown threat and risk [113].

5 Summary of Cloud Security Issues

The review of the literature presented in the previous sections shows that security concerns are focused on the new characteristics of cloud environments. Although

their unique and innovative nature brings new challenges to the IT industry and academia, some already prevalent issues in IT also affect clouds. Because clouds are accessed via the Internet, all the known issues from the latter are inherited by clouds. Some may be amplified if the cloud business model and pricing model are explored. Furthermore, virtualization, which is not a technology that emerged with clouds but an independent component that preceded clouds, got boosted up with the fuzz around cloud computing, being now one of the main cloud characteristics and of extreme importance. However, it enlarges the VM-to-VM attack surface because of VMM vulnerabilities, commonly known as *cross*-VM attacks. Several studies focus on this topic alone, some showing the malicious exploitability of popular cloud solutions and, henceforth, raising alarms for this topic. The fact of sharing a network medium and physical devices might be a major decision factor for cloud customers not adopting cloud solutions. As a consequence, the provider-customer trust bridge might get smaller if auditability is not possible to conduct. Further, the possibility of computer forensics seizing a data center to carry out their duties and the existence of out-of-date acts also contribute to the discussion of cloud security. Outsourcing IT duties to third-party cloud providers is, therefore, an issue yet to overcome.

Figure 3 contains a timeline summarizing most of the studies described in this chapter by indicating in what years they were published and the underlying issue category. In addition, the studies provided by organizations that are considered pioneering in the field are also included. By observing the figure, it is perceivable that both the industry and academia started to study the cloud computing environments and its security state soon enough. Its analysis also shows that the research in 2011 was proliferating, with many studies on the virtualization, networking, web, and hardware resources, access and trust categories. The trust studies, however, are mostly related with de-anonymization, pointing out research directions for applying anonymization in clouds. A deeper analysis uncovers an increase in the scope of issues discussed throughout the studies. In other words, in the initial years, studies focused on single issues. From then on, academia started working on understanding the wider security scope of clouds by studying more issues on single studies. For instance, the study in [19] from 2009 is included in three categories, while [41]

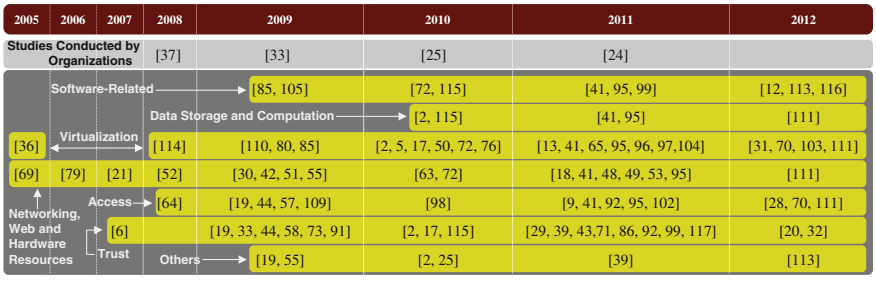

Fig. 3 Timeline exhibiting the date of publication the several studies on the cloud security subject, structured according to the categories used along the chapter

is included in five categories in 2011. Although this conclusion stands true for the sample of studies presented in the chapter, it is believed that other studies might also study the wide security scope of cloud systems.

6 Conclusions

In the last few years, the emergence of cloud and cloud computing related technologies changed the distributed systems paradigms, mainly due to the proliferation of virtualization. Clouds integrate virtualization techniques with modern IT, to allow building an elastic pool of resources that can be seamlessly delivered on-demand to costumers. These resources are normally managed remotely through self-serviced administration interfaces and billed using a pay-per-use model. These appealing features attract attentions from all over the industry and academia. A potentially very dangerous community is also drawn in, which is intrigued by the innovative operation of clouds and the data they hold for storage or processing purposes, posing as a threat to the overall business model. Enterprises changed how their IT investment is done, allowing cloud providers to boost underlying markets by creating a panoply of cloud solutions. As a consequence, data centers have been increasingly becoming more popular, spreading out the buzzword of *cloud computing* to the edges of the IT world. In order to make a completely secure investment out of clouds, it is of utmost importance and absolutely required to address the identified security issues, so as to allow a greater number of cloud native applications and products to be developed. Nonetheless, cloud technology and some of its security issues are relatively new, making some of the already existing solutions directly inapplicable.

Throughout this chapter, an extensive survey on cloud security issues was presented, discussing issues of several domains in the cloud. The literature on the subject was analyzed in the chapter, in which a review of each study was conducted to determine their goal and select the contents required to cover all topics. In addition, basic concepts of the cloud security were also included in the chapter in order to provide the fundamentals to understand the chapter. The studies analyzed emphasize the severity of the security issues related with virtualization techniques. The VM-to-VM attack surface was dramatically increased with the emergence of clouds, embracing now a large number of prominent security issues of cloud environments.

The analysis of the literature reflects a clear interest of researchers to address the cloud and cloud computing security issues. Many studies point out how critical it is to put effort in devising new security measures in order allow the development and adoption of cloud related technologies. In the meanwhile, cloud users might not be able to take full advantage of cloud applications in a fail-safe computing environment. History has proved that security should be a forefront priority and that the awareness on this area is partially motivated by issues and events faced along the way, which seems to apply in this case also.

References

1. Amazon. Amazon Web Services: Overview of Security Processes. http://s3.amazonaws.com/aws_blog/AWS_Security_Whitepaper_2008_09.pdf. White Paper. 2012
2. Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M (2010) A view of cloud computing. Commun ACM 53(2010):50–58
3. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson DA, Rabkin A, Zaharia M (2009) Above the clouds: a berkeley view of cloud computing. In: Technical report #UCB/EECS-2009-28. Electrical Engineering and Computer Sciences University of California.
4. Ateniese G, Di Pietro R, Mancini LV, Tsudik G (2008) Scalable and efficient provable data possession. In: Proceedings of the 4th international conference on security and privacy in communication networks (Istanbul, Turkey, 2008), 9:1–9:10.
5. Aviram A, Hu S, Ford B, Gummadi R (2010) Determinating timing channels in compute clouds. Proceedings of the ACM workshop on cloud computing security, Chicago, IL, USA, In, pp 103–108
6. Backstrom L, Dwork C, Kleinberg J (2007) Wherefore art thou R3579X?: anonymized social networks, hidden patterns, and structural steganography. In: Proceedings of the 16th international conference on world wide web, Banff, Alberta, Canada, pp 181–190.
7. Bahram S, Jiang X, Wang Z, Grace M, Li J, Srinivasan D, Rhee J, Xu D (2010) DKSM: subverting virtual machine introspection for fun and profit. In: 29th IEEE symposium on reliable distributed systems, New Delhi, India, pp 82–91.
8. Begum S, Khan MK (2011) Potential of cloud computing architecture. International conference on information and communication technologies, Karachi, Pakistan, In, pp 1–5
9. Behl A (2011) Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. World congress on information and communication technologies, Mumbai, India, In, pp 217–222
10. Bentounsi M, Benbernou S, Atallah MJ (2012) Privacy-preserving business process outsourcing. In: IEEE 19th international conference on web services, Honolulu, HI, USA, pp 662–663.
11. Bernstein D, Vij D (2010) Intercloud security considerations. In: IEEE 2nd international conference on cloud computing technology and science, Indianapolis, IN, USA, pp 537–544.
12. Boampong PA, Wahsheh LA (2012) Different facets of security in the cloud. In: Proceedings of the 15th communications and networking simulation symposium, Orlando, FL, USA, pp 5:1–5:7.
13. Bugiel S, Nürnberger S, Pöppelmann T, Sadeghi A-R, Schneider T (2011) AmazonIA: when elastiaddress snaps back. In: Proceedings of the 18th ACM conference on computer and communications security, Chicago, IL, USA, pp 389–400.
14. Carroll M, Kotzé P, Van der Merwe A (2011) Secure virtualization–benefits, risks and controls. CLOSER, Noordwijkerhout, Netherlands
15. Che J, Duan Y, Zhang T, Fan J (2011) Study on the security models and strategies of cloud computing. Procedia Eng 23(2011):586–593
16. Chen D, Zhao H (2012) Data security and privacy protection issues in cloud computing. International conference on computer science and electronics engineering, Hangzhou, China, In, pp 647–651
17. Chen Y, Paxson V, Katz RH (2010) What's new about cloud computing security? In: Technical report #UCB/EECS-2010-5. University of California, Berkeley, EECS Department
18. Chonka A, Xiang Y, Zhou W, Bonti A (2011) Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. J Netw Compu Appl 34(2011):1097–1107
19. 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 ACM workshop on cloud computing security. Chicago, IL, USA 2009:85–90
20. Chung H, Park J, Lee S, Kang C (2012) Digital forensic investigation of cloud storage services. Digital Investigation.

21. Cisco (2007) Cisco data center infrastructure 2.5 design guide. http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns944/white_paper_c11-680202.pdf White Paper
22. Cisco (2011) Data center power and cooling. http://www.cisco.com/univercd/cc/td/doc/solution/dcidg21.pdf White Paper
23. Corbató FJ, Vyssotsky VA (1965) Introduction and overview of the multics system. In: Proceedings of the fall joint computer conference (Las Vegas, NV, USA, 1965), pp 185–196.
24. CSA (2011) Security guidance for critical areas of focus in cloud computing v3.0. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf White Paper
25. CSA (2010) Top threats to cloud computing. https://cloudsecurityalliance.org/research/top-threats/. White paper
26. Dahbur K, Mohammad B, Tarakji AB (2011) A survey of risks, threats and vulnerabilities in cloud computing. In: Proceedings of the international conference on intelligent semantic web-services and applications, Amman, Jordan, pp 12:1–12:6.
27. Dhage SN, Meshram BB, Rawat R, Padawe S, Paingaokar M, Misra A (2011) Intrusion detection system in cloud computing environment. Proceedings of the international conference and workshop on emerging trends in technology, Mumbai, Maharashtra, India, In, pp 235–239
28. Dinesha HA, Agrawal VK (2012) Multi-level authentication technique for accessing cloud services. International conference on computing, communication and applications, Dindigul, Tamilnadu, India, In, pp 1–4
29. Ding X, Zhang L, Wan Z, Gu M (2011) De-anonymizing dynamic social networks. IEEE global telecommunications conference, Houston, USA, In, pp 1–6
30. Doroodchi M, Iranmehr A, Pouriyeh SA (2009) An investigation on integrating XML-based security into web services. In: 5th IEEE GCC conference exhibition, Kuwait City, Kuwait, pp 1–5.
31. Duncan AJ, Creese S, Goldsmith M (2012) Insider attacks in cloud computing. In: IEEE 11th international conference on trust, security and privacy in computing and communications, Liverpool, United Kingdom, pp 857–862.
32. Dykstra J, Sherman AT (2012) Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques. Digital Inv 9:S90–S98
33. ENISA (2009) Cloud computing: benefits, risks and recommendations for info-marion security. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment. White Paper
34. Firdhous M, Ghazali O, Hassan S (2011) A trust computing mechanism for cloud computing with multilevel thresholding. In: 6th IEEE international conference on industrial and information systems (Kandy, Sri Lanka, 2011), pp 457–461.
35. Foster I, Zhao Y, Raicu I, Lu S (2008) Cloud computing and grid computing 360-degree compared. Grid computing environments workshop, Austin, TX, USA, pp 1–10
36. Garfinkel T, Rosenblum M (2005) When virtual is harder than real: security challenges in virtual machine based computing environments. In: Proceedings of the 10th conference on hot topics in operating systems (Santa Fe, NM, USA, 2005), pp 20–20.
37. Gartner (2008) Assessing the security risks of cloud computing. http://cloud.ctrls.in/files/assessing-the-security-risks.pdf. White Paper
38. Gartner (2011) Summary report for gartner's top predictions for IT organizations and users, 2012 and beyond: control slips away. http://www.gartner.com/id=1861020. White Paper
39. Gonzalez N, Miers C, Redigolo F, Carvalho T, Simplicio M, Naslund M, Pourzandi M (2011) A quantitative analysis of current security concerns and solutions for cloud computing. In: IEEE 3rd international conference on cloud computing technology and science, Athens, Greece, pp 231–238.
40. Goodin D (2009) Webhost hack wipes out data for 100,000 sites. The Register.
41. Grobauer B, Walloschek T, Stocker E (2011) Understanding cloud computing vulnerabilities. IEEE Secur Privacy 9(2011):50–57
42. Gruschka N, Iacono LL (2009) Vulnerable cloud: SOAP message security validation revisited. IEEE Int Conf Web Services, Los Angeles, USA, pp 625–631

43. Habib SM, Ries S, Muhlhauser M (2011) Towards a trust management system for cloud computing. In: IEEE 10th international conference on trust. Security Privacy Comput Commun 2011:933–939
44. Hart J (2009) Remote working: managing the balancing act between network access and data security. Comput Fraud Security 2009:14–17
45. Hayes B (2008) Cloud computing. Commun ACM 51(2008):9–11
46. IDC (2009) New IDC IT cloud services survey: top benefits and challenges. http://blogs.idc.com/ie/?p=730. White Paper
47. IDC (2008) New IDC IT cloud services survey: top benefits and challenges. http://blogs.idc.com/ie/?p=210. White Paper
48. Idziorek J, Tannian M (2011) Exploiting cloud utility models for profit and ruin. IEEE Int Conf Cloud Comput, Washington, D.C., USA, pp 33–40
49. Idziorek J, Tannian M, Jacobson D (2011) Detecting fraudulent use of cloud resources. In: Proceedings of the 3rd ACM workshop on cloud computing security workshop (Chicago, IL, USA, 2011), pp 61–72.
50. Jasti A, Shah P, Nagaraj R, Pendse R (2010) Security in multi-tenancy cloud. IEEE international carnahan conference on security technology (San Jose, CA, USA, 2010), pp 35–41.
51. Jensen M, Gruschka N, Herkenhöner R (2009) A survey of attacks on web services. Comput Sci Res Dev 24(4):185–197
52. Jensen M, Gruschka N, Luttenberger N (2008) The impact of flooding attacks on network-based services. In: 3rd international conference on availability, reliability and security, Barcelona, Spain, pp 509–513.
53. Jensen M, Meyer C (2011) Expressiveness considerations of XML signatures. In: IEEE 35th annual computer software and applications conference workshop, Seoul, Korea, pp 392–397.
54. Jensen M, Schäge S, Schwenk J (2010) Towards an anonymous access control and accountability scheme for cloud computing. In: IEEE 3rd international conference on cloud computing, Miami, USA, pp 540–541.
55. Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On technical security issues in cloud computing. IEEE International conference on cloud computing, Bangalore, India, pp 109–116
56. Jin B, Wang Y, Liu Z, Xue J (2011) A trust model based on cloud model and bayesian networks. Proc, Environ Sci 11(Part A):452–459.
57. Kandukuri BR, Paturi VR, Rakshit A (2009) Cloud security issues. IEEE International conference on services computing, Bangalore, India, pp 517–520
58. Kaufman LM (2009) Data security in the world of cloud computing. IEEE Secur Privacy 7(2009):61–64
59. Khorshed MT, Ali ABMS, Wasimi SA (2012) A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Gen Comput Sys 28(2012):833–851
60. King ST, Chen PM (2006) SubVirt: implementing malware with virtual machines. IEEE Symposium on security and privacy. Oakland, CA, USA, p 327
61. Lee J-H, Park M-W, Eom J-H, Chung T-M (2011) Multi-level intrusion detection system and log management in cloud computing. In: 13th international conference on advanced communication technology, Phoenix Park, South Korea, pp 552–555.
62. Li H-C, Liang P-H, Yang J-M, Chen S-J (2010) Analysis on cloud-based security vulnerability assessment. In: IEEE 7th international conference on e-business engineering, Shanghai, China, pp 490–494.
63. Liu H (2010) A new form of DoS attack in a cloud and its avoidance mechanism. Proceedings of the ACM workshop on cloud computing security workshop, Chicago, USA, In, pp 65–76
64. Lombardi F, Pietro RD (2011) Secure virtualization for cloud computing. J Network Comput Appl 34(2011):1113–1122
65. Luo S, Lin Z, Chen X, Yang Z, Chen J (2011) Virtualization security for cloud computing service. International conference on cloud and service computing, Washington, USA, pp 174–179
66. Mansfield-Devine S (2008) Danger in the clouds. Netw Secur 2008:9–11

67. Mathisen E (2011) Security challenges and Solutions in Cloud Computing. In: Proceedings of the 5th IEEE international conference on digital ecosystems and technologies, Daejeon, South Korea, pp 208–212.
68. McGraw G (2004) Software Security. IEEE Secur Privacy 2(2004):80–83
69. McIntosh M, Austel P (2005) XML signature element wrapping attacks and countermeasures. Proceedings of the workshop on secure web services, Fairfax, USA, In, pp 20–27
70. Modi C, Patel D, Borisaniya B, Patel H, Patel A, Rajarajan M (2012) A survey of intrusion detection techniques in cloud. J Netw Comput Appl.
71. Monfared AT, Jaatun MG (2011) Monitoring intrusions and security breaches in highly distributed cloud environments. In: IEEE 3rd international conference on cloud computing technology and science, Athens, Greece, pp 772–777.
72. Morsy MA, Grundy J, Müller I (2010) An analysis of the cloud computing security problem. Proceedings of Asia pacific software engineering confernce cloud workshop, Sydney, Australia, In, pp 1–6
73. Narayanan A, Shmatikov V (2009) De-anonymizing social networks. In: 30th IEEE symposium on security and privacy, Oakland, USA, pp 173–187.
74. NIST (2012) NIST cloud computing program. http://www.nist.gov/itl/cloud/. White Paper
75. Oberheide J, Cooke E, Jahanian F (2008) Empirical exploitation of live virtual machine migration. Proceedings of the black hat conference, Washington, USA, In
76. Okamura K, Oyama Y (2010) Load-based covert channels between Xen virtual machines. Proceedings of the ACM symposium on applied computing, Sierre, Switzerland, In, pp 173–180
77. OWASP (2010) The then most critical web application security risks. http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf. White Paper
78. Patel A, Taghavi M, Bakhtiyari K, Júnior JC (2012) A systematic review. J Netw Comput Appl Intrusion Detec Prev Sys Cloud Comput.
79. PCI (2012) PCI SSC data security standards overview. https://www.pcisecuritystandards.org/security_standards/index.php. White Paper
80. Pfaff B, Pettit J, Koponen T, Amidon K, Casado M, Shenker S (2009) Extending networking into the virtualization layer. In: Proceedings of the 8th ACM workshop on hot topics in Networks.
81. Pianese F, Bosch P, Duminuco A, Janssens N, Stathopoulos T, Steiner M (2010) Toward a cloud operating system. IEEE/IFIP network operations and management symposium workshop, Osaka, Japan, In, pp 335–342
82. Rahaman MA, Schaad A, Rits M (2006) Towards secure SOAP message exchange in a SOA. In: Proceedings of the 3rd ACM workshop on secure web services, Alexandria, USA, pp 77–84.
83. Ramgovind S, Eloff MM, Smith E (2010) The management of security in cloud computing. Information security for South Africa, Johannesburg, South Africa, pp 1–7
84. Riquet D, Grimaud G, Hauspie M (2012) Large-scale coordinated attacks: Impact on the cloud security. In: 6th international conference on innovative mobile and internet services in ubiquitous computing, Palermo, Italy, pp 558–563.
85. 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, Chicago, USA, pp 199–212.
86. Roberts JC, Al-Hamdani W (2011) Who can you trust in the cloud?: A review of security issues within cloud computing. Proceedings of the information security curriculum development conference, Kennesaw, GA, In, pp 15–19
87. Rocha F, Correia M (2011) Lucy in the sky without diamonds: stealing confidential data in the cloud. In: IEEE/IFIP 41st international conference on dependable systems and networks workshops, pp 129–134.
88. Rong C, Nguyen ST, Jaatun MG (2012) A survey on security challenges in cloud computing. Comput Elect Engi Beyond Lightning.

89. Rutkowska J (2008) Subverting vistaTM Kernel for fun and profit. Black Hat Conv, Washington, D.C., USA
90. Sadashiv N, Kumar SMD (2011) Cluster, grid and cloud computing: a detailed comparison. In: 6th international conference on computer science education, SuperStar Virgo, Singapore, pp 477–482.
91. Santos N, Gummadi KP, Rodrigues R (2009) Towards trusted cloud computing. Proceedings of the conference on hot topics in cloud computing, San Diego, CA, USA, In
92. Sengupta S, Kaulgud V, Sharma VS (2011) Cloud computing security–trends and research directions. IEEE World Congress Services, Washington D.C., 2011, pp 524–531.
93. Sloan K (2009) Security in a virtualised world. Netw Secur 2009(2009):15–18
94. SplashData (2012) Scary logins: worst passwords of 2012 and how to fix them. http://splashdata.com/press/PR121023.htm. White Paper
95. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(2011):1–11
96. Suzaki K, Iijima K, Yagi T, Artho C (2011) Memory deduplication as a threat to the guest OS. In: Proceedings of the 4th European workshop on system security, New York, USA, vol 1:1–1:6.
97. Suzaki K, Iijima K, Yagi T, Artho C (2011) Software side channel attack on memory deduplication. 23rd ACM symposium on operating systems principles.
98. Takabi H, Joshi JBD, Ahn G (2010) Security and privacy challenges in cloud computing environments. IEEE Secur Privacy 8(2010):24–31
99. Taylor M, Haggerty J, Gresty D (2011) Lamb D (2011) Forensic investigation of cloud computing systems. Netw Secur 2011:4–10
100. Toubiana V, Nissenbaum H (2011) Analysis of Google logs retention policies. J Priv Confidentiality 3(2011):3–26
101. Townsend M (2009) Managing a security program in a cloud computing environment. Information security curriculum development conference, Kennesaw, GA, USA, pp 128–133
102. Tripathi A, Mishra A (2011) Cloud computing security considerations. IEEE international conference on signal processing, communications and computing, Xi'an, Shaanxi, China, In, pp 1–5
103. Tsai H-Y, Siebenhaar M, Miede A, Huang Y, Steinmetz R (2012) Threat as a service? virtualization's impact on cloud security. IT Professional 14(2012):32–37
104. Vaquero LM, Rodero-Merino L, Morán D (2011) Locking the sky: a survey on IaaS cloud security. Computing 91(2011):93–118
105. Vascellaro JE (2009) Google discloses privacy glitch. http://blogs.wsj.com/digits/2009/03/08/1214/
106. Viega J (2009) Cloud computing and the common man. Computer 42(2009):106–108
107. Wang C, Ren K, Lou W, Li J (2010) Toward publicly auditable secure cloud data storage services. IEEE Network 24(2010):19–24
108. Wang C, Wang Q, Ren K, Lou W (2009) Ensuring data storage security in cloud computing. In: 17th international workshop on quality of service, Charleston, SC, USA, pp 1–9.
109. Ward M (2009) Facebook users suffer viral surge. http://news.bbc.co.uk/2/hi/technology/7918839.stm
110. Wei J, Zhang X, Ammons G, Bala V, Ning P (2009) Managing security of virtual machine images in a cloud environment. Proceedings of the ACM workshop on cloud computing security, New York, USA, In, pp 91–96
111. Xiao Z, Xiao Y (2012) Security and privacy in cloud computing. IEEE Commun Surv Tutorials 2012:1–17
112. Yang K, Jia X (2012) Data storage auditing service in cloud computing: challenges. Methods Opportunities World Wide Web 15(2012):409–428
113. Yu H, Powell N, Stembridge D, Yuan X (2012) Cloud computing and security challenges. In: Proceedings of the 50th annual southeast regional conference, Tuscaloosa, USA, pp 298–302.
114. Zhang F, Huang Y, Wang H, Chen H, Zang B (2008) PALM: security preserving VM live migration for systems with VMM-enforced protection. In: 3rd Asia-Pacific trusted infrastructure technologies conference, Wuhan, China, pp 9–18.

115. Zhou M, Zhang R, Xie W, Qian W, Zhou A (2010) Security and privacy in cloud computing: a survey. In: 6th international conference on semantics knowledge and grid (Ningbo, China, 2010), pp 105–112.
116. Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Future Gener Comput Sys 28(2012):583–592
117. Zou B, Zhang H (2011) Toward enhancing trust in cloud computing environment. In: 2nd international conference on control, instrumentation and automation, Shiraz, Iran, pp 364–366.