Security in Cloud

1st Sebastián Aucapiña *School of Computer Science*
Universidad Internacional del Ecuador
Quito, Ecuador
seaucapinava@uide.edu.ec

***Abstract*—This paper analyzes the most common security issues in cloud computing, focusing on the critical role of the shared responsibility model and strategies to mitigate human error. A systematic literature review was conducted to establish a theoretical framework for cloud essentials, identify key vulnerabilities, and evaluate advanced mitigation strategies like Zero Trust and AI/ML applications. The findings reveal that the primary security challenge is human-induced misconfiguration and the misinterpretation of the Shared Responsibility Model, which leads to significant financial losses and data exposures across IaaS, PaaS, and SaaS models. Core technical risks, such as resource isolation flaws in multi-tenancy environments, also persist. We conclude that effective cloud security requires a mandatory shift from manual processes to proactive, automated solutions, including Cloud Security Posture Management (CSPM) and Artificial Intelligence-driven threat detection, to bridge the gap between human capability and the complexity of modern cloud architectures.**

***Index Terms*—Cloud security; Shared Responsibility Model; Misconfiguration; Human error; Zero Trust; Artificial Intelligence; Machine Learning; Cloud Security Posture Management (CSPM); Multi-tenancy; Resource isolation; IaaS; PaaS; SaaS; Threat detection; Automated security.**

I. Introduction

Cloud computing has become established as a critical area in different industries around the world due to its multiple benefits, such as scalability, agility, or lower operational costs [1], [2]. However, different security challenges need to be addressed within this environment for developing a solid infrastructure that considers security within this environment [3]. The central problem lies in differentiating the responsibility between customers and cloud service providers (CSPs) [3]–[5], including different roles that they need to achieve depending on the service that is being contracted [3]–[5]. Currently, the principal security challenge is misconfigurations caused by cloud customers rather than errors from the CSP [2]. The current scenario demonstrates the necessity to evaluate and investigate multiple solutions to mitigate threats that could affect an organization [4].

a) General Objective: Analyze and synthesize the most common security issues in cloud computing, detailing the importance of the shared responsibility model and mitigation strategies to counteract human error.

b) Specific Objectives:

- Establish a theoretical framework where cloud computing essentials are explained, including definitions and the shared responsibility model.
- Identify and present the most common vulnerabilities within the cloud computing environment and contrast them with different works to analyze areas of improvement in cloud security.
- Evaluate emerging and advanced mitigation strategies, such as Zero Trust strategies, Machine Learning & Artificial Intelligence applications, and their impact on securing organizational assets.

II. Theoretical Framework

A. Cloud Computing Essentials

Cloud computing (CC) is defined as the delivery of computing resources over the internet [6]; including compute power, storage, and databases [6]. This service is based on two main aspects: the on-demand delivery of these assets, and a pay-as-you-go pricing model [6]. 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 [1]. 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 [6]. 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 [6], [7].
- *Access through the internet:* Management tools are accessible via the internet, enabling access from various devices, such as tablets, personal computers, or mobile phones [7].
- *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 [7].
- *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 [6], [7].

1) Service Models: There are different service models associated with CC. According to [1], 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 [1], [7], these models are known as Infrastructure as a Service (IaaS), Platform as a

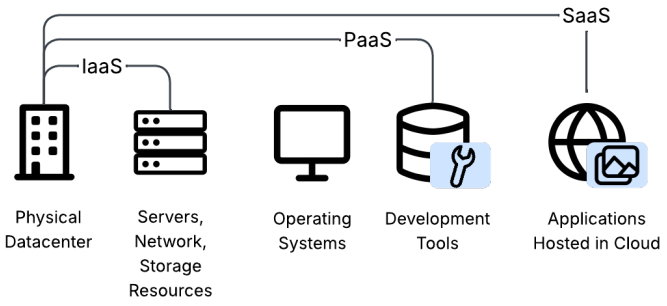

Fig. 1. Cloud Computing Service Models (Adapted from [1]).

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 one physical server. 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 [7].
- *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 [7].
- *Infrastructure as a service:* The Infrastructure as a Service model provides 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 [7].

a) Deployment Models: As defined in [1], 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 of both options, taking an on-premise or off-premise solution [7].
- *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 [7]. 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 [6].
- *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 [7]. 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 [6].

Furthermore, the private cloud has different approaches due to its requirements have higher costs than public cloud solutions. According to [8], 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 control of hardware and network elements; this solution is called as *Virtual Private Cloud* (VPC).

B. Cloud Security Principles

As described in [9], 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 enhances multiple aspects of an organization. According to [9], 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 of the CIA triad, a foundational model used for developing security systems [10], [11]. Each point within the diagram refers to the pillars of Confidentiality, Integrity and Availability (CIA).

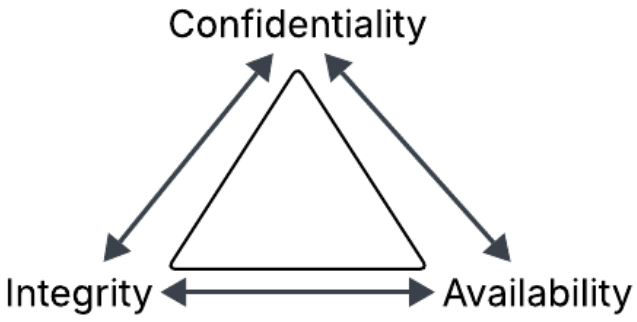

Fig. 2. CIA Triad Diagram (Adapted from [11])

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 [10], [11].
- *Integrity:* Integrity refers to maintaining data consistency, ensuring that it is not tampered with by unauthorized actors; therefore, the data is reliable, authentic and accurate [10], [11].

- *Availability:* The services are accessible when needed, reducing downtime. If the services are not available, they are useless [10], [11].

This model is fundamental for making a general review for ensuring security within cloud environments. As [10] 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 [12], the shared responsibility model refers to a compliance framework that is used to establish the responsibilities of customers and Cloud Service Providers (CSPs) within cloud environments. This framework involves the service models seen in section 1 that include Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and On-premise infrastructure [12]. Additionally, it is critical to understand that these terms differ depending on how the CSP has decided to implement their product [12], [13]. Finally, as shown in the table I regarding the service model being followed, such as SaaS, IaaS or PaaS; it is important to understand that there 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 meets customer requirements [12], [13].

C. Most Common Security Vulnerabilities

The flexible and scalable environment that cloud computing provides came with new concerns about security issues [14]; 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 [14]. Therefore, there are different security vulnerabilities that must be considered within these environments to have an up-to-date perception of the current challenges and threats in cloud environments [15].

a) Misconfiguration and Inadequate Change Control: This vulnerability refers to an incorrect or sub-optimal configuration of cloud computing resources that leaves the asset open to unintended damage or malicious activities [15]. Misconfiguration vulnerability is caused by an insufficient knowledge of cloud configurations, security measures and hostile intentions [15].

- *Common misconfigurations:* Include poor management of user credentials, lack of authorization for specific resources, unnecessary permissions for cloud assets and bad monitoring systems [15].
- *Impact for the business:* This threat impacts the data CIA pillars (Confidentiality, Integrity, Availability), affects operational processes that can lead to reputational damage for the company [15].

Based on [15], 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 Management: As defined in [15], Identity & Access Management (IAM) refers to 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 details conditions for these assignments [15].

- *Challenges:* IAM management has multiple challenges because of its complexity [15]. It is critical to implement multiple layers of security that ensure a correct management of privileges, accounts and resource access [15].
- *Impact for the business:* A bad implementation of the IAM framework could affect accounts with elevated privileges, reuse of outdated accounts, and non-compliance scenarios for multiple standards [15].

As described in [15], 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 [15]; for instance, unify IAM solutions for centralized management, provide only minimum privileges for all users, and automate the monitoring of account lifecycle [15].

c) Insecure Interfaces: As detailed in [15], 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 the shared responsibility agreement [15].
- *Impact for the business:* The business could be impacted by exploitation of backend systems, shutdown periods and penalties for violating regulatory requirements [15].

As shown in [15], 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 from an on-premise environment to a Software as a Service model.

d) Inadequate Cloud Security Strategy: According to [15], a cloud strategy is a high-level blueprint where different elements are considered, such as external factors, legacy technology, the tools that will be used and trends within the sector.

- *Considerations for cloud strategy:* There are two approaches that need to be considered for developing an appropriate cloud strategy [15]. First, it is essential to develop a technological blueprint; second, it is critical to design a sufficient security strategy [15].
- *Impact for the Business:* As shown in [15], poor cloud strategies could lead to multiple scenarios; for example, a data disclosure event, impacts on operational processes for development and engineering, or financial losses for refactoring security breaches [15].

As detailed in [15], technological strategy focuses on designing the cloud elements that will be used by considering the deployment model, the Cloud Service Provider that will be contracted or required services for developing an architecture. On the other hand, the security strategy analyzes future expansion plans that might require physical infrastructure,

TABLE I
RESPONSIBILITY BASED ON SERVICE MODELS

Responsibility	On-premise	IaaS	PaaS	SaaS	References
Application Configuration	Customer	Customer	Customer	Customer	[12], [13]
Identity & Access Controls			Customer / CSP	Customer / CSP	
Application and Data Storage		Customer / CSP			
Application		CSP		CSP	
Operating System					
Network Flow Controls					
Host Infrastructure					
Physical Security			CSP		

avoids vendor lock-ins or designs a solid Identity & Access Management (IAM) environment [15].

e) Insecure Third Party Resources: As mentioned in [15], modern cloud environments depend on third-party resources for providing a service (SaaS), including use of open source tools, or a Software as a Service product. In addition, this threat is called Cybersecurity Supply Chain Risk Management because third-party resources are part of the service that a company provides; therefore, the service is at risk if one external element is compromised [15].

- *Impact for the business:* As detailed in [15], due to third-party vulnerabilities different elements of the organization are affected; for example, data could be compromised in their confidentiality and integrity pillars, the confidence could be affected because customers may think that the company is not trustworthy or there could be an unauthorized access to the system through an external resource.

It is important to manage all the third-party tools that are used within the organization, using software officially supported, making periodic reviews of the tools used in the organization and collaborating with suppliers to ensure mutual compliance and best practices use [15].

f) Insecure Software Development: As described in [15], it is necessary to implement a secure approach for avoiding creating vulnerabilities in multiple products.

- *Approaches for secure development:* According to [15], the companies should implement different strategies for improving the development cycle; for instance, establish a cloud-first approach, implement methodologies for continuous development and integration or train developers in the shared responsibility model.
- *Impact for the business:* An insecure software development could lead to multiple impacts for the integrity and confidentiality pillars for data [15]. In addition, fixing bugs could delay the integration of new features and impact operational processes [15].

Some recommendations include establishing a secure development lifecycle for identifying vulnerabilities at an early stage [15], using cloud technologies to develop safer programs and understanding the responsibility model and contacting the cloud service provider for guidance [15].

g) Accidental Data Disclosure: As detailed in [15], data disclosure is closely related to misconfigurations and allows sensitive data to be accessed through free search tools. These exposures usually happen with storage services of different Cloud Service Providers [15], and only in 2024 it was exposed that 21.1% of these buckets had sensitive data that could include passport information, biometrics or passwords [15].

- *Impact for the business:* As reported by [15], accidental data disclosures affect the confidentiality pillar, and could lead to severe fines due to data regulations.

As reported by [15], some suggestions include implementing basic security configurations, robust educational programs and planning the identity and access management environment properly.

h) System Vulnerabilities: This threat refers to security breaches within cloud systems that could be exploited to affect the confidentiality, integrity and availability pillars [15]. As described in [15], there are different categories for system vulnerabilities:

- *Misconfiguration:* Threats increase significantly with default or bad configurations [15].
- *Zero-day Vulnerabilities:* This threat refers to system vulnerabilities discovered by malicious actors that are unknown to cloud service providers or software vendors [15].
- *Unpatched Software:* Software that has known vulnerabilities that have not been fixed despite resources for solving the failure [15].
- *Weak or Default Credentials:* This refers to a lack of robust authentication processes that allows access to unauthorized actors [15].

As detailed in [15], some recommendations include continuous monitoring of the system, auditing for covering vulnerabilities before hackers and implementing a zero trust architecture through constant authentication to protect access to sensitive resources.

i) Limited Cloud Visibility/Observability: This threat describes that an organization does not visualize and analyze if the cloud services are used properly [15]. In addition, [15] details that there are two scenarios; non-authorized application use and authorized application misuse [15].

- *Non-Authorized application use:* This scenario occurs when employees utilize applications without company's support or security measures, and it is risky when confidential information is involved [15].
- *Authorized application misuse:* On the other hand, this context occurs when organizations do not manage suitably how approved applications are used by employees or targeted by malicious actors [15].

- *Impact for the business:* According to [15], some impacts include weak security due to lack of control for non-visible issues, business interruptions for customers and partners and lost revenue because of restoration or control costs.

As described in [15], it is recommended to use a top-down cloud strategy approach to include people, processes and technology within the cloud architecture. In addition, it is critical to train employees in the cloud corporative environment and manage enterprise cloud applications effectively [15].

j) Unauthenticated Resource Sharing: As detailed in [15], this threat involves a weak authentication process for cloud resources, such as virtual machines or storage services that contain sensitive data. In addition, [15] describes some security measures and impact for the business of this threat:

- *Multi-factor authentication (MFA):* When a user accesses a resource, a second authorization method is required that could include a one-time code or biometrics [15].
- *Third-party authentication platforms:* As reported by [15], using external services improves user management and gives a user-friendly authorization process for company members.
- *Managing user access:* Users should only access the resources that they require [15].
- *Continual monitoring activity:* It is critical to monitor any suspicious activity of any user [15].
- *Impact for the business:* As described in [15], some impacts include compromise of the confidentiality and availability data pillars, impacts on operational business in securing these shared points or reputational damage due to this security breach.

Finally, [15] details that at least basic password authentication should be implemented, including MFA tools from third-party vendors and analyzing user actions.

k) Advanced Persistent Threats: As described in [15], Advanced Persistent Threats (APTs) are composed of different sophisticated adversaries that have resources and knowledge to deploy a long-term attack targeting important assets. Usually, APTs include nation-state agencies or organized criminal gangs that have been increasing their attacks exploiting zero-day vulnerabilities, third-party vendor resources or identity and access management environments [15].

- *Impact for the business:* Some impacts include a higher exposition from not addressed APTs, reputational damage due to a big exposure of the attack or business disruptions because of different threat scenarios [15].

As described in [15], an organization should identify critical assets and potential vulnerabilities, participate in information groups about the most dangerous APTs groups and simulate security offensives to test and improve the architecture.

III. Methodology

To develop the literature review within the cloud security environment a structured search is used. In addition, *Google Scholar* is used as the database source information due to its large number of indexed publications.

A. Binary Search

A *boolean search* is used for limiting the results and collecting higher quality results: *"cloud computing security" AND ("AWS" OR "Azure" OR "GCP") AND ("vulnerabilities" OR "vulnerability") AND ("IaaS" OR "PaaS" OR "SaaS") - "IoT"*.

a) Inclusion Criteria:: Inclusion criteria includes the following requirements:

- Publication between 2019-2025.
- Open access or limited access via email login.
- Most cited publications.
- Surveys, technical analyses or systematic reviews.

b) Exclusion Criteria:: Exclusion criteria includes the following requirements:

- Documents with paywalls access to the full content.
- Documents not related to cloud security; for instance, hardware, economics, etc.

IV. State of the Art

The current state of cloud security is characterized by a high degree of technological innovation paired with persistent vulnerabilities rooted in human error and architectural complexity [4], [16], [17].

A. Cloud Computing Necessities

Cloud environments demand strict technical and operational requirements, including robust virtualization, elasticity, and flexible service models. A core necessity is the provision of secure communication channels, including *strong authentication and encryption*, as well as rigorous separation between tenants in multi-tenancy scenarios [18], [19].

B. Threat and Vulnerability Landscape

The literature identifies key risks such as data breaches, data manipulation, unauthorized access, and insecure interfaces [19]–[21]. The complexity of the threat landscape is exacerbated by the convergence of mobile, application, and cloud domains, creating intertwined attack surfaces that facilitatemulti-stage breaches [22]. Additionally, a detailed investigation reveals that security issues are highly dependent on the service model, with IaaS infrastructures having specific vulnerabilities related to virtualization and hypervisor attacks, while PaaS and SaaS face greater risks from insecure APIs and weak access controls [5], [23]. Recurring threats like Account Hijacking and Malware Injection are consistently highlighted, often exploiting common misconfigurations and inadequate interfaces [24]. A critical vulnerability arises from the shared nature of resources in *Multi-tenancy* environments, where insufficient isolation can lead to side-channel attacks and resource depletion, often cited as a significant technical risk [20]. Other recurrent issues include misconfiguration, insecure APIs, privilege escalation, and attacks at the hypervisor level [19].

C. Business Impact and Consequences

Security failures lead to a range of severe consequences for organizations, including operational disruption, loss of customer trust, regulatory sanctions (e.g., GDPR), and significant financial losses [20], [21]. The recurrent failure point is often attributed to *misconfiguration* [20]. A systemic risk factor is the *misinterpretation of the Shared Responsibility Model*, which shifts certain critical security tasks to the client, leading to oversight and exposure [3], [20]. Furthermore, addressing dynamic regulatory requirements (e.g., GDPR, HIPAA) in multi-cloud environments necessitates the implementation of automated compliance enforcement solutions, as manual processes are often insufficient and not scalable to mitigate the persistent risk of non-conformity [25].

D. Mitigation Strategies and Innovative Trends

To counteract these challenges, the consensus is a multi-layered approach emphasizing automation and proactive management.

1) Proactive Security and Governance: Effective mitigation starts with strong governance and a cultural shift towards security.

- *Zero Trust Architecture (ZTA):* Requires strict verification for every user and device trying to access resources, regardless of their location [26].
- *Cloud Security Posture Management (CSPM):* Tools that continuously monitor cloud configurations and adherence to best practices, significantly reducing misconfiguration risks [26].
- *IAM and DevSecOps:* Strict Identity and Access Management and integration of security practices into the development lifecycle are non-negotiables [26].

2) Technical and Architectural Countermeasures: These involve protective measures implemented directly in the technical infrastructure.

- *Data Encryption:* Encrypting data both at rest (storage) and in transit (network) is fundamental for confidentiality and integrity [27], [28].
- *Network and Interface Security:* Deploying Web Application Firewalls (WAF), Content Delivery Networks (CDN), and securing all external APIs are essential to filter malicious traffic and prevent unauthorized access [27], [29].
- *Continuous Monitoring:* Employing Security Information and Event Management (SIEM) systems for real-time aggregation and analysis of security events [18].
- *Network Security as a Service (NSaaS):* This approach utilizes the cloud model to deliver comprehensive security functions (e.g., IDS/IPS, WAF, Vulnerability Scanning) in an adaptive and scalable manner, often integrated with tools like Snort and NMAP for proactive defense [30].

E. Innovative Trends and Future Technologies

Future security models prioritize adaptation, automation, and advanced computation [20], [31], [32]. The effectiveness of these models is often assessed through comparative analysis across leading cloud providers (AWS, Azure, GCP, etc.), focusing on key security criteria such as data encryption, IAM, and compliance [32].

- *Artificial Intelligence and Machine Learning (AI/ML):* AI/ML is essential for real-time threat detection and automated risk prevention [31], [32]. These algorithms analyze large datasets to identify patterns and anomalies, enhancing detection and response capabilities [31].
- *Blockchain Technology:* Blockchain is a partnering technology used to alleviate security concerns [20]. It provides tamper-proof logging and auditing capabilities for security-related events [31], [32].
- *Confidential Computing:* An emerging trend focused on protecting data *in use* by performing computation in a hardware-based, trusted execution environment (TEE), ensuring data remains encrypted even during processing [32].
- *Advanced Security Architecture:* Modern security models often use a multi-layered architecture including a Threat Detection Layer, a Response Layer, and a Mitigation Layer [31]. Future research should explore autonomous cybersecurity systems and quantum-resistant cryptography [31].

V. Discussion

The analysis presented in the State of the Art reveals a critical paradox in cloud computing security: while cloud environments offer inherent security advantages (e.g., professional management of physical infrastructure [23]), the shift in the operational paradigm fundamentally introduces new, systemic risks rooted in shared responsibility and human factors [2], [3].

A. The Dominance of Human Error and Misconfiguration

The most persistent threat across all service models is human-induced misconfiguration [2], [19], [21]. Empirical data strongly support that organizational failure to properly manage the Shared Responsibility Model is the primary driver of risk [2], [3].

- **Quantifiable Impact:** Misconfigurations, particularly Identity and Access Management (IAM) errors (183 occurrences) and exposed APIs (156 occurrences), are the most frequent security failures in financial SaaS applications. An increase in misconfiguration severity results in an average of $2.27M in financial losses and 93,300 compromised records.
- **The Root Cause:** This high frequency is attributable to human error, inadequate security awareness, and reliance on manual configuration processes prone to error. This deficiency translates easily into security gaps, particularly because IAM solutions offered by cloud service providers (CSPs) are complex and prone to misinterpretation by clients.
- **SLAs vs. Security:** The issue is exacerbated by the non-quantitative nature of security and privacy, which makes them difficult to incorporate into measurable Service

Level Agreements (SLAs). This leaves customers contractually exposed to failures that fall outside the typical uptime metrics prioritized by standard SLAs.

B. Layer-Specific Security Challenges

Security requirements diverge significantly across the Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models.

- **IaaS and Core Isolation:** The core vulnerability in IaaS is rooted in Shared Technology Vulnerabilities, encompassing risks like VM Escape and attacks targeting the hypervisor layer. This burden of security shifts based on the deployment model: in public IaaS (e.g., AWS EC2), the CSP maintains the hypervisor security, whereas in private IaaS (e.g., Proxmox VE), the customer assumes full responsibility for the hardware and hypervisor layers.
- **PaaS/SaaS and Access Control:** In PaaS and SaaS, the focus shifts away from infrastructure and towards application security, API security, and identity management. Attacks are often centered on the application logic or user credentials rather than the underlying virtualization layer.
- **Operational Differences:** Public IaaS typically provides high security features, such as IDS/IPS and Web Application Firewalls (WAF), integrated and managed by the vendor on a pay-as-you-go basis. Conversely, equivalent advanced solutions in private IaaS often require manual deployment and expert configuration of third-party tools like Snort.

C. The Role of Automation and Intelligent Mitigation

The complexity of the threat landscape makes automation an essential strategy to minimize human error and achieve real-time protection.

- **AI-Enhanced Detection:** Advanced solutions, particularly those leveraging Artificial Intelligence (AI) and Machine Learning (ML), demonstrate superior efficacy. One experimental study showed that an AI-driven IDS (AWS GuardDuty) successfully detected malicious webshells, a capability often missed by less intelligent IDS solutions. The projected outcome is enhanced detection accuracy (up to 95%) and significantly reduced response times (down to 10 seconds), suggesting a clear future direction for threat detection.
- **Proactive Compliance:** For multi-cloud operations, automated compliance tools (like AWS Macie or GCP DLP) are critical, shifting the process from manual audits to continuous, intelligent data discovery and enforcement. This approach addresses the increasing regulatory burden (GDPR, HIPAA) that manual processes cannot scale to meet.
- **The Next Generation of Defense:** Future mitigation strategies focus on protecting data *in use* and ensuring auditability. This includes:
  1) **Confidential Computing:** Protecting data during processing (memory and CPU) by keeping it encrypted in a Trusted Execution Environment (TEE), an important evolution from simple encryption at rest.
  2) **Blockchain for Accountability:** Utilizing Distributed Ledger Technology (DLT) to create immutable audit trails, enhancing transparency, accountability, and enabling forensic research after an intrusion.
  3) **Zero Trust Architecture (ZTA):** Enforcing continuous verification and the Principle of Least Privilege (PoLP) drastically reduces the vulnerability window, directly addressing the risks posed by compromised credentials and human error.

VI. Conclusions

The systematic review and critical analysis of cloud security literature confirm that despite the technological maturity of major Cloud Service Providers (CSPs), cybersecurity remains the paramount concern for adoption, fundamentally challenged by systemic and human factors inherent to the cloud model. The findings lead to several key conclusions regarding risk posture, mitigation efficacy, and future strategic direction.

A. Risk Posture: The Misconfiguration Paradox

The primary vulnerability vector is not the compromise of the CSP's core infrastructure, but rather the failure of customers to manage their portion of the shared responsibility model.

- **Quantifiable Impact:** Misconfiguration, dominated by IAM errors and insecure APIs, is the leading cause of breaches across IaaS, PaaS, and SaaS, driving significant financial losses and exposing millions of records. This empirical evidence underscores the high stakes associated with human error and policy misinterpretation.
- **Systemic Vulnerabilities:** Core technical risks persist, particularly those related to resource isolation in multi-tenancy environments, where flaws can manifest as side-channel attacks, resource contention, and, in severe cases, VM escape vulnerabilities.
- **SaaS Security:** In the Software-as-a-Service model, where customers rely most heavily on the provider, the main challenges revolve around data breaches, lack of user control/visibility, and maintaining regulatory compliance, emphasizing the criticality of trust and governance external to the application itself.

B. Mitigation Efficacy and Operational Imperatives

Effective cybersecurity demands a shift from passive perimeter defense to proactive, layered, and context-aware strategies.

- **Security as a Service (SECaaS):** The integration of Network Security as a Service (NSaaS) and similar SECaaS models is crucial for centralized monitoring and proactive defense, allowing organizations to deploy specialized tools (e.g., Snort, Honeypot) without compromising the inherent flexibility and scalability of the cloud platform.

- **Automation is Mandatory:** Manual compliance and configuration management are neither scalable nor feasible in complex multi-cloud environments. The adoption of comprehensive solutions like Cloud Security Posture Management (CSPM) and the enforcement of Zero Trust Architecture (ZTA) reduce breach probability significantly by automating policy enforcement and continuous verification.
- **AI for Superior Detection:** Artificial Intelligence and Machine Learning demonstrate superior efficacy in identifying novel and low-volume threats, as evidenced by AI-driven IDS solutions achieving higher accuracy and faster response times compared to traditional rule-based mechanisms.

VII. Future Research Directions

Future work should concentrate on addressing the core limitations of the current security landscape to ensure resilient and scalable solutions:

- **Trusted Execution and Data in Use:** Further development and industry integration of **Confidential Computing** technologies are essential to protect data during processing (data in use), mitigating side-channel and insider threats that bypass current encryption protocols.
- **Accountability and Forensics:** Research is needed to develop unified, cross-platform standards for **Blockchain-based auditing** to create immutable, verifiable log trails for forensic analysis and compliance enforcement across multi-cloud environments.
- **Usability and Abstraction:** Future security frameworks must focus on reducing the complexity barrier for end-users, leveraging intelligent automation to translate high-level security goals (e.g., PoLP) into low-level, error-proof cloud configurations, effectively closing the gap between the shared responsibility model and human capability.

References

[1] 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).

[2] O. C. Metibemu, T. Adesokan-Imran, A. J. Ajayi, O. Tiwo, A. Olutimehin, and O. Olaniyi, "Developing Proactive Threat Mitigation Strategies for Cloud Misconfiguration Risks in Financial SaaS Applications," *Journal of Engineering Research and Reports*, vol. 27, pp. 393–413, Mar. 15, 2025. DOI: 10.9734/jerr/2025/v27i31442.

[3] C. Mendoza and C. Reyes, "EXPLORING THE IMPACT OF SHARED RESPONSIBILITY MODELS ON CLOUD SECURITY POSTURE AND VULNERABILITY MANAGEMENT," *Journal of Emerging Technologies*, Apr. 1, 2023.

[4] M. R. Soni and D. N. Uikey, "Cloud Computing Security and Challenges: An In-Depth Analysis," *IJSAT - International Journal on Science and Technology*, vol. 16, no. 2, May 17, 2025, ISSN: 2229-7677. DOI: 10.71097/IJSAT.v16.i2.5286. [Online]. Available: https://www.ijsat.org/research-paper.php?id=5286 (visited on 12/07/2025).

[5] A. Sharma and U. K. Singh, "Investigation of cloud computing security issues & challenges," in *Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)*, Atlantis Press, 2021, pp. 445–453, ISBN: 978-94-6239-428-5. DOI: 10.2991/ahis.k.210913.055. [Online]. Available: https://doi.org/10.2991/ahis.k.210913.055.

[6] 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).

[7] 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).

[8] 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).

[9] 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).

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

[11] 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).

[12] 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).

[13] 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).

[14] 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).

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

[16] V. Sureshkumar and B. Baranidharan, "A study of the cloud security attacks and threats," *Journal of Physics: Conference Series*, vol. 1964, no. 4, p. 042 061, Jul. 2021, ISSN: 1742-6596. DOI: 10.1088/1742-6596/1964/4/042061. [Online]. Available: https://doi.org/10.1088/1742-6596/1964/4/042061 (visited on 12/07/2025).

[17] N. K. Sehgal, P. C. P. Bhatt, and J. M. Acken, *Cloud Computing with Security and Scalability: Concepts and Practices*, 3rd ed. Cham: Springer Nature Switzerland AG, 2023, ISBN: 978-3-031-07242-0. DOI: 10.1007/978-3-031-07242-0. [Online]. Available: https://doi.org/10.1007/978-3-031-07242-0.

[18] I. Ilochonwu, "Cloud security paradigms: A systematic review of threat mitigation strategies in cloud-based applications," *International Journal of Cloud Computing and Database Management*, vol. 5, pp. 97–108, Jul. 1, 2024. DOI: 10.33545/27075907.2024.v5.i2b.75.

[19] S. S. Pericherla, "Cloud computing threats, vulnerabilities and countermeasures: A state-of-the-art," *ISeCure: The ISC International Journal of Information Security*, vol. 15, no. 1, pp. 1–58, Jan. 2023. DOI: 10.22042/ISECURE.2022.312328.718. [Online]. Available: http://www.isecure-journal.org.

[20] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," *IEEE Access*, vol. 9, pp. 57 792–57 807, 2021, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3073203. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9404177 (visited on 12/07/2025).

[21] M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas, and S. U. Rehman, "Cyberattacks and security of cloud computing: A complete guideline," *Symmetry*, vol. 15, no. 11, 2023, ISSN: 2073-8994. DOI: 10.3390/sym15111981. [Online]. Available: https://www.mdpi.com/2073-8994/15/11/1981.

[22] M. Mthunzi. "Mobile, App, and Cloud Security: Threats, Vulnerabilities, and Defense Mechanisms." (Oct. 15, 2025), [Online]. Available: https://zenodo.org/doi/10.5281/zenodo.17371259 (visited on 12/07/2025), pre-published.

[23] İ. Yoşumaz, "An Examination of Cyber Security Solutions in Public and Private IaaS Infrastructures," *International Journal of Information Security Science*, vol. 13, no. 3, pp. 1–29, Sep. 30, 2024, ISSN: 2147-0030. DOI: 10.55859/ijiss.1475423. [Online]. Available: https://dergipark.org.tr/en/pub/ijiss/issue/87464/1475423 (visited on 12/07/2025).

[24] O. Mykhaylova, M. Korol, and R. Kyrychok, "Research and analysis of issues and challenges in ensuring cyber security in cloud computing," *Cybersecurity Providing in Information and Telecommunication Systems II 2024*, vol. 3826, pp. 30–39, 2024, ISSN: 1613-0073. [Online]. Available: https://ceur-ws.org/Vol-3826/ (visited on 12/07/2025).

[25] V. M. L. G. Nerella, "Automated Compliance Enforcement in Multi-Cloud Database Environments: A Comparative Study of Azure Purview, AWS Macie, and GCP DLP," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 11, pp. 270–283, Jul. 23, 2025. DOI: 10.32628/CSEIT25111668.

[26] W. Hashim and N. A.-H. K. Hussein, "Securing Cloud Computing Environments: An Analysis of Multi-Tenancy Vulnerabilities and Countermeasures," *SHIFRA*, vol. 2024, pp. 8–16, Feb. 5, 2024, ISSN: 3078-3186. DOI: 10.70470/SHIFRA/2024/002. [Online]. Available: https://peninsula-press.ae/Journals/index.php/SHIFRA/article/view/47 (visited on 12/07/2025).

[27] Janet Julia Ang'udi, "Security challenges in cloud computing: A comprehensive analysis," *World Journal of Advanced Engineering Technology and Sciences*, vol. 10, no. 2, pp. 155–181, Dec. 30, 2023, ISSN: 25828266. DOI: 10.30574/wjaets.2023.10.2.0304. [Online]. Available: https://wjaets.com/content/security-challenges-cloud-computing-comprehensive-analysis (visited on 12/07/2025).

[28] I. S. M. Fadhil, N. B. M. Nizar, and R. J. Rostam, "Security and Privacy Issues in Cloud Computing," [Online]. Available: https://www.authorea.com/doi/full/10.36227/techrxiv.23506905?commit=1e8b34bf89fb83efa820cca6704fa98691c26ea2 (visited on 12/07/2025).

[29] M. Humayun, M. Niazi, M. F. Almufareh, N. Z. Jhanjhi, S. Mahmood, and M. Alshayeb, "Software-as-a-service security challenges and best practices: A multivocal literature review," *Applied Sciences*, vol. 12, no. 8, 2022, ISSN: 2076-3417. DOI: 10.3390/app12083953. [Online]. Available: https://www.mdpi.com/2076-3417/12/8/3953.

[30] A. S. Gouda, "SECURENET: SAFEGUARDING NETWORKS ON THE AWS CLOUD PLATFORM,"

[31] A. A. Fadele, A. Rocha, E. J. Ahmed, and A. Ibrahim. "Cybersecurity Model for Intelligent Cloud Computing Systems." (2024), [Online]. Available: https://www.ssrn.com/abstract=4970422 (visited on 12/07/2025), pre-published.

[32] S. M. Levin, "Comparative analysis of security models in cloud platforms," *Izvestiya Tomskogo Politekhnicheskogo Universiteta. Promyshlennaya Kibernetika*, vol. 2, no. 2, pp. 1–16, 2024. [Online]. Available: https://cyberleninka.ru/article/n/comparative-analysis-of-security-models-in-cloud-platforms (visited on 12/07/2025).