Cyber-storms come from clouds

Security of cloud computing in the IoT era

De Donno, Michele; Giaretta, Alberto; Dragoni, Nicola; Bucchiarone, Antonio; Mazzara, Manuel

Published in:
Future Internet

Link to article, DOI:
10.3390/fi11060127

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

Citation (APA):
De Donno, M., Giaretta, A., Dragoni, N., Bucchiarone, A., & Mazzara, M. (2019). Cyber-storms come from clouds: Security of cloud computing in the IoT era. *Future Internet*, *11*(6), [127]. https://doi.org/10.3390/fi11060127

future internet

MDPI

Article

Cyber-Storms Come from Clouds: Security of Cloud Computing in the IoT Era

Michele De Donno [1], Alberto Giaretta [2], Nicola Dragoni [1,2] and Antonio Bucchiarone [3,*] and Manuel Mazzara [4,*]

[1] DTU Compute, Technical University of Denmark, 2800 Kongens Lyngby, Denmark; mido@dtu.dk (M.D.D.); ndra@dtu.dk (N.D.)

[2] Centre for Applied Autonomous Sensor Systems Orebro University, 701 82 Orebro, Sweden; alberto.giaretta@oru.se

[3] Fondazione Bruno Kessler, Via Sommarive 18, 38123 Trento, Italy

[4] Institute of Software Development and Engineering, Innopolis University, Universitetskaya St, 1, 420500 Innopolis, Russian Federation

* Correspondence: bucchiarone@fbk.eu (A.B.); m.mazzara@innopolis.ru (M.M.)

Received: 28 January 2019; Accepted: 30 May 2019; Published: 4 June 2019

Abstract: The Internet of Things (IoT) is rapidly changing our society to a world where every "thing" is connected to the Internet, making computing pervasive like never before. This tsunami of connectivity and data collection relies more and more on the Cloud, where data analytics and intelligence actually reside. Cloud computing has indeed revolutionized the way computational resources and services can be used and accessed, implementing the concept of utility computing whose advantages are undeniable for every business. However, despite the benefits in terms of flexibility, economic savings, and support of new services, its widespread adoption is hindered by the security issues arising with its usage. From a security perspective, the technological revolution introduced by IoT and Cloud computing can represent a disaster, as each object might become inherently remotely hackable and, as a consequence, controllable by malicious actors. While the literature mostly focuses on the security of IoT and Cloud computing as separate entities, in this article we provide an up-to-date and well-structured survey of the security issues of cloud computing in the IoT era. We give a clear picture of where security issues occur and what their potential impact is. As a result, we claim that it is not enough to secure IoT devices, as cyber-storms come from Clouds.

Keywords: security; Internet of Things; Cloud computing

1. Introduction

The Internet of Things (IoT) is rapidly and inevitably spreading in our society, with the promise of rising efficiency and connectivity. Although the number of "things" has strongly been increasing over the past few years, statistics predict an even further growth in the future. Indeed, if the number of IoT connected devices in 2017 was around 20 billion, there will be about 30 billion in 2020 and more than double in 2025 [1]. This dramatic increase will bring challenges together with opportunities, and the massive introduction of this technology will need to be managed by several points of views such as legal, social, business-wise and of course technological [2].

IoT applications span from industrial automation to home area networks to smart buildings, pervasive healthcare and smart transportation [3–5]. For instance, smart homes will heavily rely upon IoT devices to monitor the house temperature, possible gas leakages, malicious intrusions, and several other parameters concerning the house and its inhabitants. In pervasive healthcare, IoT devices are used to perform continuous biological monitoring, drug administration, elderly monitoring conditions and habits for an improved lifestyle, and so on. Last but not least, with the Industry 4.0 technological revolution, Industrial IoT (IIoT) is entering its golden age.

From a security perspective, this plethora of IoT devices flooding the world is having tremendous consequences, so that it is not an exaggeration to talk about a security and privacy disaster [6]. In fact, IoT devices are often bad or not protected at all, thus, easily exploitable from different families of malware to perpetrate large scale attacks (this is the case of Distributed Denial of Service-Capable IoT malwares such as Mirai [7,8], just to mention a key example).

If we refer to one of the most common definitions of IoT, we can see that it is based on a single layer of devices with embedded computation and connectivity: "the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data" [9]. This definition depicts the traditional scenario which most of the literature about IoT security focuses on ([10–12], just to mention a few papers). Nevertheless, focusing only on the security of end devices risks to make us lose the sight of the overall picture.

Today, IoT systems strongly rely on the Cloud. End devices are increasingly used as lightweight devices that collect data and connect to powerful Cloud servers responsible for all the application intelligence and data analytics [13–15]. This huge amount of data sent to the Cloud is one of the main motivations for the investigation of new distributed computing paradigms, such as Fog Computing [16].

For this reason, we think that it is no longer enough to consider Cloud computing and IoT as two different entities, but we need to change the perspective, especially when looking at how to protect IoT systems. Similarly to other works in the literature, such as [17–20], we assume a picture of IoT in which Cloud computing and end devices are the two tight layers constituting a broader Internet of Things. In this new setting, IoT cannot disregard Cloud computing, as the Cloud is a core component of the overall IoT architecture, rather than an external entity. Note that the viceversa is not true, as the Cloud was not originally thought for IoT devices and it has been widely studied as a stand-alone paradigm.

From a security perspective, this vision of Cloud computing as a key component of the IoT architecture implies that all security issues that the Cloud drags on need to be analyzed and addressed when referring to IoT security. The result, depicted in Figure 1, is a metaphoric rainstorm of cyber-security issues potentially affecting every context of the current and future society. For this reason, we strongly believe that a clear and detailed analysis of the security issues of the "clouds" is essential to improve the security on the "ground".

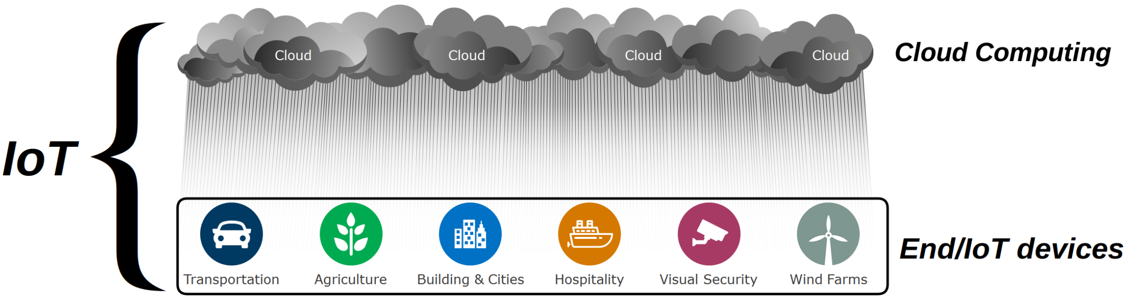

Figure 1. A broader definition of IoT (adapted from [21]): a two layered architecture in which End/IoT devices strongly rely on the Cloud.

Contribution and Outline of the Paper

This paper aims at providing an up-to-date and well-structured survey of the security issues of Cloud computing in the era of the IoT revolution. Hence, we do not aim at proposing yet another survey of security issues of Cloud computing as a stand-alone paradigm, but we aim at discussing security issues of the Cloud when considered as a core component of the broader IoT architecture. For this purpose, we use a structured approach. First, we distinguish security issues specific of Cloud computing from issues not strictly related to the Cloud but still having an impact on the overall IoT architecture (depicted in Figure 1). Then, we classify both types of issues according to two different angles: the affected Cloud architectural layer and the impacted security property (in terms of confidentiality, integrity, availability). We believe that this classification is vital to understand security issues of Cloud computing, having a clear picture of where issues occur and what their potential impact is. Since there is no IoT without Cloud, we cannot secure IoT without securing the Cloud.

In summary, the contribution of the paper is twofold:

- We provide a novel Cloud-centered perspective of IoT security. As already mentioned, Cloud computing has become of paramount importance for Internet of Things. Nevertheless, most of the works related to IoT security focus on the security of end devices. In this paper, we fill this gap providing an analysis of Cloud security issues and how they affect IoT security.
- We propose and discuss a structured classification of Cloud computing security issues: differently from other works, security issues associated with Cloud computing will be classified according to different layers. First, we distinguish between Cloud-specific security issues and other issues non strictly related to the Cloud but still important in the IoT context. Then, for each layer of the Cloud architecture, we investigate security properties affected by each issue. This contribution aims at giving a clear overall picture of all aspects of Cloud security.

Outline of the Paper. The rest of this work is organized as follows. Section 2 reviews similar efforts and compares them with the rationale behind our manuscript. Section 3 gives basic notions on Cloud computing. Section 4 describes the methodology adopted in our research, which is of key importance in order to understand the classification proposed in the paper. In particular, it first depicts the assumed reference architecture. Then, it explains how the classification has been structured. Sections 5 and 6 discuss the Cloud-specific security issues and the generic security issues, respectively. Finally, Section 8 wraps up and concludes the work.

2. Related Work

In this section, we review relevant works related to our research and we discuss how our contribution extends and complements the literature.

Various research groups focused on identifying security and privacy challenges in Cloud computing, such as Liu et al. [22], Shazhad [23], and Ryan [24], to name a few. In particular, Ryan [24] sums up three key directions to strengthen confidentiality: homomorphic encryption, key translation within-browser, and hardware-anchored security.

Subashini and Kavitha [25] group security issues in relation to the service model they affect, having a focus on the Software as a Service (SaaS) one. For each service model, the authors report different categories of security issues without clear classification criteria. The result is a mixture of categories often overlapped with each other. We claim that this lack of separation between classes, along with the intrinsic complexity of the Cloud, does not allow the reader to develop a clear picture of where issues occur within the Cloud architecture and what security property they affect.

Grobauer et al. [26] are the first authors proposing a differentiation between general security issues and Cloud specific ones. They focus on Cloud-specific issues and classify them in relation to the architectural level they occur. However, no focus is placed on the security property each issue affects.

Similarly, Modi et al. [27] classify security issues based on a Cloud architecture that is alike to the one used in this paper. However, they do not specify which security property is affected by each issue.

Singh et al. [28] group security issues in relation to different categories whose choice is unclear. This makes difficult for the reader to understand how the different categories are related and consequently it complicates the comprehension of security issues. However, some of the identified threats are contextualized with the security attribute they compromise.

Fernandes et al. [29] produced one of the most comprehensive surveys on Cloud computing security issues. They identify a large number of security issues and group them based on a taxonomy that is clearly defined. Nevertheless, they do not specify which security property is affected by each issue. A lot of different researchers proposed taxonomies, and Polash et al. conducted a survey that recollects many of them [30].

Singh and Chatterjee [31] extend the work of Fernandes et al. to include possible solutions to the identified problems, while Xiao and Xiao [32] propose to classify security issues in relation to the properties they affect. However, they identify only a small subset of threats, together with a list of possible solutions.

Instead of classifying Cloud security issues at a fine-grained level, Ardagna et al. [33] choose to classify literature works in relation to the security property affected by the issues considered in such works. However, this coarse-grained approach does not allow to achieve the desired level of detail. Indeed, since many of the classified works do not specify the impact of each issue, the approach used by Ardagna et al. [33] does not help the understanding of what security property is affected by each security issue.

Hashizume et al. [34] present a categorization of security issues focusing on a service model perspective while distinguishing between threats and vulnerabilities.

To the best of our knowledge, there is no work in the literature proposing a structured classification of Cloud computing security issues in the IoT context.

3. Background: Cloud Computing Paradigm

Nowadays, Cloud computing is a well-known paradigm. However, for the sake of readability and self-containment of the paper, we consider relevant to recap basic notions of Cloud computing. This also allows us to define a common terminology that is going to be used throughout the rest of this paper. For these reasons, background notions about Cloud computing are provided in this section.

NIST [35] defines Cloud computing as "a model for enabling 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".

Figure 2 depicts the NIST Cloud computing reference architecture [36]. It provides a high-level overview of the Cloud and identifies the main actors and their role in Cloud computing. Each actor is an entity, i.e., a person or an organization, that either takes part in a transaction/process or performs some tasks in Cloud computing. There are five main actors:

- *Cloud Provider*: an entity that provides a service to interested parties;
- *Cloud Consumer*: an entity that uses a service from, and has a business relationship with, one or more *Cloud providers*;
- *Cloud Broker*: an entity that mediates affairs between *Cloud providers* and *Cloud consumers*, and that manages the use, performance, and delivery of Cloud services;
- *Cloud Carrier*: an intermediary that supplies connectivity and delivery of Cloud services from *Cloud providers* to *Cloud consumers*;
- *Cloud Auditor*: a party that conducts independent assessments of the Cloud infrastructure, including services, information systems operations, performances, and security of the Cloud implementation.

In terms of interactions, there are several possible scenarios [36]. Generally, a Cloud consumer may request a Cloud service from a Cloud provider, either directly or via a Cloud broker. A Cloud auditor conducts independent audits and may contact other actors to collect the necessary information.

The NIST defines the Cloud by means of five essential characteristics, three service models, and four deployment models [35].

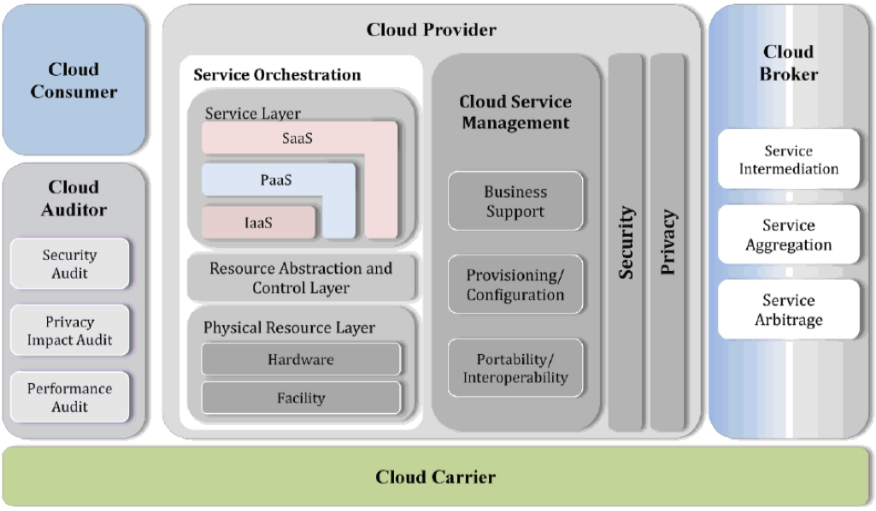

Figure 2. NIST Cloud computing reference architecture (source [36]).

3.1. Essential Characteristics

The essential characteristics of Cloud computing can be summarized as follows [35]:

- *On-demand self-service*: computing capabilities can be provided automatically when needed, without requiring any human interaction between consumer and service provider;
- *Broad network access*: computing capabilities are available over the network and accessible through several mechanisms which are disposable for a wide range of client platforms (e.g., workstations, laptops, and mobile devices);
- *Resource pooling*: computing resources are pooled to accommodate multiple consumers, dynamically allocating and deallocating them according to consumer demand. In addition, the provider resources are location independent, i.e., the consumer does not have any knowledge or control of their exact location;
- *Rapid elasticity*: computing capabilities can flexibly be provided and released to scale in and out according to the demand. As a result, the consumer has the perception of unlimited, and always adequate, computing capabilities;
- *Measured service*: resource usage can be monitored and reported according to the type of service offered. This is particularly relevant in charge-per-use, or pay-per-user, services because it grants great transparency between the provider and the consumer of the service.

A *Cloud infrastructure* is a collection of hardware and software that empowers the aforementioned essential characteristics of Cloud computing.

3.2. Service Models

The three main types of service models used in Cloud computing are described below [35]:

- *Infrastructure as a Service* (IaaS*)*: processing, storage, networks, and other fundamental computing resources (both software and hardware) are provided to the consumer. The consumer can run and deploy any software and can control operating systems, storage, and deployed applications. The consumer does not control or manage the underlying Cloud infrastructure;
- *Platform as a Service* (PaaS*)*: the consumer is provided with a whole development stack that can be used to develop and deploy new applications. The development stack includes programming languages, libraries, services, and tools that are supported by the provider. The consumer controls both deployed applications and possible configuration settings for the applications environment. The consumer does not control or manage the underlying Cloud infrastructure, operating systems, and storage;

- *Software as a Service (*SaaS*)*: the consumer can use the applications offered by the provider, running on the Cloud infrastructure. The consumer does not control or manage the underlying Cloud infrastructure, operating systems, storage, and individual applications capabilities.

In all the service models, Cloud provider and Cloud consumer share the control of the Cloud system. However, as shown in Figure 3, each service model implies a different degree of control over the computational resources for each party, thus different responsibilities [36].

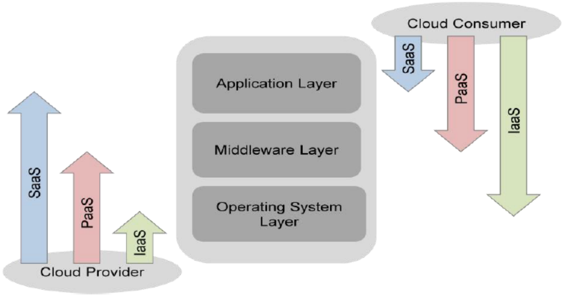

Figure 3. Scope of control between provider and consumer (source [36]).

3.3. Deployment Models

The four main models used for the deployment of Cloud computing are discussed below [35]:

- *Private Cloud*: the Cloud infrastructure is provided for the exclusive use of a single organization. The organization can include different consumers (e.g., business units);
- *Community Cloud*: the Cloud infrastructure is provisioned for the exclusive use of organizations with shared concerns, such as security requirements, policy, and mission. Each organization can include multiple consumers;
- *Public Cloud*: the Cloud infrastructure is provided for open use by the general public over the Internet. It is ideal either for small to medium size businesses, or for single customers;
- *Hybrid Cloud*: the Cloud infrastructure is a combination of two or more infrastructures deployed with different models (private, community, or public). Each Cloud infrastructure remains a unique entity, but it is bound together with the others by standardized or proprietary technologies enabling portability.

In all the aforementioned models, the Cloud infrastructure may be owned, managed, and operated by one or more consumer organizations (if any), a third party organization (e.g., business organization, academic organization, or government organization), or any combination of them.

4. Methodology

In this section, we introduce the methodology adopted to classify security issues. First, we describe the simplified Cloud architecture that we use as a reference. Then, we explain how the classification is organized.

4.1. Reference Architecture

Cloud computing is one of the most complex computing paradigms existing today. For this reason, it is essential to take apart irrelevant details when it comes to classify its security issues. To reach this objective, we introduce a simplified architecture of the Cloud infrastructure, which is depicted in Figure 4. This architecture is an abstraction of the architecture proposed in [27] and it is simplified to such an extent that Cloud computing is considered as composed of four main layers: *physical layer*, *virtualization layer*, *application layer*, and *data storage*.

The key components we consider at the physical layer are computational, storage, and networking resources. However, since security issues of physical resources are beyond the purposes of this work, at this layer we only consider *network security issues*.

In the virtualization layer, we locate Virtual Machines (VM), Virtual Machine Monitors (VMM), virtual networks, and all the infrastructure directly or indirectly supporting virtualization (e.g., mechanisms enabling virtual machine migration, management of VMs, and so on).

We consider all the remaining software as part of the application layer: specific applications, APIs, tools, middlewares, management services, monitoring systems, load balancing systems, and others. Further, all software (above the virtualization level) used to build PaaS and SaaS Cloud implementations is considered part of the application level. Hence, in this respect, we consider PaaS and SaaS as parts of the application level. Indeed, we see them just as any other application offering some special type of services.

Finally, we consider data storage services as part of all the layers of the architecture, therefore, they are treated alongside the other layers.

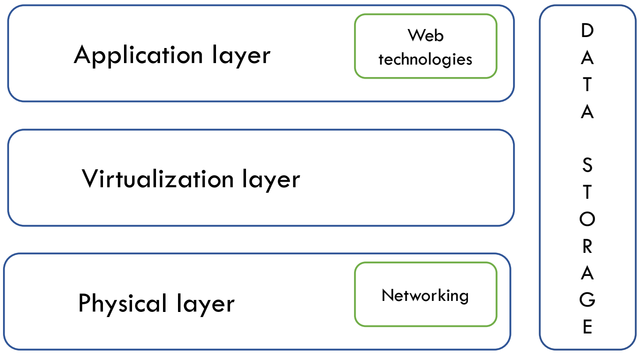

Figure 4. Simplified Cloud reference architecture.

4.2. Structured Classification

In this section, we describe how our reference architecture is adopted to classify Cloud security issues. The overall classification is depicted in Figure 5.

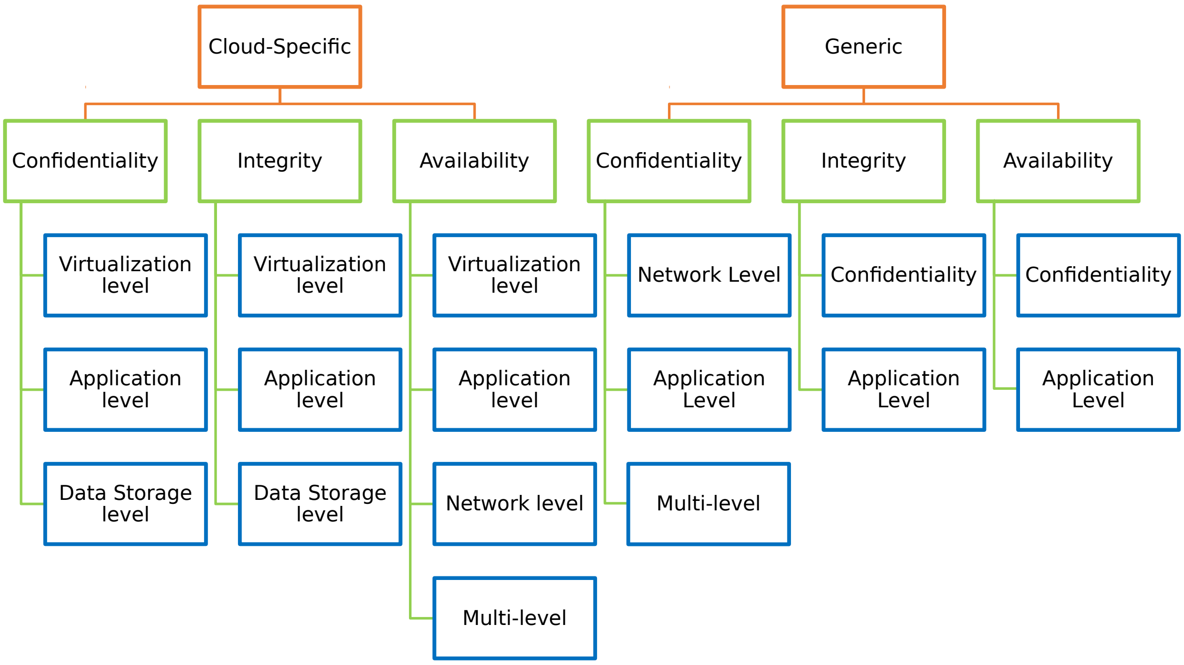

Figure 5. Classification of Cloud security issues.

Firstly, we separate Cloud-specific security issues from generic ones. Details about the criteria used for performing such distinction are provided in Section 5. In short, many security issues of the Cloud exist also in other paradigms, since rooted in common technologies employed to build distributed systems. Thus, we distinguish between issues that we consider specific of the Cloud environment and other common security issues not strictly related to the Cloud but still having an impact on the overall IoT architecture (depicted in Figure 1). However, even if we also present a subset of generic security issues, our main focus is on Cloud-specific ones.

Secondly, security issues are further classified from two different perspectives: the Cloud architectural level at which they occur and the security property they affect. In other words, given a certain level x of the Cloud reference architecture and a certain security property y, the following questions are answered: *(1) What are the security problems at level x of the Cloud architecture?*, *(2) How do they affect property y?* In answering these questions, the security properties we consider are the well-known confidentiality, integrity, and availability (CIA). We have decided to stick only with these security properties to keep the scope of the paper well focused and manageable in terms of literature and analysis. However, the same methodology can be applied to and iterated with other security properties (e.g., authenticity and accountability).

The classification resulting from the analysis described in Sections 5 and 6 is depicted at the end of the paper in Tables 1 and 2, respectively. These tables show each issue in relation to the architectural level it occurs and the CIA property it affects. For each cell of the table (associated with a specific pair: issue, security property) a mark is applied according to the following rules:

- "✓": it is placed if we found a literature work describing an attack affecting the corresponding security property, or if we found a literature work stating that the issue might affect the corresponding property;
- "∼": it is placed if, although the previous condition is not verified, we believe that the given issue might allow compromising the corresponding security property;
- an empty cell, if the previous conditions do not hold.

Moreover, in the last column of each table, we highlight the relationship between each security issue, the Cloud, and the IoT devices. In details, we indicate which party can be exploited because of the specific security issue, and which party might be the victim of an attack perpetrated exploiting that issue. If neither the Cloud nor IoT devices are involved, we draw a "-".

Table 1. Summary of Cloud-specific issues. "✓": existence of literature works indicating that the issue affects the property. "∼": despite we found no evidence in the literature, we believe that the issue might affect the property. EXPLOITED/VICTIM: how parties of the IoT architecture (Figure 1) are affected from the issue.

ARCHITECTURAL LEVEL	ISSUES	CONFIDENTIALITY	INTEGRITY	AVAILABILITY	EXPLOITED/VICTIM *(Cloud, IoT Devices, Both)*
Virtualization	Multi-tenancy	✓		✓	Cloud/IoT devices
	VM isolation	✓	✓	✓	Cloud/IoT devices
	Virtual network	✓	∼	✓	Both/Both
	VM introspection	✓			Cloud/IoT devices
	VM management	✓	✓	✓	Cloud/Both
	VM migration	✓	✓	✓	Both/IoT devices
Application	Isolation	✓	✓	∼	Cloud/IoT devices
	Synchronization mechanisms	✓	✓	∼	Both/IoT devices
	Insecure APIs, management and control interfaces	∼	✓	∼	Both/Both
	Resource accounting			✓	IoT devices/Cloud
Network	Network under-provision			✓	Both/Both
Data Storage	Outsourcing	✓	✓		Cloud/IoT devices
	Data deletion	✓			Cloud/IoT devices
Multi-level	Economic sustainability			✓	Both/IoT devices

Table 2. Summary of generic security issues. "✓": existence of literature works "∼": despite we found no evidence in the literature, we believe that the issue might affect the property. EXPLOITED/VICTIM: how parties of the IoT architecture (Figure 1) are affected from the issue.

ARCHITECTURAL LEVEL	ISSUES	CONFIDENTIALITY	INTEGRITY	AVAILABILITY	EXPLOITED/VICTIM *(Cloud, IoT Devices, Both)*
Network	Man In The Middle (MITM) attack	✓	✓	✓	Both/Both
	DDoS attack			✓	Both/Both
Application	Cross-site scripting (XSS) attack	✓	∼		Cloud/IoT devices
	Injection flaws	✓	✓	✓	Cloud/Both
	Man in the Browser (MitB) attack	✓	✓	∼	IoT devices/Both
	Cross-site request forgery (CSRF) attack	∼	✓		Cloud/IoT devices
	Hidden field manipulation and cookie poisoning	∼	✓		Cloud/IoT devices
	XML Signature Element Wrapping	∼	✓		Cloud/Both
	Metadata Spoofing attack	∼	✓	∼	Cloud/Both
	Application-bug level DoS attack			✓	Both/Both
	Flooding DoS attack			✓	Both/Both
Multi-level	Advanced Persistent threats	✓	∼	∼	Both/Both

5. Cloud-Specific Security Issues

In this section, we present security issues peculiar for Cloud computing. Inspired by the work in [26], we consider as Cloud-specific issues all those problems that are rooted in at least one of the essential Cloud characteristics defined by NIST and reported in Section 3. Please consider that, according to such definitions, network-level and web-technologies issues (discussed in Section 6) should be considered specific for the Cloud. However, since those security issues are also really common in a number of distributed paradigms, we have decided to consider them as generic security issues and to not discuss them in this section.

In the following, we present Cloud-specific security issues based on a two-layer classification. First, we classify security issues based on what CIA propriety they affect. Then, for each property, the issues are further organized in relation to the Cloud architectural level they affect.

5.1. Confidentiality

According to [37], confidentiality is the "property that information is not made available or disclosed to unauthorized individuals, entity or processes". Hence, it is the property indicating absence of unauthorized disclosure of information and data [38]. We present a classification of security issues that can impair data confidentiality. Each class of our classification is a component of the Cloud architecture (defined in Section 4.1) while the entries of each class are the security issues rooted in that specific level.

5.1.1. Virtualization Level Issues

Virtualization technology is one of the key enablers of Cloud computing. However, this additional abstraction layer has severe security repercussions. In the following paragraphs, we report key security issues caused by this layer and capable of compromising data confidentiality.

Multi-Tenancy Issues

Virtualization technology allows to develop a multi-tenant environment in which virtual machines operate sharing communal hardware resources. The placement of different users on the same platform is what enables new types of attacks on data confidentiality. In [39], the authors describe how they were able to exploit several characteristics of Amazon Elastic Compute Cloud (EC2) in such a way to have their own virtual machine co-resident (i.e. on the same physical machine) with that of a victim. Once co-residence is reached, an attacker has the unprecedented possibility of performing several types of side-channel attacks in such a way to extract confidential information from users who are sharing the same machine with the attacker. Consequently, through attacks struck to the Cloud, a malicious user could be capable to disrupt the confidentiality of IoT devices data, stored on the Cloud infrastructure. In [39], it is shown that, by means of cache measurements, an attacker can perform: keystroke timing attack, traffic rates estimation of victim's web servers and even co-residence detection.

Moreover, side-channel attacks affecting cryptographic implementations have been reported in [40–43]. The work in [44] shows the possibility to exploit memory deduplication issues for performing another type of cross-VM side channel attack. Furthermore, the recent vulnerabilities Meltdown [45] and Spectre [46] have demonstrated that not only memory-based side-channel attacks are possible, but that even processor vulnerabilities can be exploited to perform attacks capable of breaking any security assumption and allowing other co-resident VMs to access confidential information belonging to other users.

From the IoT devices' point of view, virtualization issues have a critical implication: security cannot be solely evaluated by looking at the characteristics of a single product. Even if we assume that an IoT device is bug-less on every layer (from the hardware layer to the Cloud APIs one), its data could be accessed by an attacker capable of trespassing isolation limits. Indeed, other services hosted on the same physical machine might exhibit exploitable vulnerabilities, which might allow the attacker to access to sections meant to be off-limits.

VM Isolation Issues

According to [28], virtual machine isolation is the principal factor that can lead to cross-VM data leakage. Virtualization is based on the hypervisor ability to isolate VMs from each other. However, due to several reasons (e.g., misconfiguration, design and implementation bugs), an attacker can compromise the hypervisor, evade from isolation and potentially take over all the other guests [47]. We refer to such a situation as virtual machine escape [48]. Escaped VMs can access data and information belonging to other VMs [49], resulting in paramount confidentiality issues. Appropriate security mechanisms are therefore required for isolating virtual machines from each other and hence preventing data leakage. Some possible techniques for isolation enforcement are described in [49], while in [48], techniques for providing integrity of VMs are reported. Issues at this level are similar to the ones described for the multi-tenancy section. An attacker can exploit the capability of positioning herself on the same machine of the target, and this capability enables both side-channel attacks and isolation evasion techniques that lead to leakage of IoT devices data.

Virtual Network Issues

According to [50,51], not only virtual machine isolation is needed but also isolation of virtual networks is required. Therefore, virtual networks are another source of vulnerability for confidentiality and, as such, need to be protected. Even though some traditional controls (such as virtual local area networks and firewalls) have been proven to be less effective in virtual networks [52], in [50], the authors propose to implement traditional network security solutions into virtual environments. Typical confidentiality threats that can affect virtual networks are sniffing and spoofing attacks [53]. Even though from a user's perspective a virtual network might look like a private one, in reality, it might rely on public infrastructure. Therefore, appropriate protections to secure communications are needed [54].

A novel type of attack that exploits virtual networks as a cornerstone for subsequently compromising the whole Cloud system is the "virtual switch attacker model for packet-parsing" (vAMP attack) [55]. This attack exploits vulnerabilities of specific packet parsing systems deployed in virtual switches for generating a series of attacks that eventually allow taking control of the entire Cloud system.

Virtual Machine Introspection Issues

Different literature works, such as [50,56,57], propose to use the hypervisor for monitoring virtual machines with the objective of preventing or discovering attacks on the integrity of guest systems. From the one hand, this kind of approach presents important advantages, on the other hand, it also highlights the possibility for the Cloud provider or malicious insiders (or even for an external attacker able to take control of the hosting platform) to break users' confidentiality by exploiting virtual machine introspection. This problem is linked to the more general and emblematic question of deciding whether the Cloud provider and the infrastructure it provides, should be considered trusted or not, a typical problem of every scenario in which outsourcing is present. It is worth noting that, in case the Cloud provider is considered trusted, the Cloud infrastructure might also play a key role in solving many of the existing security issues [58].

An example of attack that can allow a malicious insider to exploit virtual machine introspection is described in [59].

For the sake of completeness, it should also be mentioned that attacks targeting virtual machine introspection mechanisms have been reported in the literature. An example of such an attack is Direct Kernel Structure Manipulation (DKSM) [60].

VM Management Issues

VM image cloning enables Cloud providers to supply on-demand services to their clients. Cloned VMs can be moved on different servers in relation to clients' needs but this also makes clients unaware of how many VMs copies exist, where these are specifically located and who is possessing them. Such availability, allows a malicious insider to exploit one of the existing VM copies to attempt breaking the VM password and gain access to all the information saved into the VM [61] while leaving the owner unaware of such situation.

VM image sharing is another key service enabled by VM image cloning. VM image sharing is one of the Cloud foundations [62], however, both the VM image publisher and the retriever are subject to confidentiality concerns [63]. Indeed, by publishing an image, the publisher may release his own confidential information, while, on the other side, user's data confidentiality can be compromised by shared malicious images, for instance, they can contain backdoors for silently access confidential data [26,64]. Moreover, VM image sharing makes also possible for attackers to rent cloned VMs with the only purpose of analyzing their content and therefore to identify possible vulnerabilities that could be exploited in future attacks. Consequently, from the confidentiality point of view this can have a dangerous effect not only on Cloud providers that manage such VMs, but on the IoT end devices as well.

VM Migration Issues

Virtual Machine migration allows to transfer running VMs from one host to another in a transparent fashion for the final user [65,66]. The Cloud advantages of using such mechanisms are obvious, just to name a few: enables load-balance when hosts are overloaded, allows to reduce costs through VMs consolidation, and improves the overall manageability of the system [65–67]. However, protocols used in implementing live migration have to be secured: if control messages and migrating VMs are not encrypted, common attacks on confidentiality (such as passwords eavesdropping) might be easily performed [65,68].

5.1.2. Application Level Issues

We are now going to consider what are the Cloud issues for confidentiality whose causes are rooted at the application level. According to our reference architecture (defined in Section 4.1), every software deployed on top of the virtualization layer has been considered part of the application level. Since we consider PaaS and SaaS systems special types of application-level services, these are considered part of this level too. We remind to the reader that even if we consider web-related issues part of the application layer, they are not specifically related only to the Cloud but common of any distributed system and for this reason these are discussed in Section 6.

Isolation Issues

Users of PaaS systems can develop and run their own applications on platforms provided by Cloud providers. These platforms allow applications developed by different users to share communal libraries and supporting services [69]. Even if the platform (or container system) can be a proper Operating System, in most cases it is a Virtual Platform (e.g., Java or .Net) [69]. Irrespectively from the specific implementation, a common concern of PaaS systems is to ensure that isolation of tenants is properly implemented and that an application can not explore or modify other data and applications. The work in [69] presents a panoramic of isolation issues that could have arisen when Java or .Net technologies were used to create PaaS implementations. However, PaaS implementations vary deeply from provider to provider [70]. At this point, it should be noted that the isolation dangers at the application level are extremely similar to the ones at the virtualization layer, which we described in the previous section.

Within SaaS models, multitenancy is present also at the application level. In [51], the authors describe how multitenancy can be implemented in order to allow the same application to be shared among different users. As result of multitenancy at the application level, data of different users are stored in common structures [25] which enables malicious tenants to exploit applications loopholes, masked code injection, or security misconfigurations to sneak into other users data [25,51].

Isolation issues of the Cloud also heavily affect the security of IoT devices relying on it. For instance, in the context of IP cameras, if the isolation between device owners is not properly implemented, a malicious user can have complete control of someone else's IP camera and collect sensitive multimedia content from it in an absolute stealthy way [71].

Synchronization Mechanisms Issues

Synchronization mechanisms are common in Cloud storage SaaS implementations [72]. When modifications of files are performed on a local device, such mechanisms allow propagating updates to all other devices interested in those files [72]. These mechanisms are typically implemented by the use of tokens which have been shown to introduce new vulnerabilities that can lead to data exfiltration [72,73]. An example of attack exploiting such vulnerability is the Man in the Cloud (MitC) attack [73]. Due to its propagation characteristics, this kind of attack can both be struck on an IoT device and on the Cloud platform, subsequently allowing to attack other IoT devices that share the same implementation.

5.1.3. Data Storage Level Issues

In the following paragraphs, we are going to report some confidentiality issues that, despite being specific of the Cloud, are not strictly related to a specific level of the Cloud architecture but that embrace more than one level.

Outsourcing Issues

Applications deployed on the Cloud have to be remotely accessed by users who, depending on the type of application and elaboration needed, may be requested to outsource private and confidential information. The immediate consequence of outsourcing is a loss of control which impedes the owner of outsourced data to directly dispose and control them as he prefers, making it difficult to protect confidentiality with traditional methods [32]. To understand the reasons behind such difficulty it is paramount to distinguish between applications offering storage services and applications offering some type of remote elaborations. In both cases, it is legitimate to assume that the service provider will implement access policies and security mechanisms for protecting users' data [74] but it also implies that it is in the perfect position to access such data and therefore break users' data confidentiality. However, while in the former case users can easily prevent such situation by encrypting data before storing on the Cloud (which could also make it much more secure than unencrypted storing habits [75]), in the latter case, the possibility to protect confidentiality by means of traditional encryption schema is not feasible due to the service provider need of performing elaborations [76].

Nevertheless, plain text data should be avoided in order to prevent Cloud providers from accessing information which, due to the lack of control, could even be stored or transmitted to third parties and be used for other purposes (there are examples in the literature demonstrating how such situations can produce unwanted consequences; some of these threats, which are also related to multi-location, can be found in [75]). If we consider that Cloud applications take advantage of composite request processing [77], which allows service providers itself to outsource part of the computation, it is clear that the confidentiality risks are even higher. Full homomorphic encryption could be the solution to alleviate confidentiality concerns of outsourced data but according to [78,79] this approach is neither efficient nor adequate for general purpose elaborations, yet.

In the IoT world, we witnessed a similar issue with CloudPets teddy bears, which allowed malicious users to access kids' voice messages, simply by knowing the path to the object (stored on an Amazon S3 bucket), without requiring any login nor authentication token (https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/).

In some cases, even applications offering a pure storage service may still require some amount of computations on encrypted data (for instance, content research may be required for enabling fine-grained retrieval) [80]. To face this necessity, confidentiality-preserving query evaluation approaches are reported in [81], but, similarly to the case of homomorphic encryption, they only support partial query execution. Moreover, even if encryption or fragmentation techniques are used to protect the confidentiality of data, it may also be required to hide information about which data is accessed (access confidentiality) together with the patterns exhibited in accessing such data (pattern confidentiality) [74,82]. Indeed, in [83] it is demonstrated that lacks in protecting such information can result in contents disclosures.

In case that data are remotely elaborated on the Cloud by means of programs written by the owner of such data (which is typically the case for IaaS and PaaS services), to protect confidentiality and integrity from an untrusted Cloud provider, solutions relying on Intel software guard extensions (SGX) have recently been proposed [84]. SGX features allow processors to instantiate secure memory regions which are protected from hardware attacks or malicious privileged code [84]. This capability could be used for executing programs in the Cloud with a similar level of security to the one in which programs are executed on hardware resources belonging and controlled by the owner of data [84].

Data Deletion Issues

Data deletion needs special attention since if it is not correctly performed it leads to greater confidentiality threats. From the one hand, even if the delete operation has been correctly performed, the integrity of the operation can indirectly be breached due to data recovery vulnerabilities [26]. An example of such situation arises due to the physical features of storage devices which can allow restoring original data [76] even if the delete operation has actually been performed at the software level. On top of these cases, the service provider may directly impact on the integrity of the delete operation by incorrectly performing such operation (for instance due to not properly taking into account data replication) [85] or even by not performing it at all.

5.2. Integrity

Integrity is the "assurance that the information is authentic, complete and can be relied upon to be sufficiently accurate for its purpose. It refers to whether the information is correct and can be trusted and relied upon" [37]. We extend such definition to embrace also the integrity of computations. This implies that the integrity is also about guaranteeing that information resulting from computations is authentic, complete and can be relied upon.

The same classification of security issues that has been previously performed in relation to confidentiality is going to be repeated for integrity issues. Besides, taken into consideration the fact that confidentiality and integrity issues often go hand in hand, we have found out that the threats to the two properties overlap quite considerably.

5.2.1. Virtualization Level Issues

In the following paragraphs, security issues rooted in the virtualization layer and with the potential to impact the integrity of data are presented.

VM Isolation Issues

At this level, virtual machine escaping is the way in which data and software integrity can be attacked. Indeed, a compromised VMM can threaten the integrity of data [74]. More specifically, if a virtual machine is able to escape from isolation and compromise the VMM, it can access memory locations belonging to other users while having the required privileges to write or delete their content [47,49], in such a way to perform a VM hopping attack [86,87]. The VMM can possibly be attacked through several attack vector: device drivers, VM exit events or hypercalls [88]; a throughout list of vulnerabilities typical of common VMMs used to deploy Cloud systems, can be found in [89]. For this reason, in order to protect users' data integrity, it is essential to protect the isolation capabilities and integrity of virtual machine monitors. A list of possible mechanisms to guarantee VMM integrity and enhance isolation is reported in [48,49].

VM Management Issues

Bad management of VM images has negative repercussion on the integrity of the Cloud environment. Indeed, vulnerabilities in the Cloud environment can be introduced by injecting malware into VM images repositories [67]. Thereafter, with lacks of proper VM image management and controls, sporadically running images are in the perfect position to carry worms and compromise the integrity of other images while avoiding detection thanks to low activity level [62]. Therefore, integrity checks and scans of VM images are required as a consequence of VM cloning and sharing. Moreover, such controls are also paramount in relation to the necessity to protect Cloud repositories against the increasing trend of "bad repositories", i.e., the use of Cloud repositories as containers of services for illicit activities [90].

VM Migration Issues

Live virtual machine migration is paramount for Cloud environments, however, it needs to be properly implemented from a security perspective (see also Section 5.1). As for integrity, the attack surface of the migration protocol is potentially quite vast [65]: common vulnerabilities may be used to inject malicious code in the programs implementing the migration process; if no encryption is used to secure the exchange of messages controlling the transfer, then, messages might be manipulated to impair integrity of the process; moreover, even compromised hosts might be exploited for affecting integrity of the migrated VM once it is moved to a controlled malicious host.

5.2.2. Application Level Issues

We are now going to present integrity issues that are rooted in the application layer. We take into account issues affecting the integrity of data and elaborations.

Computation Cheating Issues

The combination of outsourcing together with the transparency lack in the way Cloud services are implemented, allows service providers to alter the results of computations or even to not perform elaborations in the proper way [80]. If at first such a situation might seem strange, there are actually several reasons behind it. For example, driven by the desire to reduce costs, service providers may be tempted to simplify computations when lots of resources are needed [91]. Remote computation can be cheated in several ways: elaborations can be performed on partial or not up to date data, they can be performed incorrectly or may even return partial results [74,92]. Remote computation audit and verifiable computation have therefore been proposed to face this issue. A review of possible solutions trying to address such a problem is presented in [32].

Computation might also be cheated not because of the service provider but due to specific attacks. An example of such inconvenience is the Cloud malware injection attack. Cloud providers are responsible for redirecting user's requests toward appropriate services capable of satisfying them [93]. An adversary can exploit such situation to create malicious service implementations, add them to the Cloud and trick the Cloud provider to believe that they are real implementation of some services by falsifying metadata descriptors used to identify functionalities offered by applications [93]. This type of attack results in applications integrity breach since from a user perspective the service has not performed as expected.

Insecure APIs, Management and Control Interfaces

By means of APIs and management interfaces Cloud users can request, monitor, and obtain resources dynamically based on their needs, making the Cloud an on-demand self-service platform [94]. However, since these interfaces are accessible through the internet and because of web vulnerabilities [85], the risk of unauthorized access is much higher if compared to traditional systems [26]. It follows that if an attacker is able to gain unauthorized access to the data contained in such interfaces, then he can compromise services and break applications integrity [95].

Currently, this is a considerable problem in the IoT landscape. Some manufacturers store personal data of their customers in plain text, which means that any unauthorized access to the storage service could automatically lead to data leakage. As a practical example of this, in 2015 Rapid7 (an IT security company) published a technical report that analyzed 7 baby-monitors on the market [96]. Among them, Fisher-Price Smart Toy, a smart teddy-bear capable of learning kids' basic information (name, date of birth, and so on) was found to handle authentication tokens. This enabled attackers to perform unauthorized actions, such as accessing and editing kids' personal information, finding whether parents were actively using the connected smartphone application, as well as if kids were actively playing with the toy. In the same report, similar issues were found in other consumer devices, such as the Philips In.Sight B120 and the Summer Infant Baby Zoom Monitor. The former was found to be vulnerable to reflective and stored XSS, which enabled potential session hijacking that would allow an attacker to create a valid streaming session, without any authorization. The latter product enabled a regular user to escalate privileges and access to the cloud service administrative interface, simply by manually inserting the URL to the admin page.

Isolation Issues

Isolation issues within platforms used to create PaaS systems (see also Section 5.1) can affect integrity of data and applications belonging to other tenants [69].

Synchronization Mechanisms Issues

According to [73] vulnerabilities in synchronization mechanisms might also be exploited to compromise the integrity of data. An example of attack that can allow achieving this is the Man in the Cloud (MitC) attack (see also Section 5.1). The integrity of data can be compromised by such attacks since authentication vulnerabilities are exploited. Therefore, once the attacker takes advantage of tokens and authenticates as a different user, then he is able to impair both confidentiality and integrity of all data belonging to that user.

5.2.3. Data Storage Level Issues

In the following paragraph, we discuss integrity issues related to the protection of data storage. We have decided to not directly associate these issues to any of the previous levels as we consider data storage related to all levels of our reference architecture and not predominant of any of them.

Outsourcing Issues

As is the case for confidentiality, outsourcing of data is the Cloud feature that arises new integrity challenges. Data integrity can be compromised in several possible ways and reasons: a Cloud service provider, for economic reasons, may delete users' rarely accessed data in order to release storage space that can be sold to other users; even assuming a perfectly behaving provider, malfunctions are still there to compromise data (which is indeed what happened to Amazon S3 some years ago [97]); more in general, external attackers, driven by economic reasons, might compromise data integrity and this might even not be timely discovered by users [98] due the Cloud providers' tendency of hiding unpleasant events that could affect their businesses.

The need for integrity mechanisms is therefore clear. However, due to outsourcing, traditional integrity mechanisms are not applicable in this scenario since they would require the download of outsourced data for allowing local integrity checks to be performed [80,98]. Indeed, this is unacceptable for efficiency reasons as it would nullify the Cloud advantages (especially in relation to a situation where high amounts of data are outsourced). Therefore, remote data integrity checking protocols are required [99]. Nevertheless, challenges do exist for the development of such protocols especially in relation to efficiency requirements and the possibility to guarantee the integrity of dynamic data (i.e., data that are modified or updated after they have been loaded in the Cloud). For limited resourced clients, the burden of computation and communication imposed by such protocol has to be as limited as possible, which has lead to the idea of using protocols based on third parties auditors [92]. In [100], an in-depth review of remote data integrity checking protocol is presented with associated issues for their development and possible attacks they may face.

5.3. Availability

Availability is the "assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them" [37]. Hence, availability is the property indicating the possibility, for authorized users, to access (and modify) data whenever needed [38].

This subsection is aimed at presenting availability and performance degradation issues that arise at the different levels of our architecture.

5.3.1. Virtualization Level Issues

Virtualization technology introduces new attack vectors that can be exploited to impact on the availability and performances of Cloud systems. In the next paragraphs, we seek to report the main issues we have identified in relation to this concern.

Multi-Tenancy Issues

According to [39], an attacker can exploit co-residence, and act on shared physical resources, in such a way to perform denial-of-service attacks or cross-VM performance degradation attacks. The possibility to verify co-residence might also be exploited to provoke changes in resource utilization of co-resident VMs in such a way to make them use fewer resources (and hence impacting on their availability) and therefore let the attacker gain high resource availability. This attack is known as Resource-Freeing attack [101].

VM Management Issues

Availability issues may also arise due to bad VM management policy. An example of such eventuality is VM sprawling, which is a situation where the number of hosted virtual machines keep increasing while most of them are idle [102]. VM sprawling can also result from specific attacks aiming at discarding confirmation messages generated from the Cloud service to confirm users that their requests of VM execution have been correctly performed. If users do not receive such confirmation messages, they will keep instantiating VMs even if their action has already been performed. This attack leads to the creation of orphan VMs which can degrade performance and eventually exhaust the pool of resources [103].

VM Isolation

Availability can be compromised by virtual machines breaking out of isolation and being able to either use all host resources or performing a system halt [49].

Scheduling issues might be exploited to impact on the performance (and also availability) of other VMs. Indeed, an attacker can manipulate hypervisor scheduling mechanisms in such a way to obtain more resources for his own VM at the expenses of other clients [104]. Such a situation, taken to the limit, can lead to starvation of other VMs or, more in general, can degrade services to such an extent of making services deployed within VMs unusable.

Virtual Network Issues

According to [52], poor scalability of virtual networks is another factor that can be exploited for a denial of service (DoS) attack.

VM Migration Issues

Malicious VMs can take advantage of live virtual machine migration to perform DoS attacks or achieve performance degradation. The migrant attack is an example of such type of DoS attack. In a migrant attack, a small set of compromised VMs is coordinated to generate useless resource consumption in order to mislead the Cloud monitoring mechanisms to trigger migration processes [66]. Since live migrations are expensive processes, this allows attackers to waste Cloud resources and degrade performances of other VMs. An equivalent class of DoS attack similar to the previous one is Cloud-Internal Denial of Service attacks (CIDoS) [105].

Researchers in [106,107], proposed to use live migration for reducing the time of co-residency among virtual machines and hence prevent side-channel attacks. However, it has been recently shown that it could be possible for an adversary to slow down migration processes and therefore still permit the attackers to perform side-channel information stealing [108]. In relation to availability, this attack (known as stalling attack) demonstrates the possibility for co-resident adversaries to prevent migrations and hence degrade performances by obstructing the performance gain that would follow from migrations.

Cloud-Droplet-Freezing (CDF) is another type of DoS attack which is based on the observation that if migrations of VMs are carried on during a flooding attack for the purpose of load-balancing and trying to mitigate the attack, then it might also contribute to increase the overhead for the Cloud and weaken even more its resource availability [109].

5.3.2. Application Level Issues

By excluding application layer protocols that support networking (which are not specific of the Cloud, and for this reason discussed in Section 6), at this layer, we have identified only one relevant Cloud specific issue that can impact on the availability of data.

Resource Accounting Issues

PaaS systems enable third-party applications to run on a shared platform (see also Section 5.1). Resource accounting mechanisms are required in order to monitor and limit the applications utilization of resources. In [69], it was shown that both Java and .Net (which can both be used to implement a PaaS system) lacked mechanisms for monitoring resources. This situation could have been exploited by malicious tenants to keep instantiating objects until the Cloud provider memory was exhausted.

5.3.3. Network Level Issues

As for the previous layer, even in this case we have identified only one Cloud specific issue located at the network level and capable of affecting Cloud availability.

Network Under-Provisioning Issues

A new form of DoS attack in Cloud scenarios that exploits network under-provisioning is described in [110].

5.3.4. Multi-Level Issues

In the next paragraph, we present a class of attacks, also known as Economic Denial of Sustainability attacks, that have the potential to impact the availability of services deployed on the Cloud. Since this class of attacks represents a methodology to strike a Cloud system, which can be implemented by exploiting several protocols located at more than one layer of our architecture, we have decided to present it in this parallel subsection and separated from the layer-oriented classification.

Economic Sustainability Issues

This category represents a set of attacks aimed at causing a financial burden for providers offering services through the Cloud [111] with the purpose of making the Cloud economically unsustainable [112].

An example of such attack is Fraudulent Resource Consumption (FRC). In this case, the adversary behaves as a normal user and requests to the victim's service deployed on the Cloud to perform some operations. However, differently from a flooding attack, the adversary does not seek to congest the service provider resources; instead, he seeks to maintain a low profile of requests (i.e., produce a number of requests that will not be as overwhelming as is the case for flooding attacks) with the purpose of being able to produce them for a long period of time [32]. As a result, the adversary exploits the pay as you go and auto-scaling models for billing to the service provider an unforeseen amount of resource utilization. The attacker's aim is that, eventually, the service provider will face unexpected expenses which will lead to economic losses and therefore deprive the long-term economic availability of using the Cloud [32], which in turn may also result in a denial of service attack and make the targeted services unavailable on the Cloud [113].

When the resource consumed by an FRC attack is the electrical energy and power of the Cloud infrastructure, we refer to such an attack as Energy-related Denial of Service attack (e-DoS) [114]. In this case, the adversary's goal is to produce a limited amount of requests that will switch the victim's electronic facilities from low energy consumption states to high energy consumption states [114].

As noted in [111], a naive solution to this type of attacks would be to disable the auto-scaling capabilities offered by the Cloud. However, with the lack of auto-scaling, the attack would directly result in a denial of service and would also nullify the elastic advantages of the Cloud environment.

Even if this category of attacks is not completely aimed at compromising the availability of services, similarly to various works in literature (e.g., [32]), we consider it as a problem of availability. The main reason behind this choice is related to the similarity that these attacks have with DoS attacks. Moreover, by making the Cloud economically disadvantageous, the service provider may be pushed to remove their services from the Cloud and hence, in a Cloud perspective, factually render such service unavailable on it.

6. Generic Security Issues

In this section, we present a brief overview of generic security issues, which are also relevant to Cloud computing. Such topics have been extensively covered by many other researchers, therefore, we will simply provide a quick description of all of them, as well as the main consequences for the Cloud. We use the same approach used in Section 5, where we grouped security issues by means of CIA properties.

6.1. Confidentiality

In this section, we present a short recap of generic security issues that apply to Cloud as well, and that can specifically endanger confidentiality.

6.1.1. Network Level Issues

Well-known examples of network-level attacks that can affect the confidentiality of networked systems are packet sniffing, IP spoofing, ARP spoofing, and Man In The Middle attacks (MITM) [27,115,116]. Since the Cloud heavily relies on networks and communication protocols, such as Message Queue Telemetry Transport (MQTT), MITM attacks are the most dangerous threat when it comes to network confidentiality.

6.1.2. Application Level Issues

We can enlist a number of different attacks that can lead to confidentiality issues at the web-technology layer, such as Cross-site scripting (XSS), code injection, and Man-in-the-Browser (MitB) [25,116,117]. Operating at the application level, these attacks have the capability of stealing cookies [118], personal passwords through keyloggers [117], and confidential information that transits through browsers [119].

Besides, improperly programmed applications are probably the main cause of IoT security flaws. In 2012, TRENDnet SecurView cameras were found to be extremely insecure, at the point that their devices allowed unauthorized users to access their live recordings, simply by connecting directly to their IP addresses with a browser (http://console-cowboys.blogspot.com/2012/01/trendnet-cameras-i-always-feel-like.html). What is troublesome is that these recurring events are not triggered by mere human errors, happened while implementing security countermeasures, but by the widespread attitude to simply ignore security best practices.

6.1.3. Multi-Level Issues

Advanced Persistent Threats can potentially attack the victim at different architectural layers. For example, the attacker can utilize different techniques to gather information, from MITM attacks to phishing emails, with an ultimate goal in mind: uploading a malware on the victim's machine, and extract private data through covert channels [120–122].

The Cloud can be affected by similar attacks in two ways. First, it can be exploited to silently transmit information from the victim to the attacker (e.g., by means of covert channels). Second, it can be directly attacked with a malware [120], with the objective of stealing Cloud users' data for long periods of times [123]. The last case is particularly dangerous for a Cloud environment because, once a user gets infected, it can also compromise other services and users [120].

6.2. Integrity

In this section, we follow the same pattern used in Section 6.1, and we give some examples of generic attacks that can tamper with data integrity at different levels. Similarly to what we have done in Section 5.3, when we talk about integrity we also take into consideration the integrity of computation outputs, not only of raw data.

6.2.1. Network Level Issues

Similarly to confidentiality issues in Section 6.1.1, integrity can be heavily endangered by Man In The Middle attacks (MITM). In particular, the attacker might decide to manipulate specific packets and tamper with the intended communication flow.

6.2.2. Application Level Issues

At the application level, various attacks can interfere with data integrity. Among the others, Cross-site request forgery (CSRF) [124,125], hidden field manipulation [25,126], cookie poisoning [127], and XML Signature Element Wrapping [93]. In particular, in the past Amazon EC2 has been found vulnerable to XML Signature Element Wrapping.

6.3. Availability

Last, availability issues due to generic security attacks apply both at the network level and at the application level. In this section, we give a brief summary of such attacks.

6.3.1. Network Level Issues

DoS attacks, as well as Distributed Denial of Service (DDoS) attacks, are the main categories of attacks that can affect availability at the network level. DDoS attacks are more dangerous than SDoS ones [128], since they hide the original attacker, make it difficult to distinguish between a legit overload and a malicious attack, and generate a huge quantity of traffic [129,130].

Notably, even though DoS and DDoS attacks affect other paradigms than Cloud computing, researchers demonstrated that these are critical threats for Cloud computing. As a matter of fact, not only Cloud can be the victim of such attacks, but it can be part of the attacking infrastructure; for example, botClouds [131] are DDoS botnets deployed in the Cloud environment.

Yan et al. [132] identified a growing number of DoS attacks occurrences in Cloud environments, and argue that this relationship may be rooted in the intrinsic characteristics of the Cloud which, in a certain way, support the success of DoS attacks. For the sake of brevity, we are not going to dig into each and every kind of DoS attack. We point out that authors of [93] identified two types of flooding attacks effects which are specific of the Cloud, namely Direct DoS and Indirect DoS.

To have a clear picture of the impact that DoS attacks can have, it is sufficient to consider that the DDoS Mirai malware infected over 600.000 devices and its DDoS attacks reached traffic peaks of 1 Tbit/s [7,133].

6.3.2. Application Level Issues

Similarly to what we have described in Section 6.3, availability can be impeded by DoS attacks performed at the application level. Here we choose to not emphasize the difference among SDoS and DDoS attacks but to distinguish between application-enabled DoS and flooding attacks.

In the first category, we can enlist all the DoS attacks that exploit vulnerabilities at the application level. It is worth noting that anything from misconfiguration to software bugs can potentially enable a DoS attack [134]: examples comprise HTTP POST attacks [135], Coercive parsing [136], and Chained encrypted keys [136].

In the second category, HTTP flooding attacks [134,137,138] and XML Oversize Payload attacks [116,136] are good examples. Contrary to the previous category, here the attacker does not exploit any configuration nor software error, but she simply aims to fill up the target's resources by issuing as many requests as possible, eventually impeding honest users to access the target's services.

7. IoT Security Issues

The Internet of Things (IoT) pervades more and more aspects of our lives and often involves many types of smart connected objects and devices. These are becoming smarter and smarter with the ability to accumulate private data (i.e., current location, heartbeat, etc.), to share them with other devices or with cloud-based infrastructures and, to control and adapt the behavior of critical systems (i.e., autonomous cars). In this Section, we present some of the set of security issues peculiar for IoT-based systems . For each issue we give a short description, its possible impact and a set of possible solution to mitigate it. Most of the IoT products are provided and purchased with a first level of security. During its usage some of them don't get enough updates while, some don't get updates at all. This leaves their trusted customers exposed to potential attacks as a result of outdated hardware and software. To solve this issue, in [139,140], the authors propose a blockchain based privacy-preserving software updates protocol, which delivers secure and reliable updates with an incentive mechanism, as well protects the privacy of involved users. The vendor delivers the updates and it makes a commitment by using a smart contract to provide financial incentive to the transmission nodes who deliver the updates to the IoT devices. PAST [141] is a self-adaptive security tool for discovering the features of the protocols adopted by the devices in an IoT ecosystem. With PAST, specific security defenses are deployed on the basis of (i) the attacks targeting such protocols, and (ii) the security features provided by the protocols themselves. Many IoT devices are released with *default passwords* and lack basic security mechanisms, making them easy prey for malware. In [142], the authors propose three approaches for framework design and collecting the network data, each providing different levels of visibility into IoT device behavior. They also present a methodology for anomaly detection and IoT device identification using the data collected by the gateways behind them, or in the cloud. They pose a vision that can be summarized with the following sentence: "securing IoT devices can be more efficient and effective when there is more visibility into device activity and security capabilities are deployed close to the devices, in the gateway". However, a hybrid approach in which data is collected on the gateways and analyzed in the cloud can be more practical; special considerations regarding sensitive data storage and privacy guarantees have to be taken into account. IoT devices not only work in isolation but sometimes they collaborate sending also messages to the network without any encryption. Data is constantly being collected, transmitted, stored and shared by various devices (i.e., Smart TV, Mobile Phone, Wi-Fi printers, etc.) produced by different companies. In this way, all of these data are shared between companies with the possibility to violate the users privacy and data security. This issue is very much in evidence in the Internet of Vehicles (IoV) context, where information is gathered and disseminated among vehicles, roadside infrastructures and surrounding environments. Approaches as the one proposed in [143] propose location privacy-preserving data sharing scheme which enables the collection and distribution of the data captured by vehicular sensors. The proposed scheme enables a data querying vehicle to retrieve the sensory data captured by other vehicles at the network edge, i.e., without the involvement of the trusted central traffic management authority.

Discussion

As we have seen in this section, IoT devices facilitate the data gathering and collection pushing the proliferation of a lot of smart applications in different domains (i.e., automotive, healthcare, education, logistics, etc.). However, due to the significant number of issues related to the security and privacy management of these data, the way in which the IoT devices are produced and maintained, sometimes creates fertile ground for all the activities aimed at making applications vulnerable and therefore dangerous, both for the privacy and security of the users. This aspect open many research challenges in the context of systems where IoT and Cloud are two sides of the same coin. Since finding solutions only in one side or in another is not sufficient, there is an increasing need to find solution able to make the convergence of Cloud and IoT as the way towards their potential security solutions [144].

8. Conclusions and Future Work

In this paper, we have analyzed the security of Cloud computing from a specific perspective: Cloud computing considered as a core component of the IoT architecture. The motivation behind this work resides on the evidence that, today, IoT devices strongly rely on the Cloud, where data analytics and intelligence reside. Therefore, addressing the security of IoT devices and Cloud computing as different concerns is no longer enough to tackle security issues of the IoT, in its broader meaning.

It is worthy of note that the vast majority of attacks currently directed to IoT devices are fuelled by trivial errors, such as lack of authentication routines, and that the vulnerabilities we have described in this paper are far more complex than the exploited ones in real-life scenarios. However, once the basic IoT shortcomings will be remedied, malicious attackers might start to dig deeper into the relationship between IoT and Cloud computing.

As a result, we have provided an up-to-date and well-structured survey of the security issues of Cloud computing in the IoT era. The analysis has been based on a structured approach, distinguishing between Cloud-specific and generic security issues, and classifying both classes from two angles: the affected Cloud architectural layer and the impacted CIA security property (i.e., confidentiality, integrity, availability). We believe that this classification is important to have a clear picture of where security issues occur and what their potential impact is. As a result, our analysis points out that, since there is no IoT without the Cloud, we cannot secure IoT without securing the Cloud. Thus, we consider this work as a first step toward the investigation of IoT security in its broader meaning.

This work can be extended in different ways. For instance, it could be useful to add a risk analysis, specifying the risk associated with each vulnerability. Moreover, due to the broad nature of the topic covered in this paper, we have tried to keep its scope very well focused, considering only the fundamental and well-known CIA security properties. Nevertheless, it would be interesting to extend the analysis by taking into consideration other relevant security properties, such as authenticity and accountability. In particular, IoT systems are meant to work in unreliable contexts where it is important not only to protect interactions and services against malicious attack (self-protection), but also against accidental failures (self-healing) [145].

Looking at Microservices as an architectural approach for creating cloud applications, where each application is designed and built as a set of services defined by business capabilities, the analysis could expand into this domain and the related programming languages [146]. Microservices, IoT, and related security challenges have certainly a lot in common with what described in his work, but certain peculiarities would deserve a separate discussion. Formal approaches and rigorous semantics have also not been considered in this work despite their importance for Cloud and distributed/concurrent systems in general [147–149].

Author Contributions: Writing—original draft, M.D.D., A.G., N.D., A.B. and M.M.; Writing—review & editing, N.D., A.B. and M.M.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. IoTdevs. Available online: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (accessed on 21 January 2019).
2. Rehman, H.U.; Asif, M.; Ahmad, M. Future applications and research challenges of IOT. In Proceedings of the 2017 International Conference on Information and Communication Technologies (ICICT), Karachi, Pakistan, 30–31 December 2017; pp. 68–74.
3. Nalin, M.; Baroni, I.; Mazzara, M. A Holistic Infrastructure to Support Elderlies' Independent Living. In *Encyclopedia of E-Health and Telemedicine*; IGI Global: Hershey, PA, USA, 2016.
4. Salikhov, D.; Khanda, K.; Gusmanov, K.; Mazzara, M.; Mavridis, N. Microservice-based IoT for Smart Buildings. In Proceedings of the 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, Taiwan, 27–29 March 2017.
5. Salikhov, D.; Khanda, K.; Gusmanov, K.; Mazzara, M.; Mavridis, N. Jolie Good Buildings: Internet of things for smart building infrastructure supporting concurrent apps utilizing distributed microservices. In Proceedings of the 1st International conference on Convergent Cognitive Information Technologies, Moscow, Russia, 25–26 November 2016; pp. 48–53.
6. Dragoni, N.; Giaretta, A.; Mazzara, M. The Internet of Hackable Things. In Proceedings of the 5th International Conference in Software Engineering for Defense Applications (SEDA'16), Rome, Italy, 10 May 2016; Springer: Berlin/Heidelberg, Germany, 2018.
7. De Donno, M.; Dragoni, N.; Giaretta, A.; Spognardi, A. DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation. *Secur. Commun. Netw.* **2018**, *2018*, 7178164. [CrossRef]
8. Donno, M.D.; Dragoni, N.; Giaretta, A.; Mazzara, M. AntibIoTic: Protecting IoT Devices Against DDoS Attacks. In Proceedings of the 5th International Conference in Software Engineering for Defence Applications—SEDA 2016, Rome, Italy, 10 May 2016; pp. 59–72.
9. Online Oxford Dictionary. Available online: https://en.oxforddictionaries.com/definition/internet_of_things (accessed on 3 December 2018).

10. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A survey on security and privacy issues in Internet-of-Things. *IEEE Internet Things J.* **2017**, *4*, 1250–1258. [CrossRef]
11. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [CrossRef]
12. Conti, M.; Dehghantanha, A.; Franke, K.; Watson, S. Internet of Things security and forensics: Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *78*, 544–546. [CrossRef]
13. Guan, Z.; Li, J.; Wu, L.; Zhang, Y.; Wu, J.; Du, X. Achieving Efficient and Secure Data Acquisition for Cloud-Supported Internet of Things in Smart Grid. *IEEE Internet Things J.* **2017**, *4*, 1934–1944. [CrossRef]
14. Mihovska, A.; Sarkar, M. Smart Connectivity for Internet of Things (IoT) Applications. In *New Advances in the Internet of Things*; Yager, R.R., Pascual Espada, J., Eds.; Springer International Publishing: Cham, Switerland, 2018; pp. 105–118.
15. Malik, A.; Om, H. Cloud Computing and Internet of Things Integration: Architecture, Applications, Issues, and Challenges. In *Sustainable Cloud and Energy Services: Principles and Practice*; Rivera, W., Ed.; Springer International Publishing: Cham, Switerland, 2018; pp. 1–24.
16. Mahmud, R.; Kotagiri, R.; Buyya, R. Fog Computing: A Taxonomy, Survey and Future Directions. In *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives*; Di Martino, B., Li, K.C., Yang, L.T., Esposito, A., Eds.; Springer: Singapore, 2018; pp. 103–130.
17. Botta, A.; de Donato, W.; Persico, V.; Pescapé, A. On the Integration of Cloud Computing and Internet of Things. In Proceedings of the 2014 International Conference on Future Internet of Things and Cloud, Barcelona, Spain, 27–29 August 2014; pp. 23–30. [CrossRef]
18. Botta, A.; De Donato, W.; Persico, V.; Pescapé, A. Integration of cloud computing and internet of things: A survey. *Future Gener. Comput. Syst.* **2016**, *56*, 684–700. [CrossRef]
19. Díaz, M.; Martín, C.; Rubio, B. State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *J. Netw. Comput. Appl.* **2016**, *67*, 99–117, [CrossRef]
20. Cook, A.; Robinson, M.; Ferrag, M.A.; Maglaras, L.A.; He, Y.; Jones, K.; Janicke, H. Internet of Cloud: Security and Privacy Issues. In *Cloud Computing for Optimization: Foundations, Applications, and Challenges*; Mishra, B.S.P., Das, H., Dehuri, S., Jagadev, A.K., Eds.; Springer International Publishing: Cham, Switerland, 2018; pp. 271–301.
21. OpenFog Consortium Architecture Working Group. *OpenFog Reference Architecture for Fog Computing*. 2017. Available online: https://www.openfogconsortium.org/wp-content/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL.pdf (Accessed on 4 June 2019).
22. Liu, Y.; Sun, Y.; Ryoo, J.; Rizvi, S.; Vasilakos, A.V. A survey of security and privacy challenges in cloud computing: solutions and future directions. *J. Comput. Sci. Eng.* **2015**, *9*, 119–133. [CrossRef]
23. Shahzad, F. State-of-the-art survey on cloud computing security Challenges, approaches and solutions. *Procedia Comput. Sci.* **2014**, *37*, 357–362. [CrossRef]
24. Ryan, M.D. Cloud computing security: The scientific challenge, and a survey of solutions. *J. Syst. Softw.* **2013**, *86*, 2263–2268. [CrossRef]
25. Subashini, S.; Kavitha, V. A survey on security issues in service delivery models of cloud computing. *J. Netw. Comput. Appl.* **2011**, *34*, 1–11. [CrossRef]
26. Grobauer, B.; Walloschek, T.; Stocker, E. Understanding cloud computing vulnerabilities. *IEEE Secur. Priv.* **2011**, *9*, 50–57. [CrossRef]
27. Modi, C.; Patel, D.; Borisaniya, B.; Patel, A.; Rajarajan, M. A survey on security issues and solutions at different layers of Cloud computing. *J. Supercomput.* **2013**, *63*, 561–592. [CrossRef]
28. Singh, S.; Jeong, Y.S.; Park, J.H. A survey on cloud computing security: Issues, threats, and solutions. *J. Netw. Comput. Appl.* **2016**, *75*, 200–222. [CrossRef]
29. Fernandes, D.A.B.; Soares, L.F.B.; Gomes, J.V.; Freire, M.M.; Inácio, P.R.M. Security issues in cloud environments: A survey. *Int. J. Inf. Secur.* **2014**, *13*, 113–170. [CrossRef]
30. Polash, F.; Abuhussein, A.; Shiva, S. A survey of cloud computing taxonomies: Rationale and overview. In Proceedings of the 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014), London, UK, 8–10 December 2014; pp. 459–465. [CrossRef]
31. Singh, A.; Chatterjee, K. Cloud security issues and challenges: A survey. *J. Netw. Comput. Appl.* **2017**, *79*, 88–115. [CrossRef]

32. Xiao, Z.; Xiao, Y. Security and privacy in cloud computing. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 843–859. [CrossRef]
33. Ardagna, C.A.; Asal, R.; Damiani, E.; Vu, Q.H. From security to assurance in the cloud: A survey. *ACM Comput. Surv.* **2015**, *48*, 2. [CrossRef]
34. Hashizume, K.; Rosado, D.G.; Fernández-Medina, E.; Fernandez, E.B. An analysis of security issues for cloud computing. *J. Internet Serv. Appl.* **2013**, *4*, 5. [CrossRef]
35. Mell, P.; Grance, T. *The NIST Definition of Cloud Computing*; Technical Report, 2011. Available online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (accessed on 4 June 2019).
36. Liu, F.; Tong, J.; Mao, J.; Bohn, R.; Messina, J.; Badger, L.; Leaf, D. *NIST Cloud Computing Reference Architecture*; Technical Report 2011; NIST: Gaithersburg, MD, USA, 2011.
37. Glossary of Terms Related to Fog Computing. Available Online: https://www.openfogconsortium.org/wp-content/uploads/OpenFog-Consortium-Glossary-of-Terms-January-2018.pdf (accessed on 10 October 2018).
38. Goodrich, M.; Tamassia, R. *Introduction to Computer Security*; Pearson Education, Inc.: Boston, MA, USA, 2011.
39. 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, IL, USA, 9–13 November 2009; ACM: New York, NY, USA, 2009; pp. 199–212. [CrossRef]
40. Zhang, Y.; Juels, A.; Reiter, M.K.; 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, Raleigh, NC, USA, 16–18 October 2012; ACM: New York, NY, USA, 2012; pp. 305–316.
41. Yarom, Y.; Falkner, K. FLUSH + RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack. In Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, 20–22 August 2014; pp. 719–732.
42. Liu, F.; Yarom, Y.; Ge, Q.; Heiser, G.; Lee, R.B. Last-level cache side-channel attacks are practical. In Proceedings of the 2015 IEEE Symposium on IEEE Security and Privacy (SP), San Jose, CA, USA, 17–21 May 2015; pp. 605–622.
43. Irazoqui, G.; Inci, M.S.; Eisenbarth, T.; Sunar, B. Wait a minute! A fast, Cross-VM attack on AES. In *International Workshop on Recent Advances in Intrusion Detection*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 299–319.
44. Suzaki, K.; Iijima, K.; Yagi, T.; Artho, C. Memory Deduplication As a Threat to the Guest OS. In Proceedings of the Fourth European Workshop on System Security, Salzburg, Austria, 10 April 2011; ACM: New York, NY, USA, 2011; pp. 1:1–1:6. [CrossRef]
45. Lipp, M.; Schwarz, M.; Gruss, D.; Prescher, T.; Haas, W.; Mangard, S.; Kocher, P.; Genkin, D.; Yarom, Y.; Hamburg, M. Meltdown. *arXiv* **2018**, arXiv:1801.01207.
46. Kocher, P.; Genkin, D.; Gruss, D.; Haas, W.; Hamburg, M.; Lipp, M.; Mangard, S.; Prescher, T.; Schwarz, M.; Yarom, Y. Spectre Attacks: Exploiting Speculative Execution. *arXiv* **2018**, arXiv:1801.01203.
47. Wang, Z.; Wu, C.; Grace, M.; Jiang, X. Isolating commodity hosted hypervisors with hyperlock. In Proceedings of the 7th ACM European Conference on Computer Systems, Bern, Switzerland, 10–13 April 2012; ACM: New York, NY, USA, 2012; pp. 127–140.
48. Riddle, A.R.; Chung, S.M. A survey on the security of hypervisors in cloud computing. In Proceedings of the 2015 IEEE 35th International Conference on Distributed Computing Systems Workshops (ICDCSW), Columbus, OH, USA, 29 June–2 July 2015; pp. 100–104.
49. Studnia, I.; Alata, E.; Deswarte, Y.; Kaâniche, M.; Nicomette, V. Survey of security problems in cloud computing virtual machines. In Proceedings of the C&ESAR 2012 Cloud and Security, Threat or Opportunity: Computer and Electronics Security Applications Rendez-vous; Rennes, France, 20–22 November 2012; pp. 61–74.
50. Li, J.; Li, B.; Wo, T.; Hu, C.; Huai, J.; Liu, L.; Lam, K. CyberGuarder: A virtualization security assurance architecture for green cloud computing. *Future Gener. Comput. Syst.* **2012**, *28*, 379–390. [CrossRef]
51. Almorsy, M.; Grundy, J.; Müller, I. An analysis of the cloud computing security problem. In Proceedings of the 2010 Asia Pacific Software Engineering Conference (APSEC 2010) Cloud Workshop, Sydney, Australia, 30 November–3 December 2010.
52. Vaquero, L.M.; Rodero-Merino, L.; Morán, D. Locking the sky: A survey on IaaS cloud security. *Computing* **2011**, *91*, 93–118. [CrossRef]

53. Wu, H.; Ding, Y.; Winer, C.; Yao, L. Network security for virtual machine in cloud computing. In Proceedings of the 2010 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), Seoul, Korea, 30 November–2 December 2010; pp. 18–21.
54. Schoo, P.; Fusenig, V.; Souza, V.; Melo, M.; Murray, P.; Debar, H.; Medhioub, H.; Zeghlache, D. *Challenges for Cloud Networking Security*; Pentikousis, K., Agüero, R., García-Arranz, M., Papavassiliou, S., Eds.; Mobile Networks and Management; Springer: Berlin/Heidelberg, Germany, 2011; pp. 298–313.
55. Thimmaraju, K.; Shastry, B.; Fiebig, T.; Hetzelt, F.; Seifert, J.P.; Feldmann, A.; Schmid, S. The vAMP Attack: Taking Control of Cloud Systems via the Unified Packet Parser. In Proceedings of the 2017 on Cloud Computing Security Workshop, Dallas, TX, USA, 3 November 2017; ACM: New York, NY, USA, 2017; pp. 11–15. [CrossRef]
56. Lombardi, F.; Di Pietro, R. Secure Virtualization for Cloud Computing. *J. Netw. Comput. Appl.* **2011**, *34*, 1113–1122. [CrossRef]
57. Jiang, X.; Wang, X.; Xu, D. Stealthy Malware Detection Through Vmm-based "Out-of-the-box" Semantic View Reconstruction. In Proceedings of the 14th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 28–31 October 2007; ACM: New York, NY, USA, 2007; pp. 128–138. [CrossRef]
58. Aikat, J.; Akella, A.; Chase, J.S.; Juels, A.; Reiter, M.K.; Ristenpart, T.; Sekar, V.; Swift, M. Rethinking Security in the Era of Cloud Computing. *IEEE Secur. Priv.* **2017**, *15*, 60–69. [CrossRef]
59. Rocha, F.; Gross, T.; Moorsel, V.A. Defense-in-Depth Against Malicious Insiders in the Cloud. In Proceedings of the 2013 IEEE International Conference on Cloud Engineering (IC2E), Redwood City, CA, USA, 25–27 March 2013; pp. 88–97. [CrossRef]
60. Bahram, S.; Jiang, X.; Wang, Z.; Grace, M.; Li, J.; Srinivasan, D.; Rhee, J.; Xu, D. DKSM: Subverting Virtual Machine Introspection for Fun and Profit. In Proceedings of the 2010 29th IEEE Symposium on Reliable Distributed Systems, New Delhi, India, 31 October–3 November 2010; pp. 82–91. [CrossRef]
61. Duncan, A.J.; Creese, S.; Goldsmith, M. Insider attacks in cloud computing. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Liverpool, UK, 25–27 June 2012; pp. 857–862.
62. 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*; ACM: New York, NY, USA, 2009; pp. 91–96. [CrossRef]
63. Balduzzi, M.; Zaddach, J.; Balzarotti, D.; Kirda, E.; Loureiro, S. A Security Analysis of Amazon's Elastic Compute Cloud Service. In Proceedings of the 27th Annual ACM Symposium on Applied Computing, Trento, Italy, 26–30 March 2012; ACM: New York, NY, USA, 2012; pp. 1427–1434. [CrossRef]
64. Modi, C.; Patel, D.; Borisaniya, B.; Patel, H.; Patel, A.; Rajarajan, M. A survey of intrusion detection techniques in cloud. *J. Netw. Comput. Appl.* **2013**, *36*, 42–57. [CrossRef]
65. Aiash, M.; Mapp, G.; Gemikonakli, O. Secure live virtual machines migration: Issues and solutions. In Proceedings of the 2014 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Victoria, BC, Canada, 13–16 May 2014; pp. 160–165.
66. Yeh, J.R.; Hsiao, H.C.; Pang, A.C. Migrant attack: A multi-resource dos attack on cloud virtual machine migration schemes. In Proceedings of the 2016 11th Asia Joint Conference on Information Security (AsiaJCIS), Fukuoka, Japan, 4–5 August 2016; pp. 92–99.
67. Rakotondravony, N.; Taubmann, B.; Mandarawi, W.; Weishäupl, E.; Xu, P.; Kolosnjaji, B.; Protsenko, M.; de Meer, H.; Reiser, H.P. Classifying malware attacks in IaaS cloud environments. *J. Cloud Comput.* **2017**, *6*, 26. [CrossRef]
68. Shetty, J.; Anala, M.R.; Shobha, G. A Survey on Techniques of Secure Live Migration of Virtual Machine. *Int. J. Comput. Appl.* **2012**, *39*, 34–39. [CrossRef]
69. Rodero-Merino, L.; Vaquero, L.M.; Caron, E.; Muresan, A.; Desprez, F. Building safe PaaS clouds: A survey on security in multitenant software platforms. *Comput. Secur.* **2012**, *31*, 96–108. [CrossRef]
70. Linthicum, D.S. PaaS Death Watch? *IEEE Cloud Comput.* **2017**, *4*, 6–9. [CrossRef]
71. Favaretto, M.; Anh, T.T.; Kavaja, J.; De Donno, M.; Dragoni, N. When the Price is Your Privacy: A Security Analysis of Two Cheap IoT Devices. In Proceedings of the 6th International Conference in Software Engineering for Defense Applications, Rome, Italy, 7–8 June 2018; Springer: Berlin/Heidelberg, Germany, 2019.

72. Nakouri, I.; Hamdi, M.; Kim, T.H. A new biometric-based security framework for cloud storage. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; pp. 390–395. [CrossRef]
73. Liang, X.; Shetty, S.; Zhang, L.; Kamhoua, C.; Kwiat, K. Man in the Cloud (MITC) Defender: SGX-Based User Credential Protection for Synchronization Applications in Cloud Computing Platform. In Proceedings of the 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), Honolulu, CA, USA, 25–30 June 2017; pp. 302–309. [CrossRef]
74. Samarati, P.; di Vimercati, S.D.C.; Murugesan, S.; Bojanova, I. Cloud security: Issues and concerns. In *Encyclopedia on Cloud Computing*; John Wiley & Sons: Hoboken, NJ, USA, 2016; pp. 1–14.
75. Zhou, M.; Zhang, R.; Xie, W.; Qian, W.; Zhou, A. Security and privacy in cloud computing: A survey. In Proceedings of the 2010 Sixth International Conference on Semantics Knowledge and Grid (SKG), Beijing, China, 1–3 November 2010; pp. 105–112.
76. Chen, D.; Zhao, H. Data security and privacy protection issues in cloud computing. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), Hangzhou, China, 23–25 March 2012; Volume 1, pp. 647–651.
77. Helland, P. Condos and Clouds. *Commun. ACM* **2013**, *56*, 50–59. [CrossRef]
78. Martins, P.; Sousa, L.; Mariano, A. A survey on fully homomorphic encryption: An engineering perspective. *ACM Comput. Surv. (CSUR)* **2017**, *50*, 83. [CrossRef]
79. Rong, C.; Nguyen, S.T.; Jaatun, M.G. Beyond lightning: A survey on security challenges in cloud computing. *Comput. Electr. Eng.* **2013**, *39*, 47–54. [CrossRef]
80. Ren, K.; Wang, C.; Wang, Q. Security Challenges for the Public Cloud. *IEEE Internet Comput.* **2012**, *16*, 69–73. [CrossRef]
81. di Vimercati, S.D.C.; Foresti, S.; Livraga, G.; Paraboschi, S.; Samarati, P. Confidentiality Protection in Large Databases. In *A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 457–472.
82. Tari, Z. Security and Privacy in Cloud Computing. *IEEE Cloud Comput.* **2014**, *1*, 54–57. [CrossRef]
83. Islam, M.S.; Kuzu, M.; Kantarcioglu, M. Access Pattern disclosure on Searchable Encryption: Ramification, Attack and Mitigation. In Proceedings of the 19th Annual Network and Distributed System Security Symposium, NDSS 2012, San Diego, CA, USA, 5–8 February 2012, The Internet Society. Available online: https://pdfs.semanticscholar.org/9614/87973d4b33f96406fddbfcf1235dc587571f.pdf (accessed on 4 June 2019).
84. Baumann, A.; Peinado, M.; Hunt, G. Shielding applications from an untrusted cloud with haven. *ACM Trans. Comput. Syst. (TOCS)* **2015**, *33*, 8. [CrossRef]
85. Pearson, S. Privacy, security and trust in cloud computing. In *Privacy and Security for Cloud Computing*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 3–42.
86. Jasti, A.; Shah, P.; Nagaraj, R.; Pendse, R. Security in multi-tenancy cloud. In Proceedings of the 44th Annual 2010 IEEE International Carnahan Conference on Security Technology, San Jose, CA, USA, 5–8 October 2010; pp. 35–41. [CrossRef]
87. Tsai, H.Y.; Siebenhaar, M.; Miede, A.; Huang, Y.; Steinmetz, R. Threat as a Service? Virtualization's Impact on Cloud Security. *IT Prof.* **2012**, *14*, 32–37. [CrossRef]
88. Milenkoski, A.; Payne, B.D.; Antunes, N.; Vieira, M.; Kounev, S. HInjector: Injecting hypercall attacks for evaluating VMI-based intrusion detection systems. In Proceedings of the 2013 Annual Computer Security Applications Conference (ACSAC 2013), New Orleans, LA, USA, 9–13 December 2013.
89. Perez-Botero, D.; Szefer, J.; Lee, R.B. Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers. In Proceedings of the 2013 International Workshop on Security in Cloud Computing, Hangzhou, China, 8 May 2013; ACM: New York, NY, USA, 2013; pp. 3–10. [CrossRef]
90. Liao, X.; Alrwais, S.; Yuan, K.; Xing, L.; Wang, X.; Hao, S.; Beyah, R. Lurking Malice in the Cloud: Understanding and Detecting Cloud Repository As a Malicious Service. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; ACM: New York, NY, USA, 2016; pp. 1541–1552. [CrossRef]
91. Wang, C.; Ren, K.; Wang, J. Secure and practical outsourcing of linear programming in cloud computing. In Proceedings of the 2011 Proceedings IEEE INFOCOM, Shanghai, China, 10–15 April 2011; pp. 820–828.
92. Wei, L.; Zhu, H.; Cao, Z.; Dong, X.; Jia, W.; Chen, Y.; Vasilakos, A.V. Security and privacy for storage and computation in cloud computing. *Inf. Sci.* **2014**, *258*, 371–386. [CrossRef]

93. Jensen, M.; Schwenk, J.; Gruschka, N.; Iacono, L.L. On technical security issues in cloud computing. In Proceedings of the IEEE International Conference on Cloud Computing, Bangalore, India, 21–25 September 2009; pp. 109–116.
94. Karnwal, T.; Sivakumar, T.; Aghila, G. A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. In Proceedings of the 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 1–2 March 2012; pp. 1–5.
95. Ahuja, S.P.; Komathukattil, D. A survey of the state of cloud security. *Netw. Commun. Technol.* **2012**, *1*, 66. [CrossRef]
96. Stanislav, M.; Beardsley, T. *Hacking Iot: A Case Study on Baby Monitor Exposures and Vulnerabilities*; Technical Report. Available online: https://www.rapid7.com/ (accessed on 4 June 2019).
97. Cachin, C.; Keidar, I.; Shraer, A. Trusting the Cloud. *SIGACT News* **2009**, *40*, 81–86. [CrossRef]
98. Wang, C.; Wang, Q.; Ren, K.; Cao, N.; Lou, W. Toward secure and dependable storage services in cloud computing. *IEEE Trans. Serv. Comput.* **2012**, *5*, 220–232. [CrossRef]
99. Syam Kumar, P.; Subramanian, R. An efficient and secure protocol for ensuring data storage security in Cloud Computing. *IJCSI Int. J. Comput. Sci. Issues* **2011**, *8*, 261.
100. Zafar, F.; Khan, A.; Malik, S.U.R.; Ahmed, M.; Anjum, A.; Khan, M.I.; Javed, N.; Alam, M.; Jamil, F. A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends. *Comput. Secur.* **2017**, *65*, 29–49. [CrossRef]
101. Varadarajan, V.; Kooburat, T.; Farley, B.; Ristenpart, T.; Swift, M.M. Resource-freeing Attacks: Improve Your Cloud Performance (at Your Neighbor's Expense). In Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, NC, USA, 16–18 October 2012; ACM: New York, NY, USA, 2012; pp. 281–292. [CrossRef]
102. Luo, S.; Lin, Z.; Chen, X.; Yang, Z.; Chen, J. Virtualization security for cloud computing service. In Proceedings of the 2011 International Conference onCloud and Service Computing (CSC), Hong Kong, China, 12–14 December 2011; pp. 174–179.
103. Dabrowsk, C.; Mills, K. VM leakage and orphan control in open-source clouds. In Proceedings of the 2011 IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom), Athens, Greece, 29 November–1 December 2011; pp. 554–559.
104. Zhou, F.; Goel, M.; Desnoyers, P.; Sundaram, R. Scheduler Vulnerabilities and Coordinated Attacks in Cloud Computing. *J. Comput. Secur.* **2013**, *21*, 533–559. [CrossRef]
105. Alarifi, S.; Wolthusen, S.D. Robust Coordination of Cloud-Internal Denial of Service Attacks. In Proceedings of the 2013 International Conference on Cloud and Green Computing, Karlsruhe, Germany, 30 September–2 October 2013; pp. 135–142.[CrossRef]
106. Atya, A.O.F.; Qian, Z.; Krishnamurthy, S.V.; Porta, T.L.; McDaniel, P.; Marvel, L. Malicious co-residency on the cloud: Attacks and defense. In Proceedings of the IEEE INFOCOM 2017—IEEE Conference on Computer Communications, Atlanta, GA, USA, 1–4 May 2017; pp. 1–9. [CrossRef]
107. Moon, S.J.; Sekar, V.; Reiter, M.K. Nomad: Mitigating arbitrary cloud side channels via provider-assisted migration. In Proceedings of the 22nd ACM Sigsac Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015; ACM: New York, NY, USA, 2015; pp. 1595–1606.
108. Atya, A.; Aqil, A.; Khalil, K.; Qian, Z.; Krishnamurthy, S.V.; La Porta, T.F. Stalling Live Migrations on the Cloud. In Proceedings of the 11th USENIX Workshop on Offensive Technologies (WOOT 17), Vancouver, BC, Canada, 14–15 August 2017.
109. Wang, Y.; Ma, J.; Lu, D.; Lu, X.; Zhang, L. From high-availability to collapse: Quantitative analysis of "Cloud-Droplet-Freezing" attack threats to virtual machine migration in cloud computing. *Clust. Comput.* **2014**, *17*, 1369–1381. [CrossRef]
110. Liu, H. A New Form of DOS Attack in a Cloud and Its Avoidance Mechanism. In Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, Chicago, IL, USA, 8 October 2010; ACM: New York, NY, USA, 2010; pp. 65–76. [CrossRef]
111. Somani, G.; Gaur, M.S.; Sanghi, D.; Conti, M.; Buyya, R. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Comput. Commun.* **2017**, *107*, 30–48. [CrossRef]
112. Ficco, M.; Rak, M. Economic Denial of Sustainability Mitigation in Cloud Computing. In *Organizational Innovation and Change*; Rossignoli, C., Gatti, M., Agrifoglio, R., Eds.; Springer International Publishing: Cham, Switerland, 2016; pp. 229–238.

113. Somani, G.; Gaur, M.S.; Sanghi, D. DDoS/EDoS attack in cloud: Affecting everyone out there! In Proceedings of the 8th International Conference on Security of Information and Networks, Sochi, Russia, 8–10 September 2015; ACM: New York, NY, USA, 2015; pp. 169–176.
114. Ficco, M.; Palmieri, F. Introducing fraudulent energy consumption in cloud infrastructures: A new generation of denial-of-service attacks. *IEEE Syst. J.* **2017**, *11*, 460–470. [CrossRef]
115. Coppolino, L.; D'Antonio, S.; Mazzeo, G.; Romano, L. Cloud security: Emerging threats and current solutions. *Comput. Electr. Eng.* **2017**, *59*, 126–140. [CrossRef]
116. Kim, D.; Vouk, M.A. A survey of common security vulnerabilities and corresponding countermeasures for SaaS. In Proceedings of the Globecom Workshops (GC Wkshps), Austin, TX, USA, 8–12 December 2014; pp. 59–63.
117. Gupta, S.; Gupta, B.B. Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. *Int. J. Syst. Assur. Eng. Manag.* **2017**, *8*, 512–530. [CrossRef]
118. Putthacharoen, R.; Bunyatnoparat, P. Protecting cookies from cross site script attacks using dynamic cookies rewriting technique. In Proceedings of the 2011 13th International Conference on Advanced Communication Technology (ICACT), Seoul, Korea, 13–16 February 2011; pp. 1090–1094.
119. Morrow, B. BYOD security challenges: Control and protect your most sensitive data. *Netw. Secur.* **2012**, *2012*, 5–8. [CrossRef]
120. Sood, A.K.; Enbody, R.J. Targeted cyberattacks: A superset of advanced persistent threats. *IEEE Secur. Priv.* **2013**, *11*, 54–61.
121. Chen, P.; Desmet, L.; Huygens, C. A Study on Advanced Persistent Threats. In *Communications and Multimedia Security*; De Decker, B., Zúquete, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; pp. 63–72.
122. Caviglione, L.; Podolski, M.; Mazurczyk, W.; Ianigro, M. Covert Channels in Personal Cloud Storage Services: The Case of Dropbox. *IEEE Trans. Ind. Inform.* **2017**, *13*, 1921–1931. [CrossRef]
123. Xiao, L.; Xu, D.; Xie, C.; Mandayam, N.B.; Poor, H.V. Cloud Storage Defense Against Advanced Persistent Threats: A Prospect Theoretic Study. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 534–544. [CrossRef]
124. Shahriar, H.; Zulkernine, M. Client-side detection of cross-site request forgery attacks. In Proceedings of the 2010 IEEE 21st International Symposium on Software Reliability Engineering (ISSRE), San Jose, CA, USA, 1–4 November 2010; pp. 358–367.
125. Siddiqui, M.S.; Verma, D. Cross site request forgery: A common web application weakness. In Proceedings of the 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), Xi'an, China, 27–29 May 2011; pp. 538–543.
126. Livshits, V.B.; Lam, M.S. Finding Security Vulnerabilities in Java Applications with Static Analysis. In Proceedings of the 14th USENIX Security Symposium, Baltimore, MD, USA, 31 July–5 August 2005.
127. You, P.; Peng, Y.; Liu, W.; Xue, S. Security issues and solutions in cloud computing. In Proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW), Macau, China, 18–21 June 2012; pp. 573–577.
128. Chapade, S.; Pandey, K.; Bhade, D. Securing cloud servers against flooding based DDoS attacks. In Proceedings of the 2013 International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 6–8 April 2013; pp. 524–528.
129. Zargar, S.T.; Joshi, J.; Tipper, D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 2046–2069. [CrossRef]
130. De Donno, M.; Dragoni, N.; Giaretta, A.; Spognardi, A. Analysis of DDoS-capable IoT malwares. In Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, Prague, Czech Republic, 3–6 September 2017.
131. Badis, H.; Doyen, G.; Khatoun, R. Understanding botclouds from a system perspective: A principal component analysis. In Proceedings of the 2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, 5–9 May 2014; pp. 1–9.
132. Yan, Q.; Yu, F.R.; Gong, Q.; Li, J. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 602–622. [CrossRef]
133. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and Other Botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]

134. Osanaiye, O.; Choo, K.K.R.; Dlodlo, M. Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. *J. Netw. Comput. Appl.* **2016**, *67*, 147–165. [CrossRef]
135. Dantas, Y.G.; Nigam, V.; Fonseca, I.E. A Selective Defense for Application Layer DDoS Attacks. In Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference, The Hague, The Netherlands, 24–26 September 2014; pp. 75–82. [CrossRef]
136. Jensen, M.; Gruschka, N.; Herkenhöner, R. A survey of attacks on web services. *Comput. Sci. Res. Dev.* **2009**, *24*, 185. [CrossRef]
137. Singh, K.; Singh, P.; Kumar, K. Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges. *Comput. Secur.* **2017**, *65*, 344–372. [CrossRef]
138. Choi, J.; Choi, C.; Ko, B.; Kim, P. A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment. *Soft Comput.* **2014**, *18*, 1697–1703. [CrossRef]
139. Zhao, Y.; Liu, Y.; Yu, Y.; Li, Y. Blockchain based Privacy-Preserving Software Updates with Proof-of-Delivery for Internet of Things. *arXiv* **2019**, arXiv:1902.03712.
140. Yu, Y.; Li, Y.; Tian, J.; Liu, J. Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. *IEEE Wirel. Commun.* **2018**, *25*, 12–18. [CrossRef]
141. Rullo, A.; Bertino, E.; Saccà, D. PAST: Protocol-Adaptable Security Tool for Heterogeneous IoT Ecosystems. In Proceedings of the IEEE Conference on Dependable and Secure Computing, DSC 2018, Kaohsiung, Taiwan, 10–13 December 2018; pp. 1–8.
142. Giura, P.; Jim, T. Sapphire: Using Network Gateways for IoT Security. In Proceedings of the 8th International Conference on the Internet of Things, Santa Barbara, CA, USA, 15–18 October 2018; ACM: New York, NY, USA, 2018; pp. 5:1–5:8.
143. Kong, Q.; Lu, R.; Ma, M.; Bao, H. A privacy-preserving sensory data sharing scheme in Internet of Vehicles. *Future Gener. Comp. Syst.* **2019**, *92*, 644–655. [CrossRef]
144. Fazio, M.; Ranjan, R.; Girolami, M.; Taheri, J.; Dustdar, S.; Villari, M. A Note on the Convergence of IoT, Edge, and Cloud Computing in Smart Cities. *IEEE Cloud Comput.* **2018**, *5*, 22–24. [CrossRef]
145. Dragoni, N.; Massacci, F.; Saidane, A. A Self-protecting and Self-healing Framework for Negotiating Services and Trust in Autonomic Communication Systems. *Comput. Netw.* **2009**, *53*, 1628–1648. [CrossRef]
146. Guidi, C.; Lanese, I.; Mazzara, M.; Montesi, F. Microservices: A Language-Based Approach. In *Present and Ulterior Software Engineering*; Mazzara, M., Meyer, B., Eds.; Springer International Publishing: Cham, Switerland, 2017; pp. 217–225.
147. Yan, Z.; Cimpian, E.; Zaremba, M.; Mazzara, M. BPMO: Semantic Business Process Modeling and WSMO Extension. In Proceedings of the 2007 IEEE International Conference on Web Services (ICWS 2007), Salt Lake City, UT, USA, 9–13 July 2007; pp. 1185–1186.
148. Mazzara, M. Towards Abstractions for Web Services Composition. Ph.D. Thesis, University of Bologna, Bologna, Italy, 2006.
149. Dragoni, N.; Mazzara, M. *A Formal Semantics for the WS-BPEL Recovery Framework—The pi-Calculus Way*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2009; Volume 6194, pp. 92–109.