Cloud Computing Security: A Survey on Service-based Models

Article *in* Computers & Security · December 2021

DOI: 10.1016/j.cose.2021.102580

Fatemeh Khoda Parast
University of New Brunswick

Hadis Yekta
University of New Brunswick

Kenneth B. Kent
University of New Brunswick

Cloud Computing Security: A Survey of Service-based Models

Fatemeh Khoda Parast*, Chandni Sindhav†, Seema Nikam‡ , Hadiseh Izadi Yekta§, Kenneth B. Kent¶, and Saqib Hakak‖
fkhoda@unb.ca*, csindhav@unb.ca†, snikam@unb.ca‡, hizadi@unb.ca§, ken@unb.ca¶, shakak@unb.ca‖
Faculty of Computer Science , University of New Brunswick, Canada

Abstract—Cloud computing has recently attracted significant attention due to its economical and high-quality services. In the last decade, cloud services have inevitably entangled with business's and individuals' daily lives through products and services. On-demand, pay-per-use characteristics, encourage corporations to outsource part of their businesses to accelerate their services and multiply value. The latest market tendency toward migration to cloud environments, started in 2019, indicates a flourishing trend in the next few years. Despite the numerous benefits of the cloud computing model for businesses or individuals, security issues still have been stated as the top cloud challenge in 2020. Although various factors affect security, technologies enabling cloud computing such as virtualization and multitenancy, in addition to on-demand characteristics, initiate new security entrances for malevolent activities. In this study, we surveyed service-based cloud computing security issues to establish the current state of the field. The main contribution of this paper is to analyze the state of cloud security in the last decade and provide a unified taxonomy of security issues over the three-layer model, i.e., IaaS, PaaS, and SaaS.

Index Terms—Security, Cloud Computing, Service-based Cloud Computing, IaaS, PaaS , SaaS

1 Introduction

Cloud computing has received notable attention, providing *flexibility*, *scalability*, *reliability*, *sustainability*, and *affordability* [1], [2]. The pillar concept of the cloud, pay-per-use, has attracted not only individuals but businesses to benefit from the new approach to make profits [3]–[5]. According to a survey conducted in 2020 among 750 global cloud professionals [6], due to the COVID-19 impact, organizations will spend 47% more on cloud services in 2021 alone. Top growing cloud service consumers, i.e., IoT, machine learning/AI, data warehouse, and serverless markets will grow 47.2% on average [7]. Although tech giants such as *Google*, *Microsoft*, and *IBM* compete to provide the best solutions to users, the field still requires more research on security solutions [8]–[10].

Despite the obvious benefits of cloud computing, the complexity of the model and shared technologies have given rise to security concerns [6], [11]. The diversity of involved elements in the cloud paradigm, i.e., network, architecture, APIs, and hardware, increases the intricacy of security issues [12]. As a result, a cloud provider or client would encounter security vulnerabilities caused by a different combination of a cloud configuration [13]. The *National Institute of Standards and Technology (NIST)* has introduced the service-based model as a standard for cloud computing. This model includes *Infrastructure-as-a-Service (IaaS)*, *Platform-as-a-Service (PaaS)*, and *Software-as-a-Service (SaaS)* defining all IT sharable resources such as software, hardware, or network [14], [15].

The **Multitenancy**, **Elasticity**, and **Deployment** model raises important security implications [16]. Multitenancy allows Cloud Service Providers (CSP)s to share resources among numerous customers. Through this feature, several users coexist in a single instance of a physical device at the same time, increasing the probability of Virtual Machine (VM) or Hypervisor (HV) attacks. Elasticity provides a scaling up/down capability for increasing/decreasing resources [17], [18]. Once a user requires fewer resources, those would be allocated to another customer as needed. In such cases, the previous user's data might still exist in the allocated location, which opens up security issues [19], [20]. In addition to the cloud computing enabling technology, the availability of resources creates a perfect environment for intruders to apply attacks to other systems. Attackers have the opportunity to execute multiple penetration tests targeting known vulnerabilities to find VMs' security holes via low-priced services [21]. The administration of layers defines the other important factor in the security of service-based cloud computing. Non-uniform management in a layer creates multiple vulnerability entry points and exposes the system to more threats [3], [8].

In this study, we focus on the service-based cloud computing security concerns to analyze the current state of the field and classify them into a service-based taxonomy. The main contributions of this paper can be noted as follows.

1) Recent state-of-the-art service-based cloud vulnerabilities are presented.
2) A taxonomy of service-based cloud vulnerabilities and countermeasures is proposed.
3) Research challenges and future research directions are explored.
4) A classification of vulnerabilities & countermeasures is established.
5) Generic security issues in the service-based model have been identified and enumerated.

The rest of the article is organised as follows: Section 2 describes background concepts of the field. The status of the current research is presented in Section 3. Current research challenges and future research directions are discussed in Sections 4 and 5. The article presents the future and conclusions in Sections 6 and 7.

2 Cloud Computing Overview

NIST addresses cloud security concerns according to three main categories, *service-based model*, *deployment model*, and *characteristics* [3]. Regarding the focus of this study, an overview of the service-based model technologies and concepts is discussed in this section.

2.1 Cloud Computing Enabling Technologies

The existence of cloud computing has been possible only in the presence of essential concepts such as *virtualization*, *multitenancy*, and *Service Oriented Architecture (SOA)*. These techniques implement resource sharing among users from a physical instance [22], [23].

2.1.1 Virtualization

Virtualization defines an abstract approach to create a computer, enabling resource partitioning in the cloud environment. Sharing resources becomes feasible with the help of a *VM*, via a file generally known as an image, which either can be produced by users or achieved from external sources [24], [25]. In practice, any sharable IT resources could be virtualized to provide multi-user access to one resource instance. Desktop, network, storage, data, application, CPU, and cloud virtualization are the most adopted forms of virtualization. Cloud virtualization embodies IaaS, PaaS, and SaaS models, which implies resource virtualization [26]–[28]. Figure 1 presents an abstract model of the service-based cloud computing environment. In this model, physical resources are allocated to numerous users of different layers with the help of a hypervisor through virtualization.

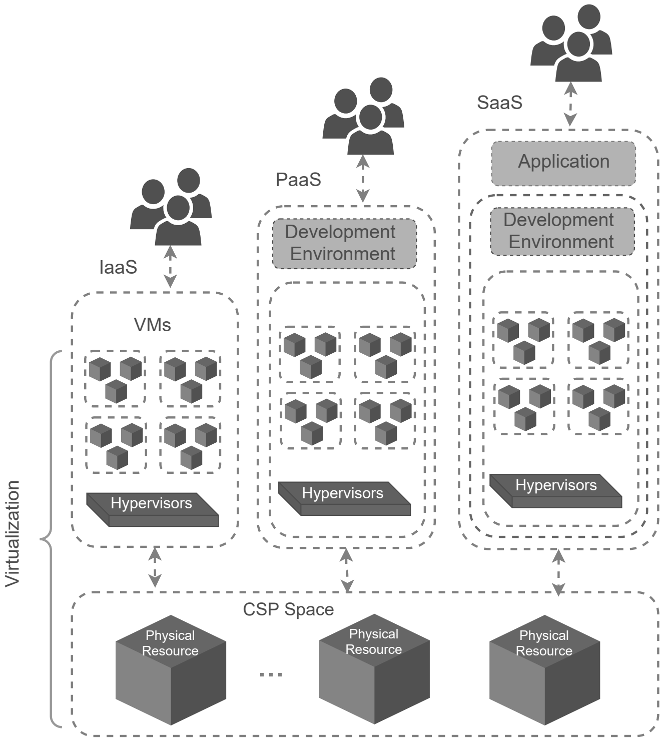

Fig. 1: Abstraction of Multitenancy by Virtualization in Service-based Cloud Environments

2.1.2 Hypervisor

A hypervisor (HV) or *Virtual Machine Monitor (VMM)* in the cloud environment behaves relatively similar to the OS in a system. As a software layer between physical hardware and VMs, it coordinates the various VMs and assures them of receiving requested resources [25], [29]. Having numerous VMs altogether at the same time on one machine becomes possible with the HV technology. The most accepted HV classification has been defined as the two type model, the *bare-metal* and *hosted* types. The former type operates directly on the bare hardware, e.g., Xen, and ESX, while the second type runs as an application on the host OS, e.g., KVM, QEMU, and VirtualBox. As a result of direct resource communication, the latency of the latter type decreases remarkably. While the high-performance capability makes bare-metal HVs a great option in a cloud environment, the root privileges turn them into an excellent target for security attacks [30]. CSPs such as Amazon AWS[1] offer various types of virtualizations such as paravirtual (PV) and hardware VM (HVM) that would be mapped

[1] https://docs.aws.amazon.com

into the hosted and bare-metal HV. Figure 1 depicts a bare metal HV in which the HV directly translates user VM commands to the hardware and there is no need for the host OS.

2.1.3 Multitenancy

Multitenancy defines a software architecture helping several customers to access one instance of software simultaneously. In this technique, multiple VMs located in a server use the same physical entities to service end-users. A *Service-Oriented Architecture (SOA)* utilizes several mediatory technologies, e.g., *HTTP* and *Simple Object Access Protocol (SOAP)*, to provide the promised services to multiple customers. Figure 1 depicts a possible resource virtualization leading to the pictured multitenancy scenario. In multitenancy, physical instances such as CPU and Memory are divided into sharable elements, through virtualization, and allocated to different clients. The simultaneous access to one instance would degrade the shared resource performance on the one hand but maximizes resource usage on the other hand. In theory, isolated user-space would prevent security issues such as data leakage; however, that is not the case in real-world scenarios, and more vulnerabilities would be introduced to the cloud paradigm as a result of this technology [8], [24].

2.1.4 Service Oriented Architecture

Service-Oriented Architecture (SOA) defines a reusable software development methodology in which components are loosely coupled to enhance interoperability and reusability. Undependability of services improves development agility and makes the SOA pattern a proper fit for new computation environments such as service-based cloud computing. In this model, target functionalities are provided through service interfaces. Services are typically defined through Web Service Definition Language (WSDL) standards and exhibited through SOAP or Representational State Transfer (REST) network protocols. This model of software development involves numerous benefits. A user needs the minimum amount of information to utilize the interface due to the loosely coupled components. The language of the provider could be different from the consumer, which increases undependability [26], [31].

2.2 Service-based Cloud Computing

Providing economical high-quality services to users defines the main goal of the cloud computing paradigm. These services can be any sharable IT resources such as hardware, software, or network [14], [15]. IaaS, PaaS, and SaaS define three famous service-based cloud models that make the cost-effectiveness, availability, and scalability of these services popular for mid-size to large businesses [26].

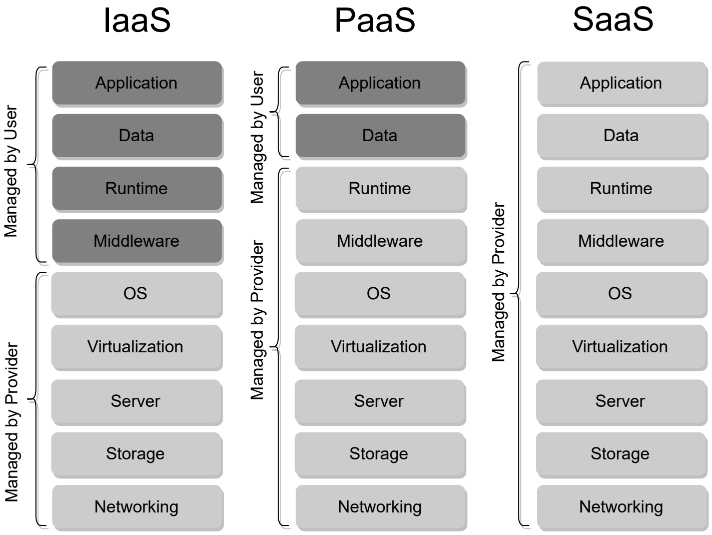

Fig. 2: Resource Management in IPS Model [26]

2.2.1 Infrastructure-as-a-Service

IaaS defines all computational resources in a virtual environment such as networking, data storage, servers, virtualization, and OS to facilitate remote services for clients. A user then can access the presented services through APIs via the internet. A company can rent all required IT resources to build a software ecosystem on a pay-per-use basis subscription. Amazon EC2 (Elastic Compute Cloud) represents an example of the IaaS providers. In this environment, users have a higher level of flexibility in terms of having numerous VMs simultaneously. In IaaS, a user can deploy a private or public image, which is a template to configure a VM. Private images are configured by users while public images are published by an external source such as a company or an open-source organization. The architecture of IaaS might be different from that depicted in Figure 2 based on a client desired model. In the *hosted HV* the VM OS operates on the host OS, which means the CSP manages the host OS, and the user governs the VM OS. The bare metal HV type, on the other hand, can be directly executed on the hardware that eliminates the need for the host OS [26], [32], [33].

2.2.2 Platform-as-a-Service

PaaS incorporates a cloud-based development environment with all required resources through the web medium. Normally, programming languages, IDEs, databases, web servers, and OS are accessible through shared resources so that a developer can produce a program free from the lower layer dependencies [34], [35]. In this model, services are accessible through a Graphical User Interface (GUI) via the internet.

All *IaaS* layers plus *middleware* and *runtime* constitute the *PaaS* concept. Amazon web services and Windows Azure are two examples of the *PaaS* model [36], [37]. A software development team would find the required technologies for all software lifecycles, e.g., design, implementation, test, version control, and continuous integration and delivery in the PaaS model.

2.2.3 Software-as-a-Service

SaaS is a combination of all *IaaS* and *PaaS* layers in addition to *data* and *application* panels that supply on-demand application services such as email, word processors, and design applications to the end-users. In this model, a client utilizes an application located in a remote cloud environment through a single instance of the application allowing several customers to execute the software simultaneously. In this model, all software stack and hardware components are provided and managed by CSP, and a user utilizes the ready-to-use application by an annual/monthly payment. The subscription model is beneficial for both providers and users. Clients pay less than a licensing model, and providers would have more clients as the software is more affordable. Google, Microsoft and Amazon are pioneers who provide such services, e.g., Google drives, Microsoft 365, and Amazon AWS [38]–[40].

2.3 Cloud Computing Management

Management specifies the other important concept in the service-based cloud computing. In a common classification schema, a cloud computing architecture is divided into nine layers, *networking*, *storage*, *servers*, *virtualization*, *OS*, *middleware*, *runtime*, *data*, and *application*. Management of layers might be granted to a user or CSP according to the service model [1]. In IaaS, the management of networking, storage, server, virtualization, and OS are assigned to the CSP and a customer manages middleware, runtime, data, and application. In the PaaS, a user only controls the data and application layer, and the CSP oversees the other layers. In SaaS, all layers of the cloud are administrated by the vendors and the consumer has limited administration authority of an application [41]. Figure 2 illustrates a general resource management without any assumptions in the service-based cloud model. It is worth noting that in real-world scenarios, the management of layers might differ according to the users' desired configurations. As discussed in virtualization 2.1.1 and HV 2.1.2, regarding the type, the architecture and as a result, the management of layers might change, respectively [27], [28].

2.4 Deployment Model

The deployment model defines the access exclusivity of the shared resources. A *public* cloud provides services to any user through the internet, whereas the *private* cloud computing model grants exclusive resource access to an organization. In this model, the administration could be either operated by the CSP or a customer. Likewise, the infrastructure could be located in the CSP location or out-sourced to a third-party private host [42]. A *community* model presents cloud services to a group of customers with common concerns, such as security. The administration and resource access are similar to the private model; however, a consumer could access other organizations' services through the organization. A *hybrid* model describes a combination of two or more deployment models [3].

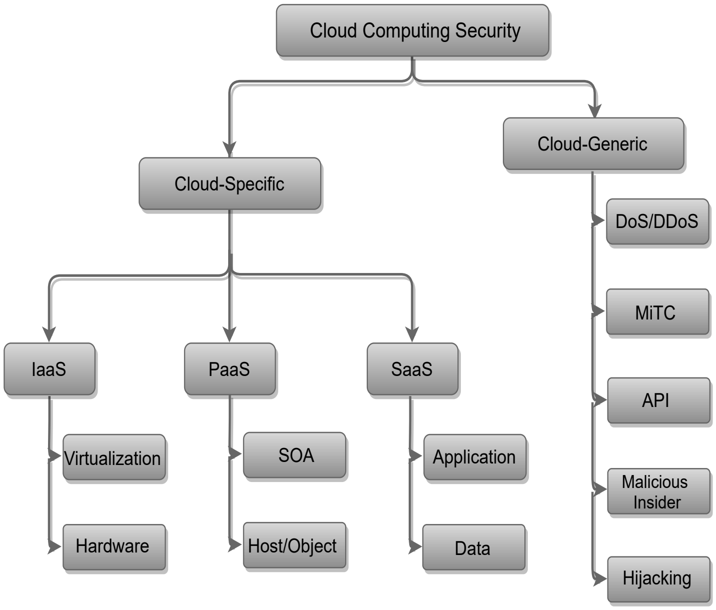

Fig. 3: Cloud Computing Security Taxonomy

3 Recent Advances in Cloud Computing Security

Researchers have studied cloud computing security issues from various viewpoints; however, *virtualization*, *multitenancy*, *data security*, and *general* vulnerabilities are the most discussed topics in the literature. Table 1 summarizes the current status of surveys in the community. In this study, we propose a security taxonomy based on the aforementioned security concerns. In this taxonomy, vulnerabilities are generalized into two primary classes as *cloud-specific* and *cloud-generic*. The former discusses service-based specific security concerns, i.e., *IaaS*, *PaaS*, and *SaaS*. The latter addresses common security issues regardless of the layer. Figure 3 illustrates the proposed taxonomy.

3.1 Cloud-Specific

The cloud computing paradigm becomes possible only in the presence of enabling technologies and concepts, such as virtualization and multi-

Table 1
Current Status of Surveys in Cloud Computing Security (Sorted by Year)

Reference	Focused Topic	IaaS	PaaS	SaaS	Generic	Countermeasure	Year
Subashini et al. [43]	Data Security	✓	✓	✓	✗	✓	2011
Vaquero et al. [32]	Multitenancy	✓	✗	✗	✗	✗	2011
Verma et al. [23]	General	✓	✓	✓	✓	✗	2011
Hashizume et al. [44]	General	✓	✓	✓	✗	✓	2013
Modi et al. [14]	Availability, confidentiality and integrity of cloud resources	✓	✓	✓	✗	✓	2013
Kim et al. [42]	General	✗	✗	✓	✗	✓	2014
Fernandes et al. [45]	General	✗	✗	✗	✓	✓	2014
Huang et al. [15]	Compare industry best-practices with academia solutions	✓	✗	✗	✗	✓	2015
Chouhan et al. [46]	Effect of data & application security in SaaS architecture	✗	✓	✗	✗	✗	2015
Khan [47]	General	✗	✗	✗	✓	✓	2016
Singh et al. [48]	General	✗	✗	✗	✓	✓	2016
Liu et al. [49]	General	✓	✓	✓	✗	✗	2016
Almorsy et al. [19]	Cloud architecture, stakeholder, and characteristic	✓	✓	✓	✗	✗	2016
Singh et al. [50]	General	✓	✓	✓	✓	✓	2017
Chawki et al. [51]	CSP & user behaviour	✓	✗	✗	✗	✗	2018
Basu et al. [52]	Virtualization & data	✓	✓	✓	✗	✓	2018
Kumar et al. [8]	Big Data, IoT, software defined network, & function virtualization	✓	✓	✓	✗	✗	2019
Guerbouj et al. [53]	IoT and Cloud of Things (CoT)	✗	✗	✗	✓	✓	2019
Nadiah [54]	Virtualization	✓	✗	✗	✗	✓	2019
Agarwal et al. [55]	Cryptography technique	✓	✓	✓	✗	✓	2020
Tabrizchi et al. [24]	General	✗	✗	✗	✓	✓	2020
Isharufe et al. [56]	General	✓	✗	✗	✗	✗	2020
Shyam et al. [57]	Software defined networking	✗	✗	✓	✗	✗	2021
Panda et al. [58]	General	✓	✓	✓	✗	✗	2021

tenancy. The service-based models, IaaS, PaaS, and SaaS apply various techniques to provide services to the target customers. However, each technology might introduce a new security vulnerability to the cloud ecosystem. In this section, the most addressed security vulnerabilities and countermeasures in the literature are presented.

3.1.1 IaaS

The virtualized physical hardware is presented as a service to customers in the IaaS model. In this layer, the most common security issues are established around the virtualization concept. VM image, virtual network, HV, and hardware define top vulnerabilities in this layer [59]. Table 2, presents a summary of vulnerabilities over the IaaS layer in addition to an associated countermeasure.

3.1.1.1 Virtualization

VM images are files including important information such as VM configurations and logs, a well-known target of attacks. Image alteration by code injection and information theft encompass some examples of image template vulnerabilities [19]. Gonzales et al. [60] analyzed four IaaS architectures with different security configurations. The architecture with a series of encryption, access control, signature policy, and isolation is introduced as the most robust model. In this model, although VM images are protected through encryption mechanisms, still VM vulnerabilities such as VM CPU timing, side-channel attack, VM attack through the HV, disk injection to live VM, etc., threaten the system. A Bayesian network approach has been proposed to mitigate the mentioned vulnerabilities. In this approach, a network from elements located in a trusted zone is produced and the probability of an attack is calculated from the network paths [60].

Zhang et al. [21] analyzed Amazon Machine Images (AMIs) security vulnerabilities on the AWS EC2. The established model calculates the risk-gain value of a vulnerability through tactical-game modelling in the system. In this model, an earlier reaction to an attack acquires more reward. The study revealed that more than 50% of VM vulnerabilities are related to the Ubuntu OS that makes the attack scenario easier for intruders. Having a misconfigured VM image increases the chance of a DoS attack. Maintaining all instances up-to-date is recommended as a feasible countermeasure, which defines a difficult obligation in practice. However, patching public VM images, maintaining running instances, giving patching priority to prevalent vulnerabilities, and shuffling cloud infrastructure smartly are introduced as more applicable solutions for mitigating VM image vulnerabilities.

Huang et al. [15] elaborated on IaaS security analysis from a stakeholder perspective. Malicious activities are categorized into CSP and user attacks. The CSP can monitor and manipulate storage, VM image, HV, and Service Level Agreement (SLA). In contrast, the user would cause cache-based or general leakage channels. Users of the public cloud services should trust the CSP to protect their data from other clients. This approach has led to new threats on confidentiality, integrity, and data availability that can be caused by malicious CSP or other clients. Contractual security is a new security property of customers specific to the cloud business model that attackers are interested in. Dedicating a VM is proposed as a solution for cross-VM leakage and cloud-side encryption issues to protect the message confidentiality in this layer [65].

VM escape denotes a vulnerability allowing an attacker in a VM to bypass the hypervisor to interact with the host OS to obtain root privilege. HyperSafe, Trusted Cloud Computing Platform (TCCP) and Trusted Virtual Datacenter (TVD) are introduced as three countermeasures of the VM escape problem. HyperSafe prevents hypervisor bypassing by preventing write-protected memory changes. TCCP provides an isolated execution environment. In this model, there exists a Trusted Third Party (TTP) that maintains a Trusted Coordinator (TC) and a Trusted Virtual Machine Monitor (TVMM). In the TVD approach, virtual machines are divided into groups with a common interest. Then, the intragroup communications are protected through secure channels [44].

The HV incorporates the multitenancy concept in the shared environment. The high privilege ability of HV vulnerates it as a target for intruders. If attackers penetrate an HV, they can execute any type of attack such as kernel structure manipulation and rootkit. Trusted Platform Module (TPM) is a hardware security solution that utilizes hardware capabilities to assure the security of the components. The technology applies the BIOS signature mechanism for secure boot time. Modern hardware processors are equipped with a crypto chip assuring secure boot time that prevents HV tampering. The processor can verify the software boot-time information through a series of assessments on the chip [60].

Mazhar et.al. [66] outlined the security concerns mainly related to the third-party service providers. The primary security issues related to third-party CSPs are the points that emerge due to the virtualization, multitenancy, and shared resource pool. Although the research in this context essentially focuses on the communication and architectural perspectives, the virtual network demands more attention. Even though virtual devices were presented to secure the virtual network, a comprehensive, well-planned design is required to regulate or monitor the traffic to prevent information leakage. Shared technologies such as virtualization, HV, and VMs have generated new security gates for adversaries. Rewriting the packets could be a solution for VM security matters, maintaining a balance between privacy and monitoring. The tamper-proof key management makes trusted computing a good candidate for providing a comprehensive security solution in cloud computing [67]. SLA specifies a countermeasure for virtualization and multitenancy; however, having the whole benefit of the solution depends on the CSP's policy. Google and Microsoft are some examples of CSPs who are reluctant to reveal all required information of SLA transparency [68].

3.1.1.2 Hardware

Cryptography mechanisms are applied to increase the security level of data in the transit and storage process. Despite the mechanism in place, data should be decrypted for process purposes at some point. The multitenancy feature of the cloud facilitates access to storage mediums such as disk, memory, and cache. Intruders located in a shared host with a victim can access the plain value of the key, or any form of confidential data in the storage mediums. Cache-based side-channel attacks, a family of cross-VM side-channel vulnerabilities, denotes a form of the mentioned concerns. Another argument with the cloud-based services is the access limitation of upper layer users to the lower layers. Intel is working on the Software Guard Extension (SGX) technology that provides a protected memory area to run an application called an enclave. In the secure enclaves, even privileged software such as the OS has no right to access the protected area [63].

3.1.2 PaaS

In this layer, all required services are provided to customers for deployment purposes via an SOA model. Resource sharing via multitenancy and an SOA increases the risk of numerous security issues [59]. Table

Table 2
IaaS Security Countermeasures

Vulnerability	Threat	Countermeasures	Definition	References
Virtualization	VM escape	HyperSafe	An approach to prevent hypervisor bypassing through preventing write-protected pages alteration	[44]
	VM escape	TCCP	Trusted cloud computing platform provides an isolated execution environment through a trusted third party	[44]
	VM escape	TVD	Trusted virtual data center divides VMs into groups with common interests and limits communication between them through secure channels	[44]
	Vulnerable VM image	Patching public images	Establish policies to keep public VM images up-to-date, either by CSP, provider, or user	[21]
	Cross-VM side-channel attack	MetaMORP(h)OSY	Is a thermal behaviour analysis tool that evaluates run-time thermal status	[61]
	Network virtualization	VM mapping	Hanging a VM to the related host by devoted physical channels	[51]
	Cross VM leakage	Dedicated instances	Normally used by large scale businesses as a resource is entirely allocated to a customer	[15]
	HV DoS	Isolation	Isolating the security monitoring VM from guest VMs	[62]
	HV tampering	TPM attestation, patch HV	Trusted platform module is a secure co-processor on the motherboard of a computer system for signing a measurement	[15]
Hardware	Cache-based side-channel attack	S-Box access	Turn off cache S-Box access, avoid lookup table, and perform cache warming	[63]
	Cache-based side-channel attack	SGX & ARM Trust-Zone	Intel software guard extension provides a hardware base solution to isolate an application's memory access	[63]
	Information leakage	PC, PLC	Partitioned cache divides cache into protected sections and allocates it to a process. In partition-locked cache, a fine-grained locking mechanism is in place for isolating only a line of cache	[63]
	XML attack	XML signature and encryption	An approach for creating a XML signature via an XML syntax	[64]

3, presents a summary of vulnerabilities over the PaaS layer in addition to an associated countermeasure.

3.1.2.1 SOA

Resource sharing raises serious issues in the presence of a conflict of interest to customers. A possible scenario is the colocation of two competitors in a single host. The *Chinese Wall Model* mitigates the accidental or intentional access to shared resources by dividing users into conflict of interest groups and allocating physical resources accordingly [69]. Arora et al. [64] propose a combination of policies, monitoring, and restrictions as the solution for multitenancy and virtualization. *SLA* represents one of the policies determining the advantages and liabilities of each participant. *Secure Configuration Policy (SCP)* describes another policy that guarantees a secure configuration in the hardware/software layer or SLA configuration.

Freet et al. [72] investigated the digital forensic security challenges in the service-based cloud environment. In this paradigm, processing power, data storage, and other shared resources rely on the IaaS layer. In a common shared resource environment, the data packets of the VM traverse in all possible ways via a host machine. Although each VM is separated from other VMs on an actual device, any undermined VM can assault another VM in the organization. Additionally, any misconfiguration of an HV results in a DoS attack as it permits one VM to utilize all framework assets against other VMs on a shared environment. Whatever changes in the configuration and settings from a malicious user in the PaaS layer can influence the whole cloud architecture. As PaaS has a service-oriented architecture, the primary security challenges are XML-related, DoS, injection, and MiTC attacks in this layer.

Rodero et al. [70] discuss two popular programming language technologies in the PaaS paradigm, i.e., Java, and .Net, in terms of multitenancy subjects. According to experimental results, Java and .NET do not offer a fully secured hosting setting. More specifically, a detailed analysis of the security features over the *Enterprise Java Bean (EJB)* and *Open Service Gateway Initiative (OSGi)* were conducted to evaluate the security of the most prominent Java containers in the cloud domain. In this study, *isolation*, *resource accounting*, and *safe thread termination* are proposed as a remedy for the multitenancy technology vulnerabilities. Java supports isolation through JVM technologies, i.e., EJB container and servlet, whereas the .Net platform facilitates the isolation through Common Language Runtime (CLR) profiling. Google App Engine (GAE), as a Java-based cloud engine, applies another approach for isolation. In a GAE, each entity resides in an isolated VM and has restricted access to resources.

3.1.2.2 Vulnerable Host/Object

In a shared environment, customers' objects are threatened by multiple elements, i.e., other tenants, hosts, and external attackers. The combined *Trusted Computing Base (TCB)* is normally applied as a solution for vulnerable objects and lack of interoperability for intra-API communications [73]. A model including four practices is proposed to address vulnerable objects. *Transport Layer Security (TLS)*, *Sticky Access Control Policy (SACP)*, *Policy Enforcement Points (PEPs)*, and *Undeniable Logging Protocol (ULP)* constitute the model. The well-known network protocol, TLS, delivers secure communication through a cryptography mechanism. The SACP and PEP deploy a fine-grained object-based access control and ULP assures the authenticity of the logging system [71]. Interoperability defines the fundamental concept enabling cloud paradigm, APIs, and platforms to communicate together but is recognized as a PaaS vulnerability. A TCB provides a solution for vulnerable hosts and lack of interoperability. An encryption layer can be added to protect against exposed objects in the proposed method [74].

3.1.3 SaaS

Built on top of two layers, SaaS inherits security issues of lower layers. In addition, dependence on web APIs makes the model vulnerable to web technology security issues [59]. Table 4 presents a summary of vulnerabilities over the SaaS layer in addition to the associated countermeasures.

3.1.3.1 Application

In the OWASP project, web technology vulnerabilities have been studied and the top ten are introduced. Broken authentication, injection, XML External Entities (XXE), broken access control, sensitive data exposure, security misconfiguration, insecure deserialization, cross-site scripting (XSS), and insufficient logging and monitoring define part of web API concerns [75].

Chouhan et al. [46] classify SaaS security issues into three main categories, data, application, and deployment. Data security includes security of data in storage, transit, backup, recovery, integrity, and access control. The delivery of SaaS services strongly depends on web technologies and concepts. Software design flow, user interface and technologies, web services, and malware define application security points. Design and implementation of a web application include front-end and back-end languages, libraries, and dependencies such as HTML, JavaScript, PHP, Java, Python, SOAP, etc. Normally, a design might not cover all security aspects and introduces subsequent vulnerabilities into the system.

Grobauer et al. [76] reviewed the security subjects of the core cloud computing technologies and their characteristics. Vulnerabilities are divided into the following categories, core technologies, essential cloud characteristics, prevalent security concerns, defects in known security controls, and architectural components. The authentication topic has been introduced as the primary vulnerability of the cloud system that compromises user data. As the SaaS layer communicates directly with the end-users through web APIs, the layer is vulnerable

Table 3
PaaS Security Countermeasures

Vulnerability	Threat	Countermeasures	Definition	References
SOA	Shared resource	Chinese wall model	An approach to allocate physical resources according to class of customers	[69]
	Resource starvation	Resource accounting	Applying tools such as Java VM tooling interface (JVMTI) to limit resource access	[70]
	Information leakage	Safe thread termination	A thread should be properly terminated to prevent leakage of information in a thread related to a user	[70]
Vulnerable Host/Object	Vulnerable object	TCB	Trusted computing base is a secure layer over the OS to cope with the lack of interoperability	[71]

to web technology security issues such as authorization, access control, and session hijacking. Each cloud environment must have strong mechanisms and protocols to control identity, authentication, authorization, and auditing. The cryptographic algorithms are counted as a remedy for a majority of security issues. A secure channel through cryptography highly alleviates the hijacking threat.

3.1.3.2 Data

Data security is an important issue in all layers of the cloud; however, SaaS users totally rely on CSP to protect any breaches of credential information either in transit or in storage. Hashizume et al. [44] discussed three countermeasures to address the data breach problem, Fragmentation-Redundancy-Scattering (FRS), digital signatures, and homomorphic encryption. FRS splits primary data into parts with little meaningful information and propagates the parts across the whole system in a redundant way. In the digital signature approach, the RSA algorithm is applied to verify data authenticity after transit through the network. Homomorphic algorithms are applied to messages that are manipulated in an encrypted format. Depending on the goal of a system, one or a combination of the aforementioned approaches would be a solution for protection against a data breach.

Data vulnerabilities in this layer can be mitigated by protocols such as Secure Socket Layer (SSL) and TLS. The protocols create a secure channel between a client and server to establish an end to end secure communication. HTTP examination is another solution to enhance data issues. To this end, a web application scanner examines the HTTP requests and responses regularly to provide log files via read only APIs through a central log server [72].

3.2 Cloud-Generic Vulnerabilities

Cloud computing embodies network technologies that comprise inherited security issues such as TCP/IP communication vulnerabilities [77]. In this model, a layer would have specific and generic security concerns. The former arises due to applied technology in a layer such as virtualization in IaaS, the latter can be either for the network or common cloud-based issues in all layers [63]. Table 5 presents a summary of cloud generic vulnerabilities in addition to associated countermeasures.

3.2.1 DoS/DDoS

In Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks, the attacker exploits a TCP vulnerability to cause resource starvation for a legitimate user. In the cloud paradigm, VMs are exposed to DoS attacks due to the insufficient bandwidth under-provisioning issue. A series of papers propose solutions to mitigate this attack [64], [78].

SYN cookie analysis and connection limitation outline a series of solutions to prevent DoS attacks. In SYN flow analysis, a sequence of synchronization messages are communicated between client and server. In the SYN flood attack, the attacker initiates the handshaking for synchronization, but never completes it entirely. To prevent this type of DoS attack, the server never waits for an acknowledgement. The handshaking process will be completed once the SYN-ACK is correctly received. By this approach, the server is never occupied with the incomplete synchronization mechanism required for a TCP connection. The other DoS attack is applied by holding resources busy through open connections. This type of attack is normally prevented by limiting connections from a client with the same IP address [63].

DoS/DDoS attacks can be detected by thermal behaviour analysis. MetaMORP(h)OSy is a formal massive object-based profiler for the

Table 4
SaaS Security Countermeasures

Vulnerability	Threat	Countermeasures	Definition	References
Application	Unauthorized access	IAAA	A cloud service must have a strong identity, authentication, authorization, and auditing control mechanism	[76]
	Web API security	Isolation	Isolating transactions in memory to limit data access of tenants located in the same instance	[59]
Data	Data breach	FRS	FRS technique splits data into low informative parts and propagates them in the whole system in a redundant way	[44]
	Data breach	Digital signature	A cryptographic approach, normally using RSA algorithm, to confirm authenticity of data after transit	[44]
	Data breach	Homomorphic encryption	A cryptographic approach that provides process over encrypted context	[44]
	Data recovery	Cryptography	Cryptography and strong key management mechanisms help to mitigate user-related data recovery	[76]
	Data alteration	SSL/TLS	SSL and TLS create a secure tunnel between a client and server making a communication end to end secure	[72]
	Data vulnerability	HTTP examination	A web application scanner examines HTTP requests and responses, and provides log files via read only APIs through a central log server	[72]
	Data breach	Cryptography	Applying cryptographic algorithm and facilitates data storage backup	[51]

real-time behaviour modelling of a software system. The profiler can be extended to examine thermal requirements and behaviours. Formal models are adopted to determine strange actions, verify functional and non-functional properties at the early stage, and implement monitoring at run-time. MetaMORP(h)OSY produces an *observer* at runtime for evaluating thermal properties. The observer monitors central interfaces and thermal regions on a remote system to find any differences between expected and normal thermal behaviour, the monitor evaluates new process parameters in small time fractions [61].

3.2.2 MiTC

Man-in-The-Cloud (MiTC) attack determines the second important vulnerability in the generic category. In this threat, the intruder commences with collecting information from the web to target a victim, once detecting vulnerabilities such as open ports or unprotected servers, the attacker performs a malicious activity. Therefore, a series of operations is recommended to mitigate the probability of MiTC [64]. Probes should be prevented through strongly configured firewalls and IDSs and critical data should be hidden. Closing non-essential ports and preventing routing bypass through any mechanism. In addition, the current recommendations are beneficial in DoS attack prevention [78].

3.2.3 API

API denotes the key concept of the cloud ecosystem for communication. Although this feature facilitates a convenient way of information transmission it raises security concerns. A lack of interoperability would lead to a serious issue if a well-defined policy is not already in place [71]. To prevent malicious activity such as eavesdropping or alteration, the customer can benefit from a central server log system that captures all activities. Then, the log file is stored signed and encrypted to prevent alteration [72].

Ishare et al. [56] address PaaS security issues due to cloud features, i.e., *on-demand self-service*, *broad network access*, *resource pooling*, *rapid elasticity*, and *measured service*. On-demand self-service capa-

Table 5
Cloud-Generic Security Countermeasures

Vulnerability	Countermeasures	Definition	References
DoS	Filtering	Ingress filtering assures that an IP matches with a domain prefix, otherwise it will be dropped	[63]
	SYN analysis	Prevent incompleted TCP handshake synchronization (SYN) processes	[63]
	Connection limit	Limiting connection numbers from one IP address	[63]
	MetaMORP(h)OSY	Thermal behaviour evaluation as a formal massive object-based profiler for the real-time modelling behaviour of a software system	[61]
MiTC	A series of predictive steps	Activate firewall and IDS, disable ping, conceal sensitive information, close unused ports	[78]
API	Central log server	Deploy a central log server, equipped with encryption and signature to prevent eavesdropping of files or any alterations	[72]
	SAML & MFA	Multi factor authentication for authentication, and security assertion markup language for transfering user credentials purposes	[56]
	Shibboleth	Shibboleth is an open-source middleware software that applies the SAML standard to guarantee proper authentication and authorization.	[9]
Malicious insider	Bayesian network	Statistical approach for finding the attack path	[60]
	DAC, MAC	Discretionary and mandatory access control, applied to the OS for access control restriction	[63]
	Agreement and breach notifications	Using agreement reporting and breach notifications besides transparent security and management policies	[51]
Hijacking	Two factor authentication	Using a secondary device or approach for authentication purposes	[51]
	Dynamic credential	A parameter based credential change approach, it can be sensitive to user location, or TCP/IP changes	[44]
	PDP	Provable data possession is a cryptography approach that regularly checks server activity on data	[79]
	NIDS	Applying an erasure code technique in network-based intrusion detection system to recognize vulnerabilities and fix them simultaneously	[51]

bility is provided through an API to customers. As recommended, the CSP should utilize a Multi-factor Authentication (MFA) mechanism to ensure the identity of the user and the confidential data should be transferred through a secure system such as the latest version of Security Assertion Markup Language (SAML).

Zissis et al. [9] analyzed authentication and authorization as two important processes in an information system. Authentication verifies user identity versus authorization defines the level of access to either hardware or software resources. Shibboleth is open-source middleware software that applies SAML standards to guarantee proper authentication and authorization. Shibboleth implies a Single Sign-On (SSO) standard that relies on a third-party mediation [9].

3.2.4 Malicious Insider

A malicious insider in the cloud computing environment can be a CSP employee who misuses his/her access privileges in a nefarious way. Discretionary Access Control (DAC) and Mandatory Access Control (MAC) introduce two approaches for preventing such vulnerabilities [22]. Both methods are applied to the OS to restrict access through strict permission policies. MAC is stated as the proper access restriction mechanism for the cloud environment due to the higher level of security. AppArmor in Linux and TrustedBSD in the Mac OS are examples of the MAC approach [63].

Kamongi et al. [80] proposed a framework for evaluating the security vulnerabilities of the Cloud Computing System (CCS) named *VULCAN*, a comprehensive security assessment via a *Natural Language Processing (NLP)* method and *ontology reasoning*. The framework benefits from the *Ontology Vulnerability Database (OVDB)* and *National Vulnerabilities Database (NVD)* repositories to identify known security issues or new patterns. The framework indexes all possible vulnerabilities based on the script of NVD and OVDB. Then, a cloud-based system should be tested for any security concerns. The VULCAN framework functions similar to a classifier in which all vulnerabilities are categorized and labelled into some groups. When a vulnerability is reached, the framework will mark that new instance as one of the known categories based on the vulnerability features. Gonzales et al. [60] applied a Bayesian network to find the malicious insider paths. The primary purpose of finding the attack path is to understand the vulnerability level of the information system to derive probabilistic standards of enterprise network security. The proposed approach has been extended to the CCSs by constructing an acyclic directed graph through the attack paths. This approach attempts to consider the contributions of specific CCS security features in reducing the vulnerabilities of elements in a CCS to reduce the overall security profile of an IaaS cloud.

3.2.5 Hijacking

Account or service hijacking is the theft of user credential data allowing further malicious activities. Proper identity and access management policies help in mitigating the issue. Dynamic credentials are a recommended countermeasure for hijacking. This method changes the secret values based on predefined parameters such as user location or received packages [44].

Khan et al. [81] present current and future privacy and security arguments by interviewing cloud developers, providers, and IT managers. A vulnerability might originate from a misconfiguration or improper action in various layers or stages. Finding the source of the issue helps in detecting and preventing hijacking. The result of the study shows that weak credentials and improper authorization validations are typical causes that lead to an account or service hijacking. Inappropriate data handling in transit, processing and storage by an untrusted third party would cause data leakage. Insecure third-party APIs increase the DoS attack probability. By cross-site scripting or SQL injection, attackers can manipulate user data. An unprotected virtual machine increases the virtual network sniffing/spoofing attack probability.

In account or service hijacking, the attacker steals credential information so that they can exploit the system. As the cloud paradigm opens new entry points for the intruders, hijacking can be operated from either layer. Two-factor authentication, Provable Data Possession (PDP), Network-based Intrusion Detection Systems (NIDS), and cryptography algorithms are a group of solutions to mitigate the account or session hijacking threats [79]. In two-factor authentication, normally a secondary device is involved to validate the user authenticity. Whereas the PDP, defines a public key-based method to verify the manipulated data by a server, NIDS apply the erasure codes method for intrusion detection [51].

4 Challenges

The cloud computing paradigm provides numerous benefits for businesses and individuals. However, applied technologies and complex architectures raise challenges that need to be addressed. Regarding the scope of the current study, we have discussed IaaS, PaaS, SaaS, and generic security challenges.

4.1 IaaS Security Challenges

According to the literature, lower layers' vulnerabilities have the most destructive effect on the whole system. That means, if a security issue initiates in the IaaS layer, that would propagate to the upper layers and endanger the whole system. Due to the access restriction to lower layers, the customer has few chances to apply an appropriate security countermeasure [44]. Virtualization and multitenancy are the top security concerns in this layer. The virtualization in the IaaS environment would cause associated security issues such as DoS and cross-VM side-channel attacks due to the bandwidth under-provisioning issues or co-location VM escape [51].

VM images in an IaaS model includes potential vulnerabilities. In this environment, the user can use a public or private image to configure VMs. Public images are published with outer providers such as individuals, open-source communities, or IT companies. Only in Amazon EC2, a user can apply more than 6000 public images. Regarding the result of a current study on public images, they have the potential of backdoors as providers might forget to remove keys or other critical information properly [21].

Stability of network configurations create a conventional attack surface for intruders. In the IaaS layer, normally the range of IP addresses is more predictable and stable compared to the traditional computing model. In addition, non-cloud machines might utilize firewalls or another protective mechanism. The heterogeneous environment of the cloud makes it easier for an intruder to exploit security holes [21].

4.2 PaaS Security Challenges

Lock-in defines a PaaS problematic concern. The PaaS paradigm provides a development environment for a software developer to enjoy extensible software and hardware resources for developing a product. As there is no unified standard for all vendors, the *lock-in* issue threatens PaaS customers. Lock-in happens once the customer requires services that are not available in the primary vendor environment [82]. To this end, the customer should migrate to another provider or host facility. However, the migration to other vendor servers is highly inefficient in terms of budget or time for the customer. Therefore, there would be a lock-in condition for PaaS customers who should decide between staying in a vendor with limitations or accept the cost of migration [64].

The **SOA** model enables PaaS customers to deploy their application or software in a shared environment. Although the model provides numerous benefits, it limits access to the lower layer, making it difficult for a PaaS customer to apply security tools. Therefore, the primary configuration makes the system vulnerable to MiTC, DoS, injection, and XML-related attacks. However, the PaaS API should necessarily include high security standards for service delivery to the upper layer customers [72].

4.3 SaaS Security Challenges

Multitenancy facilitates a cheaper service either for a provider or end-user. In some cases, users should only pay-as-you-go, while in others they might receive free services such as Google Docs. This concept supports the coexistence of numerous users in a single instance of software/hardware at the same time. In this environment, data management would become a challenging affair. Preserving data locality, integrity, confidentiality, segregation, and backup would become difficult to manage as several users will be using the same system.

Web API defines the SaaS delivery model to final customers that exposes the method to various web technology security flaws. Therefore, lack of a proper policy could lead to severe security or privacy problems such as access to user data in a common area in the presence of multitenancy and data leakage in a shared database system [32].

Control limitation explains another main challenge since a user has no control over the application, OS, and middleware in the SaaS cloud. All services are controlled by the CSP and users can access only the rented application from the CSP. This limitation intuitively means that a customer has no access to the log files or any system for monitoring or alteration for applying or improving security policies.

4.4 Cloud-Generic Security Challenges

Patching software regularly reduces all layer security concerns. Despite the provided taxonomy, we realize that the late patching process of software was mentioned as a potential vulnerability. By releasing on-time patching, software providers reduce the risk of various security issues. On the other side, users that ignore new updates would face the same consequences [21].

Cost-effectiveness of a cloud environment is not only a beneficial concept for users but also intruders. Having inexpensive machines makes the penetration test easier for attackers. Intruders can benefit from this concept to exploit cloud customers [21].

Lack of interoperability explains a potential security issue of APIs. Interoperability means the ability to communicate between different components or platforms of a system in a compatible way that normally is operated through an API. There are various scenarios underlying this ability such as migration from one CSP to another, or upgrading services in a CSP or customer side [83].

Internet protocol is associated with known security flaws such as DoS, DDoS, MiTC, and account or service hijacking. All aforementioned vulnerabilities can be operated from all layers. However, according to the PaaS architecture model, intruders tend to operate the attack scenario in this layer more than others [59].

Malicious insiders is a known security issue that needs more attention. According to Bouayad et al. [59], more than 70% of attacks are related to the company's human resources. Although products such as SGX can help us to make some progress in this direction, it still demands greater efforts [63].

5 Discussion

In the literature review DoS/DDoS, session hijacking and shared technologies are the top three discussed security concerns in the cloud computing environment [55], [85]. According to the research results, scalability is one of the core cloud characteristics, such that a user can request more resources based on a given workload. That means, on

Table 6
Top Security Threats in Service-Based Cloud Computing Environments

Vulnerability	Description	Research
DoS/DDoS	DoS attack, prevents a legitimate user from achieving desired resources. Normally, the attacker occupies all resources such as network bandwidth up to the maximum capacity.	[63] [78] [81] [62] [72] [61] [51] [64]
Shared technology	Shared technologies such as virtualization facilitate cloud computing model. The attacker tries to obtain control of VMs through the HV, which has root privilege.	[84] [70] [63] [81] [62] [60]
Session hijacking	In this attack, the attacker obtains a user's credentials by staying in a TCP/IP communication. As a result, the attacker can access user's resources, and steal their identity and sensitive data.	[76] [84] [81] [72] [51] [56]
Multitenancy	Multitenancy is the result of virtualization technology in a cloud platform. It permits coexistence of multiple users in one physical resource instance through VMs.	[19] [62] [59] [70]
VM side channel	In this attack, the attacker locates a malicious VM in the target host to collect cryptography algorithm information that allows the attack to occur in cipher texts.	[60] [62] [56] [51]
MiTC	In a cloud environment, a synchronization token is used for access to user data. Utilizing a malware, the attacker alters the token to access the required info. Having a successful implementation, the attacker has data access from any machine.	[59] [72] [56] [51]
Malicious insiders	In this attack, one of the CSP employees accesses confidential data and utilizes collected information in a malicious way. This attack defines one of the most dangerous vulnerabilities.	[63] [84] [51]
Data breach	The possibility of data leakage increases in the cloud environment. Shared technologies and multitenancy are some examples of cloud technologies that raise the data breach probability.	[63] [81]

one hand, a cloud system provides scalability to users, on the other hand, it supports inexpensive resources for intruders and attackers to target other systems [63], [86]. The second most discussed issue is the shared technology that makes the cloud so fascinating and is also a point of criticality in terms of security [63]. In a shared environment, if attackers succeed in compromising the HV, they can take control over the host system due to the HV root privilege. Apart from this, a session hijacking vulnerability is also in the top three issues in the cloud where a legitimate host can lose control over its own system, allowing intruders to compromise security requirements such as confidentiality, availability, and integrity of the deployed services in the host system. Table 6 depicts top security concerns in the literature. The results indicate that the lower layer vulnerability is more important and malicious insiders are one of the unexplored issues in the cloud system. The main contribution of this study is to provide a detailed understanding of the security vulnerabilities in the service-based cloud model. Moreover, previous studies have discussed countermeasures or vulnerabilities separately, which is fairly difficult to identify the solution for a particular vulnerability. That is why our result describes a classified table that has been produced to provide a pair of security countermeasure information.

6 Future Research Directions

Based on our literature search, most studies analyzed IaaS and SaaS security issues and there is limited research on PaaS vulnerabilities. Unfortunately, those limited number of studies poorly address countermeasures or a framework to solve security flaws. It intuitively implies either the model is less popular among others, or it has fewer known vulnerabilities in the community. However, according to the current software development trend, study over the security concerns of this layer requires more effort.

6.1 Transparent Policy Compliance

The cloud computing model suffers from a lack of coherent policies in terms of security and service compatibility. Vendors have no integrated instructions either for security policies or service delivery constraints. As discussed, the *lock-in* issue for PaaS customers arises due to the mentioned limitations of the model. Working on a universal security schema in the cloud platform is an essential future direction that necessarily improves the service quality and security status [82].

6.2 Cloud-based Hardware Security Concerns

Well-known companies, such as Intel, are working on hardware-level protection concepts such as the aforementioned technology, SGX;

however, these technologies are still experimental and need more investigations. In addition, most of them are deployable in the traditional computing model. Cloud-based hardware is still developing and requires more research and enhancement efforts [63].

6.3 Exploiting Vulnerabilities in Virtualization Technologies

The other important finding of this study is that the literature is focused on the vulnerabilities of virtualization technologies. That is obviously due to the importance of the concept in the service-based cloud computing model. Although virtualization stands among well-studied vulnerabilities, in current research exploration, it was difficult to find a study investigating all possible scenarios. Virtualization is mainly classified into four categories as discussed. However, comprehensive surveys of virtualization vulnerabilities over class types were scarce in the literature. In the future, investigating the different security aspects of one vulnerability regarding various scenarios would add value in this context. The results of such investigations would help both CSPs and users to employ best practices.

7 Conclusion

Our research studied the last decade of service-based cloud computing security issues through a comprehensive analysis of high-quality published papers. This study aims to provide a summary of the current research status and establish a taxonomy that maps vulnerabilities to proper countermeasures. To this end, security vulnerabilities were categorized into four classes, IaaS, PaaS, SaaS, and generic. The first three classes discuss common issues in a layer, while the generic category address vulnerabilities possible in all layers. Although the security concerns have more varieties, we tried to summarize the most discussed topics in the literature.

According to the research results, DoS/DDoS, shared technology, and session hijacking were among the most addressed issues. As has been presented, DoS/DDoS attacks were the most frequent concern in the literature. A series of vulnerabilities are common network security issues that arise due to the medium of the cloud, such as DoS and MiTC. While others, e.g., multitenancy, are cloud-specific groups. As studies show, common issues would be a concern for more study regardless of purposes, service model, or architecture. The complexity of cloud architectures, in addition to service diversity and user configurations, could initiate new security threats. Currently, the variety of cloud services has increased to address any form of user requirements. Although it provides more flexibility, new security holes might be introduced for malicious activities. In the literature, most vulnerabilities are discussed in the general configuration or the traditional structure; however, both providers and customers need to be more conscious of risks and challenges associated with individual decided compositions.

Acknowledgment

Authors Khoda Parast and Kent would like to acknowledge the financial support of the Lockheed Martin Cybersecurity Research Fund, mitacs and the Natural Sciences and Engineering Research Council (NSERC) for their research contributions to this paper. In addition, we would like to express special appreciation to Stephen MacKay for his professional guidance in improving the quality of the current research document. The authors thanks the anonymous reviewers for their insightful comments and constructive suggestions.

References

[1] B. Varghese and R. Buyya, “Next generation cloud computing: New trends and research directions,” *CoRR*, vol. abs/1707.07452, 2017. [Online]. Available: http://arxiv.org/abs/1707.07452

[2] T. Vasiljeva, S. Shaikhulina, and K. Kreslins, “Cloud computing: business perspectives, benefits and challenges for small and medium enterprises (case of latvia),” *Procedia Engineering*, vol. 178, pp. 443–451, 2017.

[3] R. B. Bohn, J. Messina, F. Liu, J. Tong, and J. Mao, “NIST cloud computing reference architecture,” in *World Congress on Services, SERVICES 2011, Washington, DC, USA, July 4-9, 2011*. IEEE Computer Society, 2011, pp. 594–596. [Online]. Available: https://doi.org/10.1109/SERVICES.2011.105

[4] S. Becker, G. Brataas, M. Cecowski, D. Huljenic, S. Lehrig, and I. Stupar, “Introduction,” in *Engineering Scalable, Elastic, and Cost-Efficient Cloud Computing Applications - The CloudScale Method*, S. Becker, G. Brataas, and S. Lehrig, Eds. Springer, 2017, pp. 3–21. [Online]. Available: https://doi.org/10.1007/978-3-319-54286-7_1

[5] J. Weinman, “The economics of pay-per-use pricing,” *IEEE Cloud Comput.*, vol. 5, no. 5, p. 101, 2018. [Online]. Available: https://doi.org/10.1109/MCC.2018.053711671

[6] Flexera, “Flexera 2020 state of the cloud report,” *Applied Computing and Informatics*, 2020.

[7] M. Bahrami and M. Singhal, “DCCSOA: A dynamic cloud computing service-oriented architecture,” in *2015 IEEE International Conference on Information Reuse and Integration, IRI 2015, San Francisco, CA, USA, August 13-15, 2015*. IEEE Computer Society, 2015, pp. 158–165. [Online]. Available: https://doi.org/10.1109/IRI.2015.33

[8] R. Kumar and R. Goyal, “On cloud security requirements, threats, vulnerabilities and countermeasures: A survey,” *Comput. Sci. Rev.*, vol. 33, pp. 1–48, 2019. [Online]. Available: https://doi.org/10.1016/j.cosrev.2019.05.002

[9] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” *Future Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012. [Online]. Available: https://doi.org/10.1016/j.future.2010.12.006

[10] A. Kaur, G. Raj, S. Yadav, and T. Choudhury, “Performance evaluation of aws and ibm cloud platforms for security mechanism,” in *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)*. IEEE, 2018, pp. 516–520.

[11] V. Rajaraman, “Cloud computing,” *Resonance*, vol. 19, no. 3, pp. 242–258, 2014.

[12] V. R. Pancholi and B. P. Patel, “Enhancement of cloud computing security with secure data storage using aes,” *International Journal for Innovative Research in Science and Technology*, vol. 2, no. 9, pp. 18–21, 2016.

[13] M. Ghobaei-Arani, S. Jabbehdari, and M. A. Pourmina, “An autonomic resource provisioning approach for service-based cloud applications: A hybrid approach,” *Future Gener. Comput. Syst.*, vol. 78, pp. 191–210, 2018. [Online]. Available: https://doi.org/10.1016/j.future.2017.02.022

[14] C. Modi, D. R. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of cloud computing," *J. Supercomput.*, vol. 63, no. 2, pp. 561–592, 2013. [Online]. Available: https://doi.org/10.1007/s11227-012-0831-5

[15] W. Huang, A. Ganjali, B. H. Kim, S. Oh, and D. Lie, "The state of public infrastructure-as-a-service cloud security," *ACM Comput. Surv.*, vol. 47, no. 4, pp. 68:1–68:31, 2015. [Online]. Available: https://doi.org/10.1145/2767181

[16] K. Hwang, X. Bai, Y. Shi, M. Li, W. Chen, and Y. Wu, "Cloud performance modeling with benchmark evaluation of elastic scaling strategies," *IEEE Trans. Parallel Distributed Syst.*, vol. 27, no. 1, pp. 130–143, 2016. [Online]. Available: https://doi.org/10.1109/TPDS.2015.2398438

[17] K. e Rubab, T. Azhar, M. Anwar, and S. Majeed, "Security threats in cloud computing: Trend and challenges," *International Journal of Computing and Communication Networks*, vol. 2, no. 1, pp. 29–35, 2020.

[18] T. Diaby and B. B. Rad, "Cloud computing: a review of the concepts and deployment models," *International Journal of Information Technology and Computer Science*, vol. 9, no. 6, pp. 50–58, 2017.

[19] M. Almorsy, J. C. Grundy, and I. Müller, "An analysis of the cloud computing security problem," *CoRR*, vol. abs/1609.01107, 2016. [Online]. Available: http://arxiv.org/abs/1609.01107

[20] D. George Amalarethinam and S. Rajakumari, "A survey on security challenges in cloud computing," 2019.

[21] S. Zhang, X. Zhang, and X. Ou, "After we knew it: empirical study and modeling of cost-effectiveness of exploiting prevalent known vulnerabilities across iaas cloud," in *9th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '14, Kyoto, Japan - June 03 - 06, 2014*, S. Moriai, T. Jaeger, and K. Sakurai, Eds. ACM, 2014, pp. 317–328. [Online]. Available: https://doi.org/10.1145/2590296.2590300

[22] S. Sengupta, V. S. Kaulgud, and V. S. Sharma, "Cloud computing security-trends and research directions," in *World Congress on Services, SERVICES 2011, Washington, DC, USA, July 4-9, 2011*. IEEE Computer Society, 2011, pp. 524–531. [Online]. Available: https://doi.org/10.1109/SERVICES.2011.20

[23] A. Verma and S. Kaushal, "Cloud computing security issues and challenges: A survey," in *Advances in Computing and Communications - First International Conference, ACC 2011, Kochi, India, July 22-24, 2011, Proceedings, Part IV*, ser. Communications in Computer and Information Science, A. Abraham, J. L. Mauri, J. F. Buford, J. Suzuki, and S. M. Thampi, Eds., vol. 193. Springer, 2011, pp. 445–454. [Online]. Available: https://doi.org/10.1007/978-3-642-22726-4_46

[24] H. Tabrizchi and M. K. Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," *J. Supercomput.*, vol. 76, no. 12, pp. 9493–9532, 2020. [Online]. Available: https://doi.org/10.1007/s11227-020-03213-1

[25] J. P. Barrowclough and R. Asif, "Securing cloud hypervisors: A survey of the threats, vulnerabilities, and countermeasures," *Secur. Commun. Networks*, vol. 2018, pp. 1 681 908:1–1 681 908:20, 2018. [Online]. Available: https://doi.org/10.1155/2018/1681908

[26] IBM Cloud Education, "Iaas vs. paas vs. saas, understand and compare the three most popular cloud computing service models," 2021. [Online]. Available: https://www.ibm.com/cloud/learn/iaas-paas-saas

[27] A. Rashid and A. Chaturvedi, "Virtualization and its role in cloud computing environment," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 4, pp. 1131–1136, 2019.

[28] M. I. Malik, S. H. Wani, and A. Rashid, "Cloud computing-technologies." *International Journal of Advanced Research in Computer Science*, vol. 9, no. 2, 2018.

[29] B. Asvija, R. Eswari, and M. B. Bijoy, "Security in hardware assisted virtualization for cloud computing - state of the art issues and challenges," *Comput. Networks*, vol. 151, pp. 68–92, 2019. [Online]. Available: https://doi.org/10.1016/j.comnet.2019.01.013

[30] E. Bauman, G. Ayoade, and Z. Lin, "A survey on hypervisor-based monitoring: Approaches, applications, and evolutions," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 10:1–10:33, 2015. [Online]. Available: https://doi.org/10.1145/2775111

[31] S. Wang, Z. Liu, Q. Sun, H. Zou, and F. Yang, "Towards an accurate evaluation of quality of cloud service in service-oriented cloud computing," *J. Intell. Manuf.*, vol. 25, no. 2, pp. 283–291, 2014. [Online]. Available: https://doi.org/10.1007/s10845-012-0661-6

[32] L. M. Vaquero, L. Rodero-Merino, and D. Morán, "Locking the sky: a survey on iaas cloud security," *Computing*, vol. 91, no. 1, pp. 93–118, 2011. [Online]. Available: https://doi.org/10.1007/s00607-010-0140-x

[33] A. H. Shaikh and B. Meshram, "Security issues in cloud computing," in *Intelligent Computing and Networking*. Springer, 2020, pp. 63–77.

[34] M. Bach-Nutman, "Understanding the top 10 OWASP vulnerabilities," *CoRR*, vol. abs/2012.09960, 2020. [Online]. Available: https://arxiv.org/abs/2012.09960

[35] V. V. H. Pham, X. Liu, X. Zheng, M. Fu, S. V. Deshpande, W. Xia, R. Zhou, and M. Abdelrazek, "Paas - black or white: an investigation into software development model for building retail industry saas," in *Proceedings of the 39th International Conference on Software Engineering, ICSE 2017, Buenos Aires, Argentina, May 20-28, 2017 - Companion Volume*, S. Uchitel, A. Orso, and M. P. Robillard, Eds. IEEE Computer Society, 2017, pp. 285–287. [Online]. Available: https://doi.org/10.1109/ICSE-C.2017.57

[36] A. Singh *et al.*, "Security concerns and countermeasures in cloud computing: a qualitative analysis," *International Journal of Information Technology*, vol. 11, no. 4, pp. 683–690, 2019.

[37] T. R. Toraskar and Y. Borse, "Implementation of cloud computing service delivery models (iaas, paas) by aws and microsoft azure: A survey," *International Journal of Computer Applications*, vol. 975, p. 8887, 2018.

[38] B. Cook, "Formal reasoning about the security of amazon web services," in *Computer Aided Verification - 30th International Conference, CAV 2018, Held as Part of the Federated Logic Conference, FloC 2018, Oxford, UK, July 14-17, 2018, Proceedings, Part I*, ser. Lecture Notes in Computer Science, H. Chockler and G. Weissenbacher, Eds., vol. 10981. Springer, 2018, pp. 38–47. [Online]. Available: https://doi.org/10.1007/978-3-319-96145-3_3

[39] X. Li, L. Zhou, Y. Shi, and Y. Guo, "A trusted computing environment model in cloud architecture," in *International Conference on Machine Learning and Cybernetics, ICMLC 2010, Qingdao, China, July 11-14, 2010, Proceedings*. IEEE, 2010, pp. 2843–2848. [Online]. Available: https://doi.org/10.1109/ICMLC.2010.5580769

[40] E. N. Loukis, M. Janssen, and I. Mintchev, "Determinants of software-as-a-service benefits and impact on firm performance," *Decis. Support Syst.*, vol. 117, pp. 38–47, 2019. [Online]. Available: https://doi.org/10.1016/j.dss.2018.12.005

[41] S. S. Manvi and G. K. Shyam, "Resource management for infrastructure as a service (iaas) in cloud computing: A survey," *J. Netw. Comput. Appl.*, vol. 41, pp. 424–440, 2014. [Online]. Available: https://doi.org/10.1016/j.jnca.2013.10.004

[42] D. Kim and M. A. Vouk, "A survey of common security vulnerabilities and corresponding countermeasures for saas," in *2014 IEEE GLOBECOM Workshops, Austin, TX, USA, December 8-12, 2014*. IEEE, 2014, pp. 59–63. [Online]. Available: https://doi.org/10.1109/GLOCOMW.2014.7063386

[43] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011. [Online]. Available: https://doi.org/10.1016/j.jnca.2010.07.006

[44] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernández, "An analysis of security issues for cloud computing," *J. Internet Serv. Appl.*, vol. 4, no. 1, pp. 5:1–5:13, 2013. [Online]. Available: https://doi.org/10.1186/1869-0238-4-5

[45] D. A. B. Fernandes, L. F. B. Soares, J. V. P. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: a survey," *Int. J. Inf. Sec.*, vol. 13, no. 2, pp. 113–170, 2014. [Online]. Available: https://doi.org/10.1007/s10207-013-0208-7

[46] P. K. Chouhan, F. Yao, and S. Sezer, "Software as a service: Understanding security issues," in *2015 science and information conference (sai)*. IEEE, 2015, pp. 162–170.

[47] M. A. Khan, "A survey of security issues for cloud computing," *J. Netw. Comput. Appl.*, vol. 71, pp. 11–29, 2016. [Online]. Available: https://doi.org/10.1016/j.jnca.2016.05.010

[48] S. Singh, Y. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *J. Netw. Comput. Appl.*, vol. 75, pp. 200–222, 2016. [Online]. Available: https://doi.org/10.1016/j.jnca.2016.09.002

[49] Y. Liu, Y. L. Sun, J. Ryoo, S. Rizvi, and A. V. Vasilakos, "A survey of security and privacy challenges in cloud computing: Solutions and future directions," *J. Comput. Sci. Eng.*, vol. 9, no. 3, 2015. [Online]. Available: https://doi.org/10.5626/JCSE.2015.9.3.119

[50] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *J. Netw. Comput. Appl.*, vol. 79, pp. 88–115, 2017. [Online]. Available: https://doi.org/10.1016/j.jnca.2016.11.027

[51] E. B. Chawki, A. Ahmed, and T. Zakariae, "Iaas cloud model security issues on behalf cloud provider and user security behaviors," in *The 15th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2018) / The 13th International Conference on Future Networks and Communications (FNC-2018) / Affiliated Workshops, Gran Canaria, Spain, August 13-15, 2018*, ser. Procedia Computer Science, A. Yasar and E. M. Shakshuki, Eds., vol. 134. Elsevier, 2018, pp. 328–333. [Online]. Available: https://doi.org/10.1016/j.procs.2018.07.180

[52] S. Basu, A. Bardhan, K. Gupta, P. Saha, M. Pal, M. Bose, K. Basu, S. Chaudhury, and P. Sarkar, "Cloud computing security challenges & solutions-a survey," in *IEEE 8th Annual Computing and Communication Workshop and Conference, CCWC 2018, Las Vegas, NV, USA, January 8-10, 2018*. IEEE, 2018, pp. 347–356. [Online]. Available: https://doi.org/10.1109/CCWC.2018.8301700

[53] S. S. E. Guerbouj, H. Gharsellaoui, and S. Bouamama, "A comprehensive survey on privacy and security issues in cloud computing, internet of things and cloud of things," *Int. J. Serv. Sci. Manag. Eng. Technol.*, vol. 10, no. 3, pp. 32–44, 2019. [Online]. Available: https://doi.org/10.4018/IJSSMET.2019070103

[54] N. M. Almutairy, "A taxonomy of virtualization security issues in cloud computing environments," *Indian Journal of Science and Technology*, 2019.

[55] V. Agarwal, A. K. Kaushal, and L. Chouhan, "A survey on cloud computing security issues and cryptographic techniques," in *Social Networking and Computational Intelligence*. Springer, 2020, pp. 119–134.

[56] W. Isharufe, F. Jaafar, and S. Butakov, "Study of security issues in platform-as-a-service (paas) cloud model," in *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*. IEEE, 2020, pp. 1–6.

[57] G. K. Shyam and R. S. S. Theja, "A survey on resolving security issues in saas through software defined networks," *Int. J. Grid Util. Comput.*, vol. 12, no. 1, pp. 1–14, 2021. [Online]. Available: https://doi.org/10.1504/IJGUC.2021.112475

[58] D. R. Panda, S. K. Behera, and D. Jena, "A survey on cloud computing security issues, attacks and countermeasures," in *Advances in Machine Learning and Computational Intelligence*. Springer, 2021, pp. 513–524.

[59] A. Bouayad, A. Blilat, N. E. H. Mejhed, and M. E. Ghazi, "Cloud computing: Security challenges," in *2012 Colloquium in Information Science and Technology, CIST 2012, Fez, Morocco, October 22-24, 2012*. IEEE, 2012, pp. 26–31. [Online]. Available: https://doi.org/10.1109/CIST.2012.6388058

[60] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, "Cloud-trust - a security assessment model for infrastructure as a service (iaas) clouds," *IEEE Trans. Cloud Comput.*, vol. 5, no. 3, pp. 523–536, 2017. [Online]. Available: https://doi.org/10.1109/TCC.2015.2415794

[61] F. Amato, F. Moscato, V. Moscato, and F. Colace, "Improving security in cloud by formal modeling of iaas resources," *Future Generation Computer Systems*, vol. 87, pp. 754–764, 2018.

[62] N. Rakotondravony, B. Taubmann, W. Mandarawi, E. Weishäupl, P. Xu, B. Kolosnjaji, M. Protsenko, H. de Meer, and H. P. Reiser, "Classifying malware attacks in iaas cloud environments," *J. Cloud Comput.*, vol. 6, p. 26, 2017. [Online]. Available: https://doi.org/10.1186/s13677-017-0098-8

[63] L. Coppolino, S. D'Antonio, G. Mazzeo, and L. Romano, "Cloud security: Emerging threats and current solutions," *Comput. Electr. Eng.*, vol. 59, pp. 126–140, 2017. [Online]. Available: https://doi.org/10.1016/j.compeleceng.2016.03.004

[64] P. Arora, R. C. Wadhawan, and E. S. P. Ahuja, "Cloud computing security issues in infrastructure as a service," *International journal of advanced research in computer science and software engineering*, vol. 2, no. 1, 2012.

[65] S. Anwar, Z. Inayat, M. F. B. Zolkipli, J. M. Zain, A. Gani, N. B. Anuar, M. K. Khan, and V. Chang, "Cross-vm cache-based side channel attacks and proposed prevention mechanisms: A survey," *J. Netw. Comput. Appl.*, vol. 93, pp. 259–279, 2017. [Online]. Available: https://doi.org/10.1016/j.jnca.2017.06.001

[66] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Inf. Sci.*, vol. 305, pp. 357–383, 2015. [Online]. Available: https://doi.org/10.1016/j.ins.2015.01.025

[67] S. Cabuk, C. I. Dalton, A. Edwards, and A. Fischer, "A comparative study on secure network virtualization," *HP Laboratories*, 2008.

[68] W. Halboob, H. Abbas, K. Haouam, and A. Yaseen, "Dynamically changing service level agreements (slas) management in cloud computing," in *Intelligent Computing Methodologies - 10th International Conference, ICIC 2014, Taiyuan, China, August 3-6, 2014. Proceedings*, ser. Lecture Notes in Computer Science, D. Huang, K. Jo, and L. Wang, Eds., vol. 8589. Springer, 2014, pp. 434–443. [Online]. Available: https://doi.org/10.1007/978-3-319-09339-0_44

[69] B. Hay, K. L. Nance, and M. Bishop, "Storm clouds rising: Security challenges for iaas cloud computing," in *44th Hawaii International International Conference on Systems Science (HICSS-44 2011), Proceedings, 4-7 January 2011, Koloa, Kauai, HI, USA*. IEEE Computer Society, 2011, pp. 1–7. [Online]. Available: https://doi.org/10.1109/HICSS.2011.386

[70] L. Rodero-Merino, L. M. Vaquero, E. Caron, A. Muresan, and F. Desprez, "Building safe paas clouds: A survey on security in multitenant software platforms," *Comput. Secur.*, vol. 31, no. 1, pp. 96–108, 2012. [Online]. Available: https://doi.org/10.1016/j.cose.2011.10.006

[71] M. T. Sandikkaya and A. E. Harmanci, "Security problems of platform-as-a-service (paas) clouds and practical solutions to the problems," in *IEEE 31st Symposium on Reliable Distributed Systems, SRDS 2012, Irvine, CA, USA, October 8-11, 2012*. IEEE Computer Society, 2012, pp. 463–468. [Online]. Available: https://doi.org/10.1109/SRDS.2012.84

[72] D. Freet, R. Agrawal, S. John, and J. J. Walker, "Cloud forensics challenges from a service model standpoint: Iaas, paas and saas," in *Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital EcoSystems, Caraguatatuba, Brazil, October 25 - 29, 2015*, R. Chbeir, Y. Manolopoulos, V. P. Mammana, E. A. Modena, A. J. M. Traina, O. S. S. Filho, Y. Badr, and F. Andrès, Eds. ACM, 2015, pp. 148–155. [Online]. Available: https://doi.org/10.1145/2857218.2857253

[73] G. Verma and S. Adhikari, "Cloud computing security issues: a stakeholder's perspective," *SN Computer Science*, vol. 1, no. 6, pp. 1–8, 2020.

[74] K. McKay and D. Cooper, "Guidelines for the selection, configuration, and use of transport layer security (tls) implementations (2nd draft)," National Institute of Standards and Technology, Tech. Rep., 2018.

[75] J. Li, "Vulnerabilities mapping based on OWASP-SANS: a survey for static application security testing (SAST)," *CoRR*, vol. abs/2004.03216, 2020. [Online]. Available: https://arxiv.org/abs/2004.03216

[76] B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding cloud computing vulnerabilities," *IEEE Secur. Priv.*, vol. 9, no. 2, pp. 50–57, 2011. [Online]. Available: https://doi.org/10.1109/MSP.2010.115

[77] B. A. Khalaf, S. Mostafa, A. Mustapha, A. Ismaila, M. Mahmoud, M. A. Jubaira, and M. Hassan, "A simulation study of syn flood attack in cloud computing environment," *AUS journal*, vol. 26, no. 1, pp. 188–197, 2019.

[78] R. M. Jabir, S. I. R. Khanji, L. A. Ahmad, O. Alfandi, and H. Said, "Analysis of cloud computing attacks and countermeasures," in *2016 18th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2016, pp. 117–123.

[79] K. Selvamani and S. Jayanthi, "A review on cloud data security and its mitigation techniques," *Procedia Computer Science*, vol. 48, pp. 347–352, 2015.

[80] P. Kamongi, S. Kotikela, K. Kavi, M. Gomathisankaran, and A. Singhal, "VULCAN: vulnerability assessment framework for cloud computing," in *IEEE 7th International Conference on Software Security and Reliability, SERE 2013, Gaithersburg, MD, USA, June 18-20, 2013*. IEEE, 2013, pp. 218–226. [Online]. Available: https://doi.org/10.1109/SERE.2013.31

[81] N. Khan and A. Al-Yasiri, "Identifying cloud security threats to strengthen cloud computing adoption framework," in *The 11th International Conference on Future Networks and Communications (FNC 2016) / The 13th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2016) / Affiliated Workshops, August 15-18, 2016, Montreal, Quebec, Canada*, ser. Procedia Computer Science, E. M. Shakshuki, Ed., vol. 94. Elsevier, 2016, pp. 485–490. [Online]. Available: https://doi.org/10.1016/j.procs.2016.08.075

[82] K. Kritikos, T. Kirkham, B. Kryza, and P. Massonet, "Towards a security-enhanced paas platform for multi-cloud applications," *Future Gener. Comput. Syst.*, vol. 67, pp. 206–226, 2017. [Online]. Available: https://doi.org/10.1016/j.future.2016.10.008

[83] G. S. Machado, D. Hausheer, and B. Stiller, "Considerations on the interoperability of and between cloud computing standards," in *27th open grid forum (OGF27), G2C-Net workshop: from grid to cloud networks*, 2009.

[84] B. H. Krishna, S. Kiran, G. Murali, and R. P. K. Reddy, "Security issues in service model of cloud computing environment," *Procedia Computer Science*, vol. 87, pp. 246–251, 2016.

[85] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A multi-level ddos mitigation framework for the industrial internet of things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 30–36, 2018. [Online]. Available: https://doi.org/10.1109/MCOM.2018.1700621

[86] R. V. Deshmukh and K. K. Devadkar, "Understanding ddos attack & its effect in cloud environment," *Procedia Computer Science*, vol. 49, pp. 202–210, 2015.