Research

Journal of Internet Services and Applications

December 2013, 4:5

First online: 27 February 2013

An analysis of security issues for cloud computing

- Keiko Hashizume
- , David G Rosado
- , Eduardo Fernández-Medina
- , Eduardo B Fernandez

10.1186/1869-0238-4-5

Abstract

Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. However, cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. Cloud Computing leverages many technologies (SOA, virtualization, Web 2.0); it also inherits their security issues, which we discuss here, identifying the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing and its environment as well as to identify and relate vulnerabilities and threats with possible solutions.

Keywords

Cloud computing Security SPI model Vulnerabilities Threats Countermeasures

1 1. Introduction

The importance of Cloud Computing is increasing and it is receiving a growing attention in the scientific and industrial communities. A study by Gartner [1] considered Cloud Computing as the first among the top 10 most important technologies and with a better prospect in successive years by companies and organizations.

Cloud Computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud Computing appears as a computational paradigm as well as a distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet [2, 3]. The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing [4 - 7].

Cloud Computing combines a number of computing concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, virtualization and other technologies with reliance on the Internet, providing common business applications online through web browsers to satisfy the computing needs of users, while their software and data are stored on the servers [5]. In some respects, Cloud Computing represents the maturing of these technologies and is a marketing term to represent that maturity and the services they provide [6].

Although there are many benefits to adopting Cloud Computing, there are also some significant barriers to adoption. One of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters [8]. Because Cloud Computing represents a relatively new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved and how applications security is moved to Cloud Computing [9]. That uncertainty has consistently led information executives to state that security is their number one concern with Cloud Computing [10].

Security concerns relate to risk areas such as external data storage, dependency on the “public” internet, lack of control, multi-tenancy and integration with internal security. Compared to traditional technologies, the cloud has many specific features, such as its large

scale and the fact that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form [11]. Security controls in Cloud Computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, Cloud Computing may present different risks to an organization than traditional IT solutions. Unfortunately, integrating security into these solutions is often perceived as making them more rigid [4].

Moving critical applications and sensitive data to public cloud environments is of great concern for those corporations that are moving beyond their data center's network under their control. To alleviate these concerns, a cloud solution provider must ensure that customers will continue to have the same security and privacy controls over their applications and services, provide evidence to customers that their organization are secure and they can meet their service-level agreements, and that they can prove compliance to auditors [12].

We present here a categorization of security issues for Cloud Computing focused in the so-called SPI model (SaaS, PaaS and IaaS), identifying the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing and its environment. A *threat* is a potential attack that may lead to a misuse of information or resources, and the term *vulnerability* refers to the flaws in a system that allows an attack to be successful. There are some surveys where they focus on one service model, or they focus on listing cloud security issues in general without distinguishing among vulnerabilities and threats. Here, we present a list of vulnerabilities and threats, and we also indicate what cloud service models can be affected by them. Furthermore, we describe the relationship between these vulnerabilities and threats; how these vulnerabilities can be exploited in order to perform an attack, and also present some countermeasures related to these threats which try to solve or improve the identified problems.

The remainder of the paper is organized as follows: Section 2 presents the results obtained from our systematic review. Next, in Section 3 we define in depth the most important security aspects for each layer of the Cloud model. Later, we will analyze the security issues in Cloud Computing identifying the main vulnerabilities for

clouds, the most important threats in clouds, and all available countermeasures for these threats and vulnerabilities. Finally, we provide some conclusions.

1.1 1.1 Systematic review of security issues for cloud computing

We have carried out a systematic review [13 - 15] of the existing literature regarding security in Cloud Computing, not only in order to summarize the existing vulnerabilities and threats concerning this topic but also to identify and analyze the current state and the most important security issues for Cloud Computing.

1.2 1.2 Question formalization

The question focus was to identify the most relevant issues in Cloud Computing which consider vulnerabilities, threats, risks, requirements and solutions of security for Cloud Computing. This question had to be related with the aim of this work; that is to identify and relate vulnerabilities and threats with possible solutions. Therefore, the research question addressed by our research was the following: What security vulnerabilities and threats are the most important in Cloud Computing which have to be studied in depth with the purpose of handling them? The keywords and related concepts that make up this question and that were used during the review execution are: secure Cloud systems, Cloud security, delivery models security, SPI security, SaaS security, Paas security, IaaS security, Cloud threats, Cloud vulnerabilities, Cloud recommendations, best practices in Cloud.

1.3 1.3 Selection of sources

The selection criteria through which we evaluated study sources was based on the research experience of the authors of this work, and in order to select these sources we have considered certain constraints: studies included in the selected sources must be written in English and these sources must be web-available. The following list of sources has been considered: ScienceDirect, ACM digital library, IEEE digital library, Scholar Google and DBLP. Later, the experts will refine the results and will include important works that had not been recovered in these sources and will update these work taking into

account other constraints such as impact factor, received cites, important journals, renowned authors, etc.

Once the sources had been defined, it was necessary to describe the process and the criteria for study selection and evaluation. The inclusion and exclusion criteria of this study were based on the research question. We therefore established that the studies must contain issues and topics which consider security on Cloud Computing, and that these studies must describe threats, vulnerabilities, countermeasures, and risks.

1.4 1.4 Review execution

During this phase, the search in the defined sources must be executed and the obtained studies must be evaluated according to the established criteria. After executing the search chain on the selected sources we obtained a set of about 120 results which were filtered with the inclusion criteria to give a set of about 40 relevant studies. This set of relevant studies was again filtered with the exclusion criteria to give a set of studies which corresponds with 15 primary proposals [4, 6, 10, 16 - 27].

2 2. Results and discussion

The results of the systematic review are summarized in Table 1 which shows a summary of the topics and concepts considered for each approach.
Table 1

Summary of the topics considered in each approach

Topics/References	[4]	[6]	[10]	[16]	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]	[27]
Vulnerabilities		X		X	X	X	X	X	X			X			X
Threats		X		X	X	X	X	X	X	X	X	X	X	X	X
Mechanisms/Recommendations	X			X		X		X				X	X	X	X
Security Standards							X			X					
Data Security	X		X				X		X		X		X		X
Trust			X								X		X	X	X

Topics/References	[4]	[6]	[10]	[16]	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]	[27]
Security Requirements	X		X						X		X			X	X
SaaS, PaaS, IaaS Security					X				X			X			

As it is shown in Table 1, most of the approaches discussed identify, classify, analyze, and list a number of vulnerabilities and threats focused on Cloud Computing. The studies analyze the risks and threats, often give recommendations on how they can be avoided or covered, resulting in a direct relationship between vulnerability or threats and possible solutions and mechanisms to solve them. In addition, we can see that in our search, many of the approaches, in addition to speaking about threats and vulnerabilities, also discuss other issues related to security in the Cloud such as the data security, trust, or security recommendations and mechanisms for any of the problems encountered in these environments.

2.1 2.1 Security in the SPI model

The cloud model provides three types of services [21, 28, 29]:

- Software as a Service (SaaS). The capability provided to the consumer is to use the provider’ s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).
- Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure his own applications without installing any platform or tools on their local machines. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services.
- Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

With SaaS, the burden of security lies with the cloud provider. In part, this is because of the degree of abstraction, the SaaS model is based on a high degree of integrated functionality with minimal customer control or extensibility. By contrast, the PaaS model offers greater extensibility and greater customer control. Largely because of the relatively lower degree of abstraction, IaaS offers greater tenant or customer control over security than do PaaS or SaaS [10].

Before analyzing security challenges in Cloud Computing, we need to understand the relationships and dependencies between these cloud service models [4]. PaaS as well as SaaS are hosted on top of IaaS; thus, any breach in IaaS will impact the security of both PaaS and SaaS services, but also it may be true on the other way around. However, we have to take into account that PaaS offers a platform to build and deploy SaaS applications, which increases the security dependency between them. As a consequence of these deep dependencies, any attack to any cloud service layer can compromise the upper layers. Each cloud service model comprises its own inherent security flaws; however, they also share some challenges that affect all of them. These relationships and dependencies between cloud models may also be a source of security risks. A SaaS provider may rent a development environment from a PaaS provider, which might also rent an infrastructure from an IaaS provider. Each provider is responsible for securing his own services, which may result in an inconsistent combination of security models. It also creates confusion over which service provider is responsible once an attack happens.

2.2 2.2 Software-as-a-service (SaaS) security issues

SaaS provides application services on demand such as email, conferencing software, and business applications such as ERP, CRM, and SCM [30]. SaaS users have less control over security among the three fundamental delivery models in the cloud. The adoption of SaaS applications may raise some security concerns.

2.3 2.3 Application security

These applications are typically delivered via the Internet through a Web browser [12, 22]. However, flaws in web applications may create vulnerabilities for the SaaS applications. Attackers have been using the web to compromise user’s computers and perform malicious activities such as steal sensitive data [31]. Security challenges in SaaS applications are not different from any web application

technology, but traditional security solutions do not effectively protect it from attacks, so new approaches are necessary [21]. The Open Web Application Security Project (OWASP) has identified the ten most critical web applications security threats [32]. There are more security issues, but it is a good start for securing web applications.

2.4 2.4 Multi-tenancy

SaaS applications can be grouped into maturity models that are determined by the following characteristics: scalability, configurability via metadata, and multi-tenancy [30, 33]. In the first maturity model, each customer has his own customized instance of the software. This model has drawbacks, but security issues are not so bad compared with the other models. In the second model, the vendor also provides different instances of the applications for each customer, but all instances use the same application code. In this model, customers can change some configuration options to meet their needs. In the third maturity model multi-tenancy is added, so a single instance serves all customers [34]. This approach enables more efficient use of the resources but scalability is limited. Since data from multiple tenants is likely to be stored in the same database, the risk of data leakage between these tenants is high. Security policies are needed to ensure that customer's data are kept separate from other customers [35]. For the final model, applications can be scaled up by moving the application to a more powerful server if needed.

2.5 2.5 Data security

Data security is a common concern for any technology, but it becomes a major challenge when SaaS users have to rely on their providers for proper security [12, 21, 36]. In SaaS, organizational data is often processed in plaintext and stored in the cloud. The SaaS provider is the one responsible for the security of the data while is being processed and stored [30]. Also, data backup is a critical aspect in order to facilitate recovery in case of disaster, but it introduces security concerns as well [21]. Also cloud providers can subcontract other services such as backup from third-party service providers, which may raise concerns. Moreover, most compliance standards do not envision compliance with regulations in a world of Cloud Computing [12]. In the world of SaaS, the process of compliance is complex because data is located in the provider's datacenters, which may

introduce regulatory compliance issues such as data privacy, segregation, and security, that must be enforced by the provider.

2.6 2.6 Accessibility

Accessing applications over the internet via web browser makes access from any network device easier, including public computers and mobile devices. However, it also exposes the service to additional security risks. The Cloud Security Alliance [37] has released a document that describes the current state of mobile computing and the top threats in this area such as information stealing mobile malware, insecure networks (WiFi), vulnerabilities found in the device OS and official applications, insecure marketplaces, and proximity-based hacking.

2.7 2.7 Platform-as-a-service (PaaS) security issues

PaaS facilitates deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers [21]. As with SaaS and IaaS, PaaS depends on a secure and reliable network and secure web browser. PaaS application security comprises two software layers: Security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform [10]. PaaS providers are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications. Same as SaaS, PaaS also brings data security issues and other challenges that are described as follows:

2.7.1 2.7.1 Third-party relationships

Moreover, PaaS does not only provide traditional programming languages, but also does it offer third-party web services components such as mashups [10, 38]. Mashups combine more than one source element into a single integrated unit. Thus, PaaS models also inherit security issues related to mashups such as data and network security [39]. Also, PaaS users have to depend on both the security of web-hosted development tools and third-party services.

2.7.2 2.7.2 Development Life Cycle

From the perspective of the application development, developers face the complexity of building secure applications that may be hosted in the cloud. The speed at which applications will change in the cloud

will affect both the System Development Life Cycle (SDLC) and security [12, 24]. Developers have to keep in mind that PaaS applications should be upgraded frequently, so they have to ensure that their application development processes are flexible enough to keep up with changes [19]. However, developers also have to understand that any changes in PaaS components can compromise the security of their applications. Besides secure development techniques, developers need to be educated about data legal issues as well, so that data is not stored in inappropriate locations. Data may be stored on different places with different legal regimes that can compromise its privacy and security.

2.7.3 2.7.3 Underlying infrastructure security

In PaaS, developers do not usually have access to the underlying layers, so providers are responsible for securing the underlying infrastructure as well as the applications services [40]. Even when developers are in control of the security of their applications, they do not have the assurance that the development environment tools provided by a PaaS provider are secure.

In conclusion, there is less material in the literature about security issues in PaaS. SaaS provides software delivered over the web while PaaS offers development tools to create SaaS applications. However, both of them may use multi-tenant architecture so multiple concurrent users utilize the same software. Also, PaaS applications and user’s data are also stored in cloud servers which can be a security concern as discussed on the previous section. In both SaaS and PaaS, data is associated with an application running in the cloud. The security of this data while it is being processed, transferred, and stored depends on the provider.

2.8 2.8 Infrastructure-as-a-service (IaaS) security issues

IaaS provides a pool of resources such as servers, storage, networks, and other computing resources in the form of virtualized systems, which are accessed through the Internet [24]. Users are entitled to run any software with full control and management on the resources allocated to them [18]. With IaaS, cloud users have better control over the security compared to the other models as long there is no security hole in the virtual machine monitor [21]. They control the software running in their virtual machines, and they are responsible to configure security policies correctly [41]. However, the underlying compute, network, and storage infrastructure is controlled

by cloud providers. IaaS providers must undertake a substantial effort to secure their systems in order to minimize these threats that result from creation, communication, monitoring, modification, and mobility [42]. Here are some of the security issues associated to IaaS.

2.9 2.9 Virtualization

Virtualization allows users to create, copy, share, migrate, and roll back virtual machines, which may allow them to run a variety of applications [43, 44]. However, it also introduces new opportunities for attackers because of the extra layer that must be secured [31]. Virtual machine security becomes as important as physical machine security, and any flaw in either one may affect the other [19]. Virtualized environments are vulnerable to all types of attacks for normal infrastructures; however, security is a greater challenge as virtualization adds more points of entry and more interconnection complexity [45]. Unlike physical servers, VMs have two boundaries: physical and virtual [24].

2.10 2.10 Virtual machine monitor

The Virtual Machine Monitor (VMM) or hypervisor is responsible for virtual machines isolation; therefore, if the VMM is compromised, its virtual machines may potentially be compromised as well. The VMM is a low-level software that controls and monitors its virtual machines, so as any traditional software it entails security flaws [45]. Keeping the VMM as simple and small as possible reduces the risk of security vulnerabilities, since it will be easier to find and fix any vulnerability.

Moreover, virtualization introduces the ability to migrate virtual machines between physical servers for fault tolerance, load balancing or maintenance [16, 46]. This useful feature can also raise security problems [42, 43, 47]. An attacker can compromise the migration module in the VMM and transfer a victim virtual machine to a malicious server. Also, it is clear that VM migration exposes the content of the VM to the network, which can compromise its data integrity and confidentiality. A malicious virtual machine can be migrated to another host (with another VMM) compromising it.

2.11 2.11 Shared resource

VMs located on the same server can share CPU, memory, I/O, and others. Sharing resources between VMs may decrease the security of each VM. For example, a malicious VM can infer some information about other VMs through shared memory or other shared resources without need of compromising the hypervisor [46]. Using covert channels, two VMs can communicate bypassing all the rules defined by the security module of the VMM [48]. Thus, a malicious Virtual Machine can monitor shared resources without being noticed by its VMM, so the attacker can infer some information about other virtual machines.

2.12 2.12 Public VM image repository

In IaaS environments, a VM image is a prepackaged software template containing the configurations files that are used to create VMs. Thus, these images are fundamental for the the overall security of the cloud [46, 49]. One can either create her own VM image from scratch, or one can use any image stored in the provider's repository. For example, Amazon offers a public image repository where legitimate users can download or upload a VM image. Malicious users can store images containing malicious code into public repositories compromising other users or even the cloud system [20, 24, 25]. For example, an attacker with a valid account can create an image containing malicious code such as a Trojan horse. If another customer uses this image, the virtual machine that this customer creates will be infected with the hidden malware. Moreover, unintentionally data leakage can be introduced by VM replication [20]. Some confidential information such as passwords or cryptographic keys can be recorded while an image is being created. If the image is not "cleaned", this sensitive information can be exposed to other users. VM images are dormant artifacts that are hard to patch while they are offline [50].

2.13 2.13 Virtual machine rollback

Furthermore, virtual machines are able to be rolled back to their previous states if an error happens. But rolling back virtual machines can re-expose them to security vulnerabilities that were patched or re-enable previously disabled accounts or passwords. In order to provide rollbacks, we need to make a "copy" (snapshot) of the virtual machine, which can result in the propagation of configuration errors and other vulnerabilities [12, 44].

2.14 2.14 Virtual machine life cycle

Additionally, it is important to understand the lifecycle of the VMs and their changes in states as they move through the environment. VMs can be on, off, or suspended which makes it harder to detect malware. Also, even when virtual machines are offline, they can be vulnerable [24]; that is, a virtual machine can be instantiated using an image that may contain malicious code. These malicious images can be the starting point of the proliferation of malware by injecting malicious code within other virtual machines in the creation process.

2.15 2.15 Virtual networks

Network components are shared by different tenants due to resource pooling. As mentioned before, sharing resources allows attackers to launch cross-tenant attacks [20]. Virtual Networks increase the VMs interconnectivity, an important security challenge in Cloud Computing [51]. The most secure way is to hook each VM with its host by using dedicated physical channels. However, most hypervisors use virtual networks to link VMs to communicate more directly and efficiently. For instance, most virtualization platforms such as Xen provide two ways to configure virtual networks: bridged and routed, but these techniques increase the possibility to perform some attacks such as sniffing and spoofing virtual network [45, 52].

2.16 2.16 Analysis of security issues in cloud computing

We systematically analyze now existing security vulnerabilities and threats of Cloud Computing. For each vulnerability and threat, we identify what cloud service model or models are affected by these security problems.

Table 2 presents an analysis of vulnerabilities in Cloud Computing. This analysis offers a brief description of the vulnerabilities, and indicates what cloud service models (SPI) can be affected by them. For this analysis, we focus mainly on technology-based vulnerabilities; however, there are other vulnerabilities that are common to any organization, but they have to be taken in consideration since they can negatively impact the security of the cloud and its underlying platform. Some of these vulnerabilities are the following:

- Lack of employee screening and poor hiring practices [16] – some cloud providers may not perform background screening of their employees or providers. Privileged users such as cloud administrators usually have unlimited access to the cloud data.
- Lack of customer background checks – most cloud providers do not check their customer's background, and almost anyone can open an account with a valid credit card and email. Apocryphal accounts can let attackers perform any malicious activity without being identified [16].
- Lack of security education – people continue to be a weak point in information security [53]. This is true in any type of organization; however, in the cloud, it has a bigger impact because there are more people that interact with the cloud: cloud providers, third-party providers, suppliers, organizational customers, and end-users.

Cloud Computing leverages many existing technologies such as web services, web browsers, and virtualization, which contributes to the evolution of cloud environments. Therefore, any vulnerability associated to these technologies also affects the cloud, and it can even have a significant impact.

Table 2

Vulnerabilities in cloud computing

ID	Vulnerabilities	Description	Layer
V01	Insecure interfaces and APIs	Cloud providers offer services that can be accessed through APIs (SOAP, REST, or HTTP with XML/JSON) [42]. The security of the cloud depends upon the security of these interfaces [16]. Some problems are:	SPI
		a) Weak credential	
		b) Insufficient authorization checks	
		c) Insufficient input-data validation	
		Also, cloud APIs are still immature which means that are frequently updated. A fixed bug can introduce another security hole in the application [54].	
V02	Unlimited allocation of resources	Inaccurate modeling of resource usage can lead to overbooking or over-provisioning [17].	SPI

ID	Vulnerabilities	Description	Layer
V03	Data-related vulnerabilities	a) Data can be colocated with the data of unknown owners (competitors, or intruders) with a weak separation [36]	SPI
		b) Data may be located in different jurisdictions which have different laws [19, 54, 55]	
		c) Incomplete data deletion - data cannot be completely removed [19, 20, 25, 56]	
		d) Data backup done by untrusted third-party providers [56, 57]	
		e) Information about the location of the data usually is unavailable or not disclosed to users [25]	
		f) Data is often stored, processed, and transferred in clear plain text	
V04	Vulnerabilities in Virtual Machines	a) Possible covert channels in the colocation of VMs [48, 58, 59]	I
		b) Unrestricted allocation and deallocation of resources with VMs [57]	
		c) Uncontrolled Migration - VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance [42, 44]	
		d) Uncontrolled snapshots - VMs can be copied in order to provide flexibility [12], which may lead to data leakage	
		e) Uncontrolled rollback could lead to reset vulnerabilities - VMs can be backed up to a previous state for restoration [44], but patches applied after the previous state disappear	
		f) VMs have IP addresses that are visible to anyone within the cloud - attackers can map where the target VM is located within the cloud (Cloud cartography [58])	
V05	Vulnerabilities in Virtual Machine Images	a) Uncontrolled placement of VM images in public repositories [24]	I
		b) VM images are not able to be patched since they are dormant artifacts [44]	
V06		a) Complex hypervisor code [60]	I

ID	Vulnerabilities	Description	Layer
	Vulnerabilities in Hypervisors	b) Flexible configuration of VMs or hypervisors to meet organization needs can be exploited	
V07	Vulnerabilities in Virtual Networks	Sharing of virtual bridges by several virtual machines [51]	I

From Table 2, we can conclude that data storage and virtualization are the most critical and an attack to them can do the most harm. Attacks to lower layers have more impact to the other layers. Table 3 presents an overview of threats in Cloud Computing. Like Table 2 it also describes the threats that are related to the technology used in cloud environments, and it indicates what cloud service models are exposed to these threats. We put more emphasis on threats that are associated with data being stored and processed remotely, sharing resources and the usage of virtualization.

Table 3

Threats in cloud computing

ID	Threats	Description	Layer
T01	Account or service hijacking	An account theft can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user's credential, he can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction [16].	SPI
T02	Data scavenging	Since data cannot be completely removed from unless the device is destroyed, attackers may be able to recover this data [10, 17, 25].	SPI
T03	Data leakage	Data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed [16, 17, 20, 58].	SPI
T04	Denial of Service	It is possible that a malicious user will take all the possible resources. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable.	SPI
T05	Customer-data manipulation	Users attack web applications by manipulating data sent from their application component to the server's	S

ID	Threats	Description	Layer
		application [20, 32]. For example, SQL injection, command injection, insecure direct object references, and cross-site scripting.	
T06	VM escape	It is designed to exploit the hypervisor in order to take control of the underlying infrastructure [24, 61].	I
T07	VM hopping	It happens when a VM is able to gain access to another VM (i.e. by exploting some hypervisor vulnerability) [17, 43]	I
T08	Malicious VM creation	An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository [20].	I
T09	Insecure VM migration	Live migration of virtual machines exposes the contents of the VM state files to the network. An attacker can do the following actions:	I
		a) Access data illegally during migration [42]	
		b) Transfer a VM to an untrusted host [44]	
		c) Create and migrate several VM causing disruptions or DoS	
T10	Sniffing/Spoofing virtual networks	A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VMs [45, 51].	I

The relationship between threats and vulnerabilities is illustrated in Table 4, which describes how a threat can take advantage of some vulnerability to compromise the system. The goal of this analysis is also to identify some existing defenses that can defeat these threats. This information can be expressed in a more detailed way using misuse patterns [62]. Misuse patterns describe how a misuse is performed from the point of view of the attacker. For instance, in threat T10, an attacker can read or tamper with the contents of the VM state files during live migration. This can be possible because VM migration transfer the data over network channels that are often insecure, such as the Internet. Insecure VM migration can be mitigated by the following proposed techniques: TCCP [63] provides confidential execution of VMs and secure migration operations as well. PALM [64] proposes a secure migration system that provides VM

live migration capabilities under the condition that a VMM-protected system is present and active. Threat 11 is another cloud threat where an attacker creates malicious VM image containing any type of virus or malware. This threat is feasible because any legitimate user can create a VM image and publish it on the provider's repository where other users can retrieve them. If the malicious VM image contains malware, it will infect other VMs instantiated with this malicious VM image. In order to overcome this threat, an image management system was proposed, Mirage [49]. It provides the following security management features: access control framework, image filters, provenance tracking system, and repository maintenance services.

Table 4

Relationships between threats, vulnerabilities, and countermeasures

Threat	Vulnerabilities	Incidents	Countermeasures
T01	V01	An attacker can use the victim's account to get access to the target's resources.	Identity and Access Management Guidance [65]
			Dynamic credential [66]
T02	V03a, V03c	Data from hard drives that are shared by several customers cannot be completely removed.	Specify destruction strategies on Service-level Agreements (SLAs)
T03	V03a, V03c, V03d, V03f, V04a-f, V05a, V07	Authors in [58] illustrated the steps necessary to gain confidential information from other VMs co-located in the same server as the attacker.	FRS techniques [67]
			Digital Signatures [68]
		Side channel [69]	Encryption [69]
			Homomorphic encryption [70]
T04	V01, V02	An attacker can request more computational resources, so other legal users are not able to get additional capacity.	Cloud providers can force policies to offer limited computational resources
T05	V01	Some examples are described in [32] such as SQL, command	Web application scanners [71]

Threat	Vulnerabilities	Incidents	Countermeasures
		injection, and cross-site scripting	
T06	V06a, V06b	A zero-day exploit in the HyperVM virtualization application that destroyed about 100,000 websites [72]	HyperSafe [60]
			TCCP (Trusted Cloud Computing Platform) [63]
			TVDc (Trusted Virtual Datacenter) [73, 74]
T07	V04b, V06b	[75] presents a study that demonstrates security flaws in most virtual machines monitors	
T08	V05a, V05b	An attacker can create a VM image containing malware and publish it in a public repository.	Mirage [49]
T09	V04d	[76] has empirically showed attacks against the migration functionality of the latest version of the Xen and VMware virtualization products.	PALM [64]
			TCCP [63]
			VNSS [52]
T10	V07	Sniffing and spoofing virtual networks [51]	Virtual network framework based on Xen network modes: “bridged” and “routed” [51]

2.17 2.17 Countermeasures

In this section, we provide a brief description of each countermeasure mentioned before, except for threats T02 and T07.

2.17.1 2.17.1 Countermeasures for T01: account or service hijacking

2.17.1.1 2.17.1.1 Identity and access management guidance

Cloud Security Alliance (CSA) is a non-profit organization that promotes the use of best practices in order to provide security in

cloud environments. CSA has issued an Identity and Access Management Guidance [65] which provides a list of recommended best practiced to assure identities and secure access management. This report includes centralized directory, access management, identity management, role-based access control, user access certifications, privileged user and access management, separation of duties, and identity and access reporting.

2.17.1.2 2.17.1.2 Dynamic credentials

[66] presents an algorithm to create dynamic credentials for mobile cloud computing systems. The dynamic credential changes its value once a user changes its location or when he has exchanged a certain number of data packets.

2.17.2 2.17.2 Countermeasures for T03: data leakage

2.17.2.1 2.17.2.1 Fragmentation-redundancy-scattering (FRS) technique

[67] this technique aims to provide intrusion tolerance and, in consequence, secure storage. This technique consists in first breaking down sensitive data into insignificant fragments, so any fragment does not have any significant information by itself. Then, fragments are scattered in a redundant fashion across different sites of the distributed system.

2.17.2.2 2.17.2.2 Digital signatures

[68] proposes to secure data using digital signature with RSA algorithm while data is being transferred over the Internet. They claimed that RSA is the most recognizable algorithm, and it can be used to protect data in cloud environments.

2.17.2.3 2.17.2.3 Homomorphic encryption

The three basic operations for cloud data are transfer, store, and process. Encryption techniques can be used to secure data while it is being transferred in and out of the cloud or stored in the provider’s premises. Cloud providers have to decrypt cipher data in order to process it, which raises privacy concerns. In [70], they propose a method based on the application of fully homomorphic encryption to the security of clouds. Fully homomorphic encryption allows performing arbitrary computation on ciphertexts without being decrypted. Current homomorphic encryption schemes support limited number of homomorphic operations such as addition and multiplication.

The authors in [77] provided some real-world cloud applications where some basic homomorphic operations are needed. However, it requires a huge processing power which may impact on user response time and power consumption.

2.17.2.4 2.17.2.4 Encryption

Encryption techniques have been used for long time to secure sensitive data. Sending or storing encrypted data in the cloud will ensure that data is secure. However, it is true assuming that the encryption algorithms are strong. There are some well-known encryption schemes such as AES (Advanced Encryption Standard). Also, SSL technology can be used to protect data while it is in transit. Moreover, [69] describes that encryption can be used to stop side channel attacks on cloud storage de-duplication, but it may lead to offline dictionary attacks reveling personal keys.

2.17.3 2.17.3 Countermeasures for T05: customer data manipulation

2.17.3.1 2.17.3.1 Web application scanners

Web applications can be an easy target because they are exposed to the public including potential attackers. Web application scanners [71] is a program which scans web applications through the web front-end in order to identify security vulnerabilities. There are also other web application security tools such as web application firewall. Web application firewall routes all web traffic through the web application firewall which inspects specific threats.

2.17.4 2.17.4 Countermeasures for T06: VM escape

2.17.4.1 2.17.4.1 HyperSafe

[60] It is an approach that provides hypervisor control-flow integrity. HyperSafe's goal is to protect type I hypervisors using two techniques: non-bypassable memory lockdown which protects write-protected memory pages from being modified, and restricted pointed indexing that converts control data into pointer indexes. In order to evaluate the effectiveness of this approach, they have conducted four types of attacks such as modify the hypervisor code, execute the injected code, modify the page table, and tamper from a return table. They concluded that HyperSafe successfully prevented all these attacks, and that the performance overhead is low.

2.17.4.2 2.17.4.2 Trusted cloud computing platform

TCCP [63] enables providers to offer closed box execution environments, and allows users to determine if the environment is secure before launching their VMs. The TCCP adds two fundamental elements: a trusted virtual machine monitor (TVMM) and a trusted coordinator (TC). The TC manages a set of trusted nodes that run TVMMs, and it is maintained but a trusted third party. The TC participates in the process of launching or migrating a VM, which verifies that a VM is running in a trusted platform. The authors in [78] claimed that TCCP has a significant downside due to the fact that all the transactions have to verify with the TC which creates an overload. They proposed to use Direct Anonymous Attestation (DAA) and Privacy CA scheme to tackle this issue.

2.17.4.3 2.17.4.3 Trusted virtual datacenter

TVDc [73, 74] insures isolation and integrity in cloud environments. It groups virtual machines that have common objectives into workloads named Trusted Virtual Domains (TVDs). TVDc provides isolation between workloads by enforcing mandatory access control, hypervisor-based isolation, and protected communication channels such as VLANs. TVDc provides integrity by employing load-time attestation mechanism to verify the integrity of the system.

2.17.5 2.17.5 Countermeasures for T08: malicious virtual machine creation

2.17.5.1 2.17.5.1 Mirage

In [49], the authors propose a virtual machine image management system in a cloud computing environments. This approach includes the following security features: access control framework, image filters, a provenance tracking, and repository maintenance services. However, one limitation of this approach is that filters may not be able to scan all malware or remove all the sensitive data from the images. Also, running these filters may raise privacy concerns because they have access to the content of the images which can contain customer’s confidential data.

2.17.6 2.17.6 Countermeasures for T09: insecure virtual machine migration

2.17.6.1 2.17.6.1 Protection aegis for live migration of VMs (PALM)

[64] proposes a secure live migration framework that preserves integrity and privacy protection during and after migration. The

prototype of the system was implemented based on Xen and GNU Linux, and the results of the evaluation showed that this scheme only adds slight downtime and migration time due to encryption and decryption.

2.17.6.2 2.17.6.2 VNSS

[52] proposes a security framework that customizes security policies for each virtual machine, and it provides continuous protection thorough virtual machine live migration. They implemented a prototype system based on Xen hypervisors using stateful firewall technologies and userspace tools such as iptables, xm commands program and conntrack-tools. The authors conducted some experiments to evaluate their framework, and the results revealed that the security policies are in place throughout live migration.

2.17.7 2.17.7 Countermeasures for T010: sniffing/spoofing virtual networks

2.17.7.1 2.17.7.1 Virtual network security

Wu and et al. [51] presents a virtual network framework that secures the communication among virtual machines. This framework is based on Xen which offers two configuration modes for virtual networks: “bridged” and “routed”. The virtual network model is composed of three layers: routing layers, firewall, and shared networks, which can prevent VMs from sniffing and spoofing. An evaluation of this approach was not performed when this publication was published.

Furthermore, web services are the largest implementation technology in cloud environments. However, web services also lead to several challenges that need to be addressed. Security web services standards describe how to secure communication between applications through integrity, confidentiality, authentication and authorization. There are several security standard specifications [79] such as Security Assertion Markup Language (SAML), WS-Security, Extensible Access Control Markup (XACML), XML Digital Signature, XML Encryption, Key Management Specification (XKMS), WS-Federation, WS-Secure Conversation, WS-Security Policy and WS-Trust. The NIST Cloud Computing Standards Roadmap Working Group has gathered high level standards that are relevant for Cloud Computing.

3 3 Conclusions

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some attacks especially when communicating with remote virtual machines.

Some surveys have discussed security issues about clouds without making any difference between vulnerabilities and threats. We have focused on this distinction, where we consider important to understand these issues. Enumerating these security issues was not enough; that is why we made a relationship between threats and vulnerabilities, so we can identify what vulnerabilities contribute to the execution of these threats and make the system more robust. Also, some current solutions were listed in order to mitigate these threats. However, new security techniques are needed as well as redesigned traditional solutions that can work with cloud architectures. Traditional security mechanisms may not work well in cloud environments because it is a complex architecture that is composed of a combination of different technologies.

We have expressed three of the items in Table 4 as misuse patterns [46]. We intend to complete all the others in the future.

Acknowledgments

This work was supported in part by the NSF (grants OISE-0730065). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect those of the NSF. We also want to thank the GSyA Research Group at the University of Castilla-La Mancha, in Ciudad Real, Spain for collaborating with us in this project.

Competing Interests

The authors declare that they have no competing interests.

Authors' contributions

KH, DGR, EFM and EBF made a substantial contribution to the systematic review, security analysis of Cloud Computing, and revised the final manuscript version. They all approved the final version to be published.

References

1. 1.

   Gartner Inc: *Gartner identifies the Top 10 strategic technologies for 2011*. Online. Available: http://www.gartner.com/it/page.jsp?id=1454221. Accessed: 15-Jul-2011.

2. 2.

   Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N: **Cloud Computing: A Statistics Aspect of Users.** In *First International Conference on Cloud Computing (CloudCom), Beijing, China*. Heidelberg: Springer Berlin; 2009:347–358. CrossRef

3. 3.

   Zhang S, Zhang S, Chen X, Huo X: **Cloud Computing Research and Development Trend.** In *Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China*. Washington, DC, USA: IEEE Computer Society; 2010:93–97. CrossRef

4. 4.

   Cloud Security Alliance: *Security guidance for critical areas of focus in Cloud Computing V3.0.*. 2011. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

5. 5.

Marinos A, Briscoe G: **Community Cloud Computing.** In *1st International Conference on Cloud Computing (CloudCom), Beijing, China*. Heidelberg: Springer-Verlag Berlin; 2009.

6. 6.

Centre for the Protection of National Infrastructure: *Information Security Briefing 01/2010 Cloud Computing*. 2010. Available: http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf

7. 7.

Khalid A: **Cloud Computing: applying issues in Small Business.** *International Conference on Signal Acquisition and Processing (ICSAP'10)* 2010, 278–281.CrossRef

8. 8.

KPMG: *From hype to future: KPMG's 2010 Cloud Computing survey.*. 2010. Available: http://www.techrepublic.com/whitepapers/from-hype-to-future-kpmgs-2010-clou%20d-computing-survey/2384291

9. 9.

Rosado DG, Gómez R, Mellado D, Fernández-Medina E: **Security analysis in the migration to cloud environments.** *Future Internet* 2012,**4**(2):469–487.CrossRef

10. 10.

Mather T, Kumaraswamy S, Latif S: *Cloud Security and Privacy*. Sebastopol, CA: O'Reilly Media, Inc.; 2009.

11. 11.

Li W, Ping L: **Trust model to enhance Security and interoperability of Cloud environment.** In *Proceedings of the 1st International conference on Cloud Computing*. Beijing, China: Springer Berlin Heidelberg; 2009:69–79.

12. 12.

Rittinghouse JW, Ransome JF: **Security in the Cloud.** In *Cloud Computing*. Implementation, Management, and Security, CRC Press; 2009.

13. 13.

Kitchenham B: *Procedures for perfoming systematic review, software engineering group*. Australia: Department of Computer Scinece Keele University, United Kingdom and Empirical Software Engineering, National ICT Australia Ltd; 2004. TR/SE-0401

14. 14.

Kitchenham B, Charters S: *Guidelines for performing systematic literature reviews in software engineering. Version 2.3 University of keele (software engineering group, school of computer science and mathematics) and Durham*. UK: Department of Conputer Science; 2007.

15. 15.

Brereton P, Kitchenham BA, Budgen D, Turner M, Khalil M: **Lessons from applying the systematic literature review process within the software engineering domain.** *J Syst Softw* 2007, **80**(4):571 - 583. CrossRef

16. 16.

Cloud Security Alliance: *Top Threats to Cloud Computing V1.0*. 2010. Available: https://cloudsecurityalliance.org/research/top-threats

17. 17.

ENISA: *Cloud Computing: benefits, risks and recommendations for information Security*. 2009. Available: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

18. 18.

Dahbur K, Mohammad B, Tarakji AB: **A survey of risks, threats and vulnerabilities in Cloud Computing.** In *Proceedings of the 2011 International conference on intelligent semantic Web-services and applications*. Jordan: Amman; 2011:1 - 6. CrossRef

19. 19.

Ertaul L, Singhal S, Gökay S: **Security challenges in Cloud Computing.** In *Proceedings of the 2010 International conference on Security and Management SAM'10*. Las Vegas, US: CSREA Press; 2010:36 - 42.

20. 20.

Grobauer B, Walloschek T, Stocker E: **Understanding Cloud Computing vulnerabilities.** *IEEE Security Privacy* 2011, **9**(2):50 - 57. CrossRef

21. 21.

Subashini S, Kavitha V: **A survey on Security issues in service delivery models of Cloud Computing.** *J Netw Comput Appl* 2011, **34**(1):1 - 11. CrossRef

22. 22.

Jensen M, Schwenk J, Gruschka N, Iacono LL: **On technical Security issues in Cloud Computing.** In *IEEE International conference on Cloud Computing (CLOUD'09)*. 116: 116; 2009:109 - 116. CrossRef

23. 23.

Onwubiko C: **Security issues to Cloud Computing.** In *Cloud Computing: principles, systems & applications*. Edited by: Antonopoulos N, Gillam L. Springer-Verlag: 2010; 2010.

24. 24.

Morsy MA, Grundy J, Müller I: **An analysis of the Cloud Computing Security problem.** In *Proceedings of APSEC 2010 Cloud Workshop*. Sydney, Australia: APSEC; 2010.

25. 25.

Jansen WA: **Cloud Hooks: Security and Privacy Issues in Cloud Computing.** In *Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa, Kauai, HI*. Washington, DC, USA: IEEE Computer Society; 2011:1 - 10.

26. 26.

Zissis D, Lekkas D: **Addressing Cloud Computing Security issues.** *Futur Gener Comput Syst* 2012,**28**(3):583 – 592.CrossRef

27.27.

Jansen W, Grance T: *Guidelines on Security and privacy in public Cloud Computing*. Gaithersburg, MD: NIST, Special Publication 800 – 144; 2011.

28.28.

Mell P, Grance T: *The NIST definition of Cloud Computing*. Gaithersburg, MD: NIST, Special Publication 800 – 145; 2011.

29.29.

Zhang Q, Cheng L, Boutaba R: **Cloud Computing: state-of-the-art and research challenges.** *Journal of Internet Services Applications* 2010,**1**(1):7 – 18.CrossRef

30.30.

Ju J, Wang Y, Fu J, Wu J, Lin Z: **Research on Key Technology in SaaS.** In *International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), Hangzhou, China*. Washington, DC, USA: IEEE Computer Society; 2010:384 – 387.

31.31.

Owens D: **Securing elasticity in the Cloud.** *Commun ACM* 2010,**53**(6):46 – 51.CrossRef

32.32.

OWASP: *The Ten most critical Web application Security risks*. 2010. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

33.33.

Zhang Y, Liu S, Meng X: **Towards high level SaaS maturity model: methods and case study.** In *Services Computing conference*. IEEE Asia-Pacific: APSCC; 2009:273 – 278.

34.34.

Chong F, Carraro G, Wolter R: *Multi-tenant data architecture*. 2006. Online. Available: http://msdn.microsoft.com/en-us/library/aa479086.aspx. Accessed: 05-Jun-2011

35. 35.

Bezemer C-P, Zaidman A: **Multi-tenant SaaS applications: maintenance dream or nightmare?** In *Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE), Antwerp, Belgium*. NY, USA: ACM New York; 2010:88 – 92.CrossRef

36. 36.

Viega J: **Cloud Computing and the common Man.** *Computer* 2009,**42**(8):106 – 108.CrossRef

37. 37.

Cloud Security Alliance: *Security guidance for critical areas of Mobile Computing*. 2012. Available: https://downloads.cloudsecurityalliance.org%20/initiatives/mobile/Mobile_Guidance_v1.pdf

38. 38.

Keene C: *The Keene View on Cloud Computing*. 2009. Online. Available: http://www.keeneview.com/2009/03/what-is-platform-as-service-paas.html. Accessed: 16-Jul-2011

39. 39.

Xu K, Zhang X, Song M, Song J: **Mobile Mashup: Architecture, Challenges and Suggestions.** In *International Conference on Management and Service Science. MASS' 09*. Washington, DC, USA: IEEE Computer Society; 2009:1 – 4.CrossRef

40. 40.

Chandramouli R, Mell P: **State of Security readiness.** *Crossroads* 2010,**16**(3):23 – 25.

41. 41.

Jaeger T, Schiffman J: **Outlook: cloudy with a chance of Security challenges and improvements.** *IEEE Security Privacy* 2010,**8**(1):77 – 80.CrossRef

42. 42.

Dawoud W, Takouna I, Meinel C: **Infrastructure as a service security: Challenges and solutions.** In *the 7th International Conference on Informatics and Systems (INFOS), Potsdam, Germany*. Washington, DC, USA: IEEE Computer Society; 2010:1 – 8.

43. 43.

Jasti A, Shah P, Nagaraj R, Pendse R: **Security in multi-tenancy cloud.** In *IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA*. Washington, DC, USA: IEEE Computer Society; 2010:35 – 41.

44. 44.

Garfinkel T, Rosenblum M: **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. volume 10*. CA, USA: USENIX Association Berkeley; 2005:227 – 229.

45. 45.

Reuben JS: *A survey on virtual machine Security*. Seminar on Network Security; 2007. http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf. Technical report, Helsinki University of Technology, October 2007

46. 46.

Hashizume K, Yoshioka N, Fernandez EB: **Three misuse patterns for Cloud Computing.** In *Security engineering for Cloud Computing: approaches and Tools*. Edited by: Rosado DG, Mellado D, Fernandez-Medina E, Piattini M. Pennsylvania, United States: IGI Global; 2013:36 – 53.

47. 47.

Venkatesha S, Sadhu S, Kintali S: *Survey of virtual machine migration techniques*. Technical report, Dept. of Computer

Science, University of California, Santa Barbara: ; 2009. http://www.academia.edu/760613/Survey_of_Virtual_Machine_Migration_Techniques

48. 48.

Ranjith P, Chandran P, Kaleeswaran S: **On covert channels between virtual machines.** *Journal in Computer Virology Springer* 2012, **8**:85 – 97. CrossRef

49. 49.

Wei J, Zhang X, Ammons G, Bala V, Ning P: **Managing Security of virtual machine images in a Cloud environment.** In *Proceedings of the 2009 ACM workshop on Cloud Computing Security*. NY, USA: ACM New York; 2009:91 – 96. CrossRef

50. 50.

Owens K: *Securing virtual compute infrastructure in the Cloud*. SAVVIS; Available: http:// www.savvis.com/en-us/info_center/documents/ hos-whitepaper-securingvirutalcompu%20teinfrastructureinthecloud.pdf

51. 51.

Wu H, Ding Y, Winer C, Yao L: **Network Security for virtual machine in Cloud Computing.** In *5th International conference on computer sciences and convergence information technology (ICCIT)*. DC, USA: IEEE Computer Society Washington; 2010:18 – 21.

52. 52.

Xiaopeng G, Sumei W, Xianqin C: **VNSS: a Network Security sandbox for virtual Computing environment.** In *IEEE youth conference on information Computing and telecommunications (YC-ICT)*. Washington DC, USA: IEEE Computer Society; 2010:395 – 398. CrossRef

53. 53.

Popovic K, Hocenski Z: **Cloud Computing Security issues and challenges.** In *Proceedings of the 33rd International convention MIPRO*. IEEE Computer Society Washington DC, USA; 2010:344 – 349.

54. 54.

Carlin S, Curran K: **Cloud Computing Security.** *International Journal of Ambient Computing and Intelligence* 2011, **3**(1):38 - 46. CrossRef

55. 55.

Bisong A, Rahman S: **An overview of the Security concerns in Enterprise Cloud Computing.** *International Journal of Network Security & Its Applications (IJNSA)* 2011, **3**(1):30 - 45. CrossRef

56. 56.

Townsend M: **Managing a security program in a cloud computing environment.** In *Information Security Curriculum Development Conference, Kennesaw, Georgia*. NY, USA: ACM New York; 2009:128 - 133.

57. 57.

Winkler V: *Securing the Cloud: Cloud computer Security techniques and tactics*. Waltham, MA: Elsevier Inc; 2011.

58. 58.

Ristenpart T, Tromer E, Shacham H, Savage S: **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, Illinois, USA*. NY, USA: ACM New York; 2009:199 - 212. CrossRef

59. 59.

Zhang Y, Juels A, Reiter MK, Ristenpart T: **Cross-VM side channels and their use to extract private keys.** In *Proceedings of the 2012 ACM conference on Computer and communications security, New York, NY, USA*. NY, USA: ACM New York; 2012:305 - 316. CrossRef

60. 60.

Wang Z, Jiang X: **HyperSafe: a lightweight approach to provide lifetime hypervisor control-flow integrity.** In *Proceedings of the IEEE symposium on Security and privacy*. Washington, DC, USA: IEEE Computer Society; 2010:380 - 395.

61. 61.

Wang C, Wang Q, Ren K, Lou W: **Ensuring data Storage Security in Cloud Computing.** In *The 17th International workshop on quality of service*. Washington, DC, USA: IEEE Computer Society; 2009:1 – 9.

62. 62.

Fernandez EB, Yoshioka N, Washizaki H: **Modeling Misuse Patterns.** In *Proceedings of the 4th Int. Workshop on Dependability Aspects of Data Warehousing and Mining Applications (DAWAM 2009), in conjunction with the 4th Int.Conf. on Availability, Reliability, and Security (ARES 2009), Fukuoka, Japan*. Washington, DC, USA: IEEE Computer Society; 2009:566 – 571.

63. 63.

Santos N, Gummadi KP, Rodrigues R: **Towards Trusted Cloud Computing.** In *Proceedings of the 2009 conference on Hot topics in cloud computing, San Diego, California*. CA, USA: USENIX Association Berkeley; 2009.

64. 64.

Zhang F, Huang Y, Wang H, Chen H, Zang B: **PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection.** In *Trusted Infrastructure Technologies Conference, 2008. APTC' 08, Third Asia-Pacific*. Washington, DC, USA: IEEE Computer Society; 2008:9 – 18.CrossRef

65. 65.

Cloud Security Alliance: *SecaaS implementation guidance, category 1: identity and Access managament*. 2012. Available: https://downloads.cloudsecurityalliance.org%20/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Gui%20dance.pdf

66. 66.

Xiao S, Gong W: **Mobility Can help: protect user identity with dynamic credential.** In *Eleventh International conference on Mobile data Management (MDM)*. Washington, DC, USA: IEEE Computer Society; 2010:378 – 380.CrossRef

67. 67.

Wylie J, Bakkaloglu M, Pandurangan V, Bigrigg M, Oguz S, Tew K, Williams C, Ganger G, Khosla P: *Selecting the right data distribution scheme for a survivable Storage system*. Pittsburgh, PA: CMU-CS-01－120; 2001.

68. 68.

Somani U, Lakhani K, Mundra M: **Implementing digital signature with RSA encryption algorithm to enhance the data Security of Cloud in Cloud Computing.** In *1st International conference on parallel distributed and grid Computing (PDGC)*. IEEE Computer Society Washington, DC, USA; 2010:211－216.

69. 69.

Harnik D, Pinkas B, Shulman-Peleg A: **Side channels in Cloud services: deduplication in Cloud Storage.** *IEEE Security Privacy* 2010, **8**(6):40－47. CrossRef

70. 70.

Tebaa M, El Hajji S, El Ghazi A: **Homomorphic encryption method applied to Cloud Computing.** In *National Days of Network Security and Systems (JNS2)*. Washington, DC, USA: IEEE Computer Society; 2012:86－89.

71. 71.

Fong E, Okun V: **Web application scanners: definitions and functions.** In *Proceedings of the 40th annual Hawaii International conference on system sciences*. Washington, DC, USA: IEEE Computer Society; 2007.

72. 72.

Goodin D: *Webhost hack wipes out data for 100,000 sites*. 2009. *The Register*, 08-Jun-2009. [Online]. Available: http://www.theregister.co.uk/2009/06/08/webhost_attack/. Accessed: 02-Aug-2011

73. 73.

Berger S, Cáceres R, Pendarakis D, Sailer R, Valdez E, Perez R, Schildhauer W, Srinivasan D: **TVDc: managing Security in the**

trusted virtual datacenter. *SIGOPS Oper. Syst. Rev.* 2008,**42**(1):40 – 47.CrossRef

74. 74.

Berger S, Cáceres R, Goldman K, Pendarakis D, Perez R, Rao JR, Rom E, Sailer R, Schildhauer W, Srinivasan D, Tal S, Valdez E: **Security for the Cloud infrastructure: trusted virtual data center implementation.** *IBM J Res Dev* 2009,**53**(4):560 – 571.CrossRef

75. 75.

Ormandy T: **An empirical study into the Security exposure to hosts of hostile virtualized environments.** In *CanSecWest applied Security conference*. Vancouver; 2007. http://taviso.decsystem.org/virtsec.pdf

76. 76.

Oberheide J, Cooke E, Jahanian F: **Empirical exploitation of Live virtual machine migration.** *Proceedings of Black Hat Security Conference, Washington, DC* 2008. http://www.eecs.umich.edu/fjgroup/pubs/blackhat08-migration.pdf

77. 77.

Naehrig M, Lauter K, Vaikuntanathan V: **Can homomorphic encryption be practical?** In *Proceedings of the 3rd ACM workshop on Cloud Computing Security workshop*. NY, USA: ACM New York; 2011:113 – 124.CrossRef

78. 78.

Han-zhang W, Liu-sheng H: **An improved trusted cloud computing platform model based on DAA and privacy CA scheme.** In *International Conference on Computer Application and System Modeling (ICCASM), vol. 13, V13 – 39*. Washington, DC, USA: IEEE Computer, Society; 2010:V13 – 33.

79. 79.

Fernandez EB, Ajaj O, Buckley I, Delessy-Gassant N, Hashizume K, Larrondo-Petrie MM: **A survey of patterns for Web services**

Security and reliability standards. *Future Internet* 2012, **4**(2):430 - 450. CrossRef