Security in Cloud

1st Nombre Autor *Nombre Escuela*
Nombre Universidad
Ciudad, País
email@ejemplo.com

***Abstract*—Text...**

***Index Terms*—lorem, ipsum**

I. Introduction

Text...

II. Theoretical Framework

A. Cloud Computing Essentials

Cloud computing (CC) is defined as the delivery of computing resources over the internet; including compute power, storage, and databases [1]. This service is based on two main aspects: the on-demand delivery of these assets, and a pay-as-you-go pricing model [1].

This service has changed how organizations offer their services because with CC a user can access their files from any device, which is running on a remote server rather than being locally stored. This makes it possible to store terabytes of data or stream thousands of movies [2]. Additionally, organizations can take advantage of CC since it eliminates the need for large investments in on-premise hardware and can reduce energy or maintenance costs [1].

Moreover, there are some key characteristics of CC:

- *On-demand model:* The customer can increase computing capabilities based on their needs. This is a unilateral process, where users only pay for the computing resources they use [1], [3].
- *Access through the internet:* Management tools are accessible via the internet, enabling access from various devices, such as tablets, personal computers, or mobile phones [3].
- *Resource pooling:* The cloud provider groups different resources to serve multiple customer demands. Resources are dynamically allocated to customers, often offering high-level abstract options, such as selecting the country, state, or data center group [3].
- *Speed and Agility:* Resources can be rapidly assigned, allowing services to scale based on demand. This enables customers and project teams to access more resources within minutes rather than weeks [1], [3].

1) Service Models: There are different service models associated with CC. According to [2], cloud providers offer different categories of products, each with varying levels of abstraction.

As shown in the figure 1, there are multiple service models associated with CC. As defined in [2], [3], these models are known as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) respectively. According to figure 1, PaaS and SaaS models are built on top of IaaS components because IaaS forms the basis of CC, and each service runs on at least on one physical server.

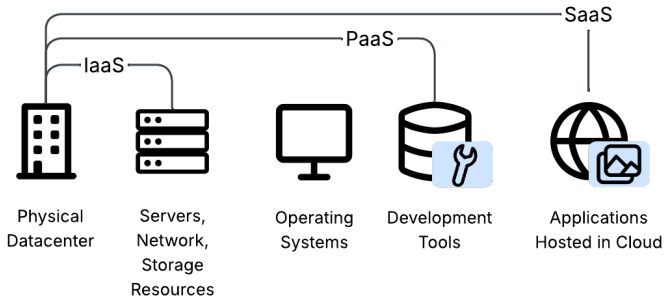

Fig. 1. Cloud Computing Service Models (Adapted from [2]).

The general description of these models is:

- *Software as a Service:* This model provides an application that is hosted within a cloud infrastructure. In addition, the customer can access these services from different devices and they do not control the resources of the application; for instance, server configurations, storage allocated, etc [3].
- *Platform as a service:* In this model, the cloud provider offers the possibility to deploy customer-created applications using programming languages, management services and other tools that support the development process of an application. Nevertheless, the customer does not manage the underlying hardware resources [3].
- *Infrastructure as a service:* The infrastructure as a Service model provides to the customer fundamental computing resources; such as networks, processing or storage. In this service, the customer can deploy specific software or services depending on their requisites. However, the customer is not able to manage physical infrastructure and security hardware components [3].

a) Deployment Models: As defined in [2], the definition of the deployment models for cloud computing (CC) is related to the specification of the location of these services, and who is responsible for management.

Different deployment models define how resources are located, managed and consumed:

- *Private Cloud:* Private cloud consists of using dedicated architecture by a single organization. In addition, the

management of these resources is the responsibility of the organization, a third party vendor or a combination or both options taking an on-premise or off-premise solution [3].

- *Public Cloud:* A public cloud offers computing resources to the general public. These resources are owned and managed by a cloud provider, which can be a commercial provider, an organization, or a government entity [3]. In addition, the public cloud is used for taking advantage of CC, develop and distribute a service using low-level infrastructure, as seen in IaaS; or a high level platform, as seen in PaaS [1].
- *Hybrid Cloud:* A hybrid cloud combines public and private cloud environments. Each model has its own independence, but they are connected through standardized processes and systems [3]. Additionally, the most common case is to use legacy on-premise infrastructure of an organization, and connect it to the cloud to improve procedures and combine the benefits of each model [1].

Furthermore, the private cloud has different approaches due to its requirements have higher costs than public cloud solutions. According to [4], there are multiple solutions for private cloud. First, the *on-premise solutions* are used for physical resources within the organization. Second, the management of the private cloud could be shared with a third party vendor that hosts the infrastructure; this is called *hosted private cloud*. Finally, there is a solution to isolate the resources used within the public cloud to have a control of hardware and network elements; this solution is called as *Virtual Private Cloud* (VPC).

B. Cloud Security Principles

As described in [5], security in cloud environments refers to the set of technologies and practices used to protect cloud-based environments from threats and vulnerabilities that could impact an organization.

Adopting these techniques enhance multiple aspects of an organization. According to [5], adopting cloud security measures can make the work environment safer for employees, ensuring data management and helping to meet regulatory compliances. Consequently, there are various principles that could be used to have a general overview of cloud security.

a) CIA Triad Model: The figure 2 shows a general diagram the CIA triad, a foundational model used for developing security systems [6], [7]. Each point within the diagram refers to the pillars of Confidentiality, Integrity and Availability (CIA).

Each pillar of CIA can be described as follows:

- *Confidentiality:* Ensures that the data is only available for authorized users, keeping it secret and private, even if the breaches of security are intentional or accidental. [6], [7].
- *Integrity:* Integrity refers to maintain a data consistency, ensuring that is not tampered by unauthorized actors; therefore, the data is reliable, authentic and accurate [6], [7].
- *Availability:* The services are accessible when needed, reducing downtime. If the services are not available, they are useless [6], [7].

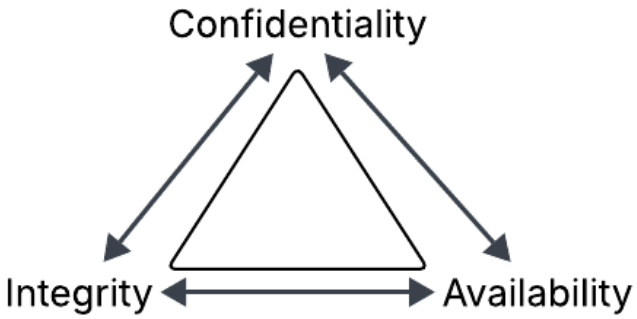

Fig. 2. CIA Triad Diagram (Adapted from [7])

These model is fundamental for making a general review for ensuring security within cloud environments. As [6] describes, an effective system covers this model, and it is deficient if one of the pillars is not met.

b) Shared responsibility Model: As defined in [8], the shared responsibility model refers to a framework a compliance framework that is used for establish the responsibilities of customers and Cloud Service Providers (CSPs) within cloud environments.

This framework involves the service models seen in section 1 that includes Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and On-premise infrastructure [8]. Additionally, it is critical to understand that these terms differs depending on how the CSP has decided to implement their product [8], [9].

Finally, as show in the table I regarding of the service model being followed, such as SaaS, IaaS or PaaS; it is important to understand that are some aspects that must be controlled by the customer; such as the data stored within the systems, the security configurations and using a service that meet customer requirements [8], [9].

C. Most Common Security Vulnerabilities

The flexible and scalable environment that cloud computing provides became with new concerns about security issues [10], this scenario is originated due to a bad transition to cloud-based environments and a lack of awareness of security threats, which have become more sophisticated and complex [10]. Therefore, there are different security vulnerabilities that must me considered within these environments to have an up-to-date perception of the current challenges and threats in cloud environments [11].

a) Misconfiguration and Inadequate Change Control: These vulnerability refers to an incorrect or sub-optimal configuration of cloud computing resources that leaves the asset to unintended damage or malicious activities [11]. Misconfiguration vulnerability is caused because an insufficient knowledge of cloud configurations, security measures and hostile intentions [11].

- *Common Misconfigurations:* Include poor management of user credentials, lack of authorization for specific resources, unnecessary permissions for cloud assets and bad monitoring systems [11].

TABLE I
RESPONSIBILITY BASED ON SERVICE MODELS

	On-premise	IaaS	PaaS	SaaS	References
Application Configuration	Customer	Customer	Customer	Customer	[8], [9]
Identity & Access Controls	Customer	Customer	Customer / CSP	Customer / CSP	[8], [9]
Application and Data Storage	Customer	Customer	Customer / CSP	CSP	[8], [9]
Application	Customer	Customer	Customer	CSP	[8], [9]
Operating System	Customer	Customer	CSP	CSP	[8], [9]
Network Flow Controls	Customer	Customer / CSP	CSP	CSP	[8], [9]
Host Infrastructure	Customer	CSP	CSP	CSP	[8], [9]
Physical Security	Customer	CSP	CSP	CSP	[8], [9]

- *Impact for the Business:* This threat impacts into data CIA pillars (Confidentiality, Integrity, Availability), affects operational processes that can lead into a reputational damage for the company [11].

Based on [11], it is recommended to implement automated monitoring, audits and assessments for cloud configurations; in addition, each change should be critically analyzed to apply a change configuration for every operation.

b) Identity & Access Managemet: As defined in [11], Identity & Access Management (IAM) refers a group of policies used for providing access to resources only for authorized individuals after proving who they are. Moreover, this critical aspect defines how the privileges are issued and detail conditions for these assignments [11].

- *Challenges:* IAM management have multiple challenges because of its complexity [11]. It is critical to implement multiple layers of security that ensures a correct management of privileges, accounts and resource access [11].
- *Impact for the Business:* A bad implementation of IAM framework could affect accounts with elevated privileges, reuse of outdated accounts, and non-compliance scenarios for multiple standards [11].

As described in [11], managing IAM is a complex process that generates multiple security breaches; in addition, the cloud service providers have different IAM rules that could create security gaps within different systems.

Finally, it is recommended to follow best practices to enhance IAM control [11]; for instance, unify IAM solutions for a centralized management, provide only minimum privileges for all users, and automate the monitoring of lifecycle accounts [11].

c) Insercure Interfaces: As detailed in [11], Cloud Service Providers, third-party vendors or developers often use Application Programming Interfaces (APIs) for communication between systems or Graphic User Interfaces (GUIs) for monitoring and control of cloud assets.

- *Common vulnerabilities:* Vulnerable interfaces have a lack of authentication mechanisms, outdated software, ineffective encryption methods or deficient compliance on share responsibility agreement [11].
- *Impact for the Business:* The business could be impact in exploitation of backend systems, shutdown periods and penalties for faulting regulatory requirements [11].

As show in [11], it is important to implement best practices for developing more secure interfaces, monitoring interfaces to identify possible exposures or identify how these interfaces work in different service models; such as migrating to a on-premise environment to a Software as a Service model.

d) Inadequate Cloud Security Strategy:

e) Insecure Third Party Resources:

f) Insecure Software Development:

g) Accidental Data Disclosure:

h) System Vulnerabilities:

i) Limited Cloud Visibility/Obervability:

j) Unauthenticated Resource Sharing:

k) Avdanced Persistent Threats:

III. METHODOLOGY

Text...

IV. STATE OF THE ART

Text...

V. RESULTS AND DISCUSSIONS

Text...

VI. CONCLUSIONS

REFERENCES

[1] Amazon Web Services, "Overview of amazon web services: Aws whitepaper," Amazon Web Services (AWS), Tech. Rep., Aug. 2025. [Online]. Available: https://docs.aws.amazon.com/pdfs/whitepapers/latest/aws-overview/aws-overview.pdf#what-is-cloud-computing (visited on 11/23/2025).

[2] Cloudflare, *What is the cloud? — cloud definition*, Web page. [Online]. Available: https://www.cloudflare.com/learning/cloud/what-is-the-cloud/ (visited on 11/23/2025).

[3] P. Mell and T. Grance, "The nist definition of cloud computing," National Institute of Standards and Technology (NIST), Tech. Rep. SP 800-145, Sep. 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf (visited on 11/21/2025).

[4] Stackscale, *Types of cloud computing: Private, public, hybrid and multicloud*, Web page, Feb. 29, 2024. [Online]. Available: https://www.stackscale.com/blog/types-of-cloud/ (visited on 11/21/2025).

[5] Fortinet, *Cloud security: The importance of safeguarding your data*, Web page. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/what-is-cloud-security (visited on 11/23/2025).

[6] Fortinet, *What is the cia triad?* Web page. [Online]. Available: https : / / www . fortinet . com / resources / cyberglossary/cia-triad (visited on 11/22/2025).

[7] GeeksforGeeks, *What is cia triad?* Web page, Sep. 18, 2025. [Online]. Available: https://www.geeksforgeeks.org/computer-networks/the-cia-triad-in-cryptography/ (visited on 11/22/2025).

[8] CrowdStrike, *Shared responsibility model*, Web page, Nov. 13, 2022. [Online]. Available: https : / / www . crowdstrike . com / en - us / cybersecurity - 101 / cloud - security/shared-responsibility/ (visited on 11/23/2025).

[9] National Cyber Security Centre, *Cloud security shared responsibility model*, Web page. Updated 2023-06-07, Nov. 17, 2018. [Online]. Available: https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model (visited on 11/24/2025).

[10] SentinelOne, *17 security risks of cloud computing in 2025*, Web page, updated 2025-08-08. [Online]. Available: https : / / www . sentinelone . com / cybersecurity - 101/cloud-security/security-risks-of-cloud-computing/ (visited on 11/24/2025).

[11] Brook et al., "Top threats to cloud computing 2024," Cloud Security Alliance (CSA), Tech. Rep., May 2024. [Online]. Available: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024 (visited on 11/24/2025).