STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Classification of threats and countermeasures of cloud computing

Rasha Almanasir[1], Deyaa Al-solomon[1], Saif Indrawes[1], Mohammed Almaiah[1], Umar Islam[2], Marwan Alshar'e[3]

[1] *King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan*
[2] *Department of Computer Science, IQRA National University, Swat Campus, Swat 19220, Pakistan*
[3] *Faculty of Computing and IT, Sohar University, Sohar, Oman*

ARTICLE INFO

Article History

Received: 10-03-2025
Revised: 27-03-2025
Accepted: 05-04-2025
Published: 08-04-2025

Academic Editor:

Prof. Youakim Badr

Vol.2025, No.2

DOI:
https://doi.org/10.63180/jcsra.thestap.2025.2.3

ABSTRACT

This article focuses on the study of cloud computing, it's various models, and cloud service types such as SaaS, PaaS, and IaaS. It emphasizes the security challenges and cyber threats associated with cloud environments, while also proposing methods and solutions to protect these systems. The study underlines the advantages of cloud computing in offering rapid, cost-effective access to technology and services, but also points out the vulnerabilities of multi-tenant architectures and the need for robust security measures to address these risks. Additionally, the article presents a detailed analysis of major security threats such as data loss, forgery, man-in-the-middle attacks, and denial of service (DoS) attacks—and explores detection and prevention techniques. These include the use of advanced tools for threat monitoring and pattern analysis, aimed at strengthening security and boosting user trust in cloud computing systems.

Keywords: Cloud computing, Security of cloud services, Risk assessment, SaaS, PaaS, and IaaS.

How to cite the article
Almanasir, R., Al-solomon, D., Indrawes, S., Amin Almaiah, M., Islam, U., & Alshar'e, M. (2025). Classification of threats and countermeasures of cloud computing. Journal of Cyber Security and Risk Auditing, 2025(2), 27–42. https://doi.org/10.63180/jcsra.thestap.2025.2.3

1. Introduction

Cloud computing has become a fundamental technology for individuals and organizations in the digital age, offering scalable and flexible solutions for data processing and storage [1]. However, these advantages come with significant security challenges that must be addressed to protect sensitive data and ensure the integrity of cloud services [2]. Major security concerns in cloud computing include data breaches, unsecured interfaces and APIs, account hijacking, insider threats, data loss, denial of service (DoS) attacks, and insufficient due diligence [3], [4]. Effective risk management and assessment are crucial in this context, enabling proactive threat mitigation, vulnerability detection, legal and regulatory compliance, sensitive data protection, business continuity, and cost control [5]. Risk assessment helps to identify weaknesses in cloud infrastructure, allowing organizations to implement policies that reduce the impact of potential threats. It also supports legal compliance and protects confidential information from unauthorized access or breaches. By ensuring service continuity and avoiding financial losses due to security incidents, risk management contributes to both operational resilience and cost efficiency [6].

*Corresponding author. Email: mlmaiah@aut.edu.jo

Cloud computing operates on a five-part architecture consisting of the consumer (end user), provider (service manager), auditor (third-party compliance verifier), broker (service mediator), and carrier (infrastructure manager). To meet diverse organizational needs, cloud deployment models include private, public, community, and hybrid clouds, while service models are categorized into Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [7], [8]. This study addresses the security issues stemming from the distinct nature of cloud environments, offering a comprehensive overview of threats and proposing effective solutions. It explores various strategies and mechanisms for managing cloud security, aiming to reduce risks and vulnerabilities while boosting users' trust in cloud services. The article also presents a detailed analysis of classified security challenges and corresponding countermeasures.

2. Background of the study

2.1 Cyber security reference model of intelligent cloud computing

To ensure the cybersecurity of cloud computing systems, it is first essential to understand their structural framework [9]. Leading organizations such as NIST, IBM, and Microsoft have proposed reference models in this context. NIST outlines a model involving five main participants: cloud client, cloud provider, cloud carrier, cloud auditor, and cloud broker, organized into layers such as orchestration, service, resource abstraction and management, physical resources, cloud service management, and security [10]. Key security considerations include authentication and authorization, resource allocation, virtual resource monitoring, activity tracking, SLA definition, and enforcement of security policies. IBM's model, as described by [11], identifies three core roles—customer, operator, and cloud service creator—and addresses security, resilience, and performance across the management platform, hardware infrastructure, and cloud services.

However, existing models often lack detailed treatment of virtualization and service layers, neglect the IoT social media sensor layer that captures attacker-generated data, and overlook cyber resilience aspects [12]. To fill these gaps, a new reference model is proposed, comprising two primary actors (cloud customer and cloud operator) and incorporating comprehensive layers: application, service, virtualization, data transmission, physical resources, IoT social media sensor, and cybersecurity and cyber resilience layers. Figure 1 represents the cyber security reference model for the cloud computing system.

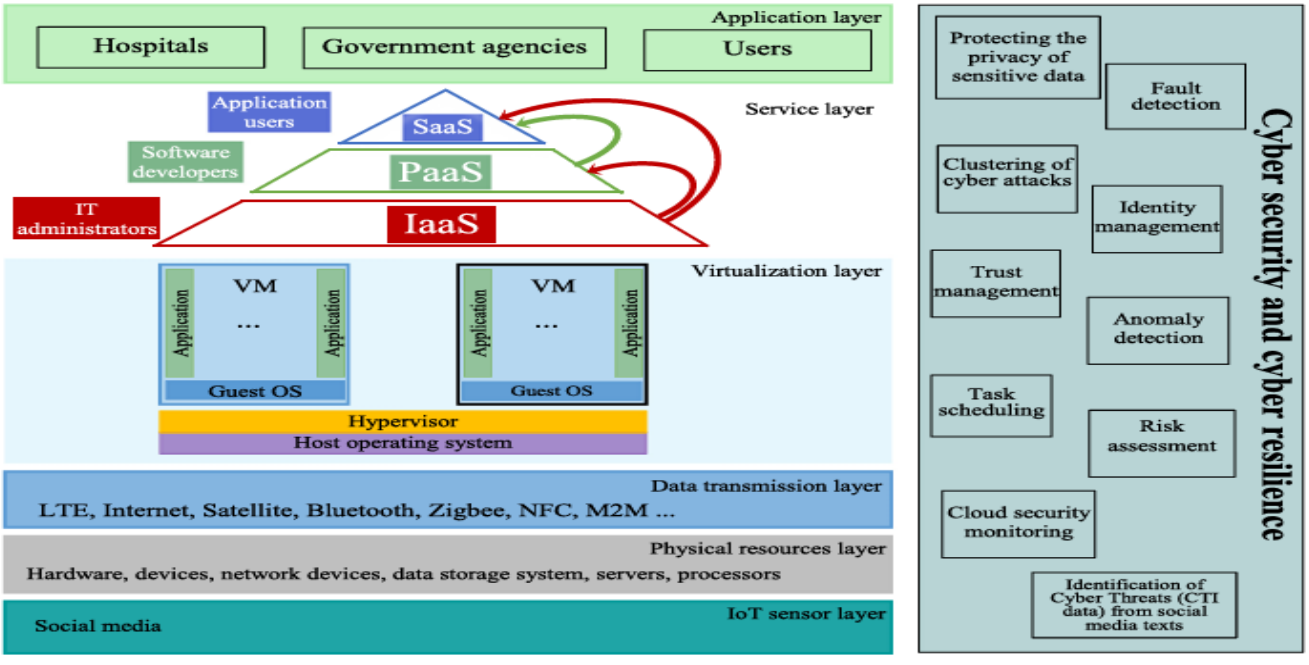


Figure 1. Cyber security reference model for the cloud computing system.

2.2 Cyber security issues of service delivery models of cloud computing systems

Cloud computing delivers a wide range of services through three primary service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These models provide users with software applications, development platforms, and infrastructure resources, respectively. Each model introduces distinct security requirements within the cloud environment. IaaS forms the foundational layer of the cloud service stack, upon which PaaS is built, followed by SaaS as the topmost layer [13]. As illustrated in Figure 2, the cloud computing architecture is composed of four key layers are: hardware layer, infrastructure layer, platform layer, and application layer. These layers are stacked sequentially, each operating independently based on the principle of loose coupling with the layers above and below. The hardware layer is responsible for managing the cloud's physical components, including servers, routers, switches, power supplies, and cooling systems [14].

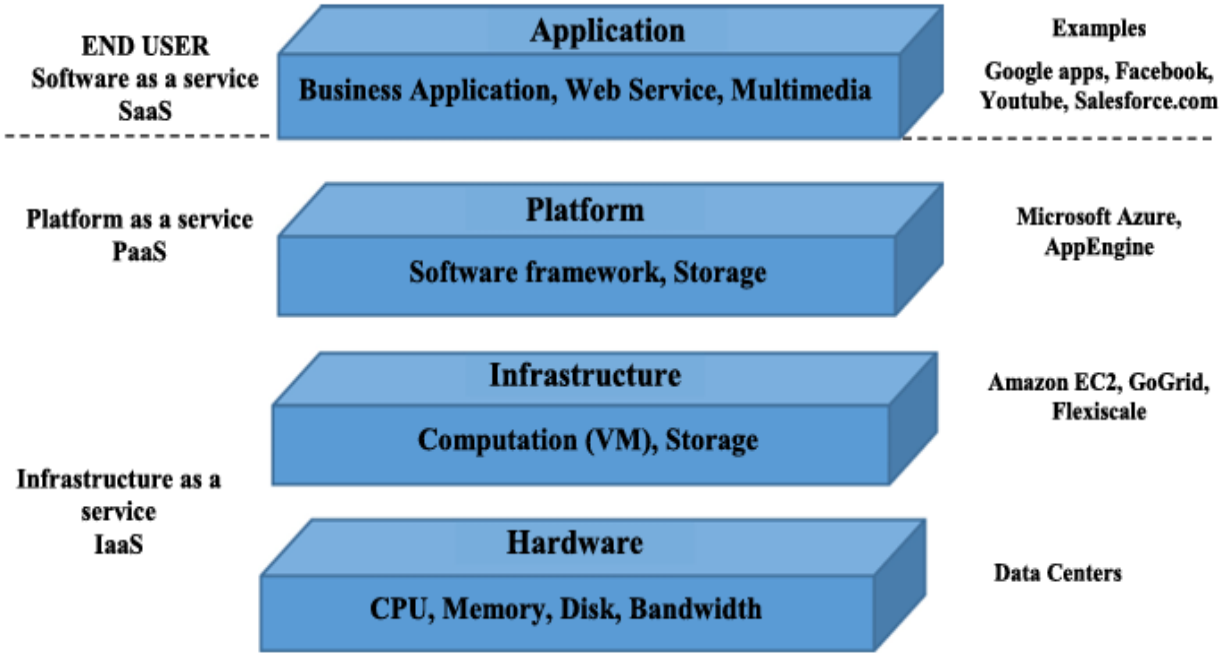


Figure 2. Layered architecture of the cloud system.

The infrastructure layer, also known as the virtualization layer, is responsible for creating a pool of computing and storage resources using virtualization technologies. Above it lies the platform layer, which includes essential components such as operating systems. At the top is the application layer, which differs from traditional applications by offering features like auto-scalability to enhance performance and availability while minimizing costs. Security responsibilities in cloud computing are shared between cloud providers and customers, varying based on the service model. In the SaaS model, customer data is stored alongside other users' data in the provider's data center, and is often replicated across countries to ensure availability. Unlike traditional systems where enterprises have control over data storage regulations, SaaS customers are often unaware of where and how their data is stored and protected, raising significant security concerns. This lack of transparency can result in issues such as data leakage, application vulnerabilities, and unauthorized access, leading to financial and legal repercussions.

In this model, the provider is fully responsible for cloud security, and key security concerns include data security, network security, data colocation and segregation, data integrity, access control, authentication, data confidentiality, web application security, and virtualization vulnerabilities. In the PaaS model, users are granted certain management rights, but the provider retains responsibility for protecting the platform below the application layer, including preventing host and network intrusions. A critical concern here is ensuring strict data isolation between applications. PaaS is primarily designed to allow developers to build and deploy their own applications. In contrast, the IaaS model gives users broader control over security

management, making the division of security responsibilities between the provider and the customer highly dependent on the specific service arrangement [15]. Deception Attacks are a significant threat in cloud-based industrial control systems, particularly as more industrial organizations migrate their management systems to the cloud due to its efficiency in storage and computing resources. These attacks aim to compromise the integrity of control signals by maliciously altering the transmitted information. To address this, [16] proposes a neural network-based method for detecting deception attacks targeting actuator signals in such systems. Denial of Service (DoS) Attacks represent another critical threat, wherein an attacker attempts to overwhelm a network, system, or application with excessive traffic, connections, or requests, rendering it incapable of functioning properly. To mitigate the impact of DoS attacks in nonlinear systems with uncertain input data, [17] presents an approach for estimating the system state under such adverse conditions. Figure 3 represents the most common Cyber-attack model for cloud system.

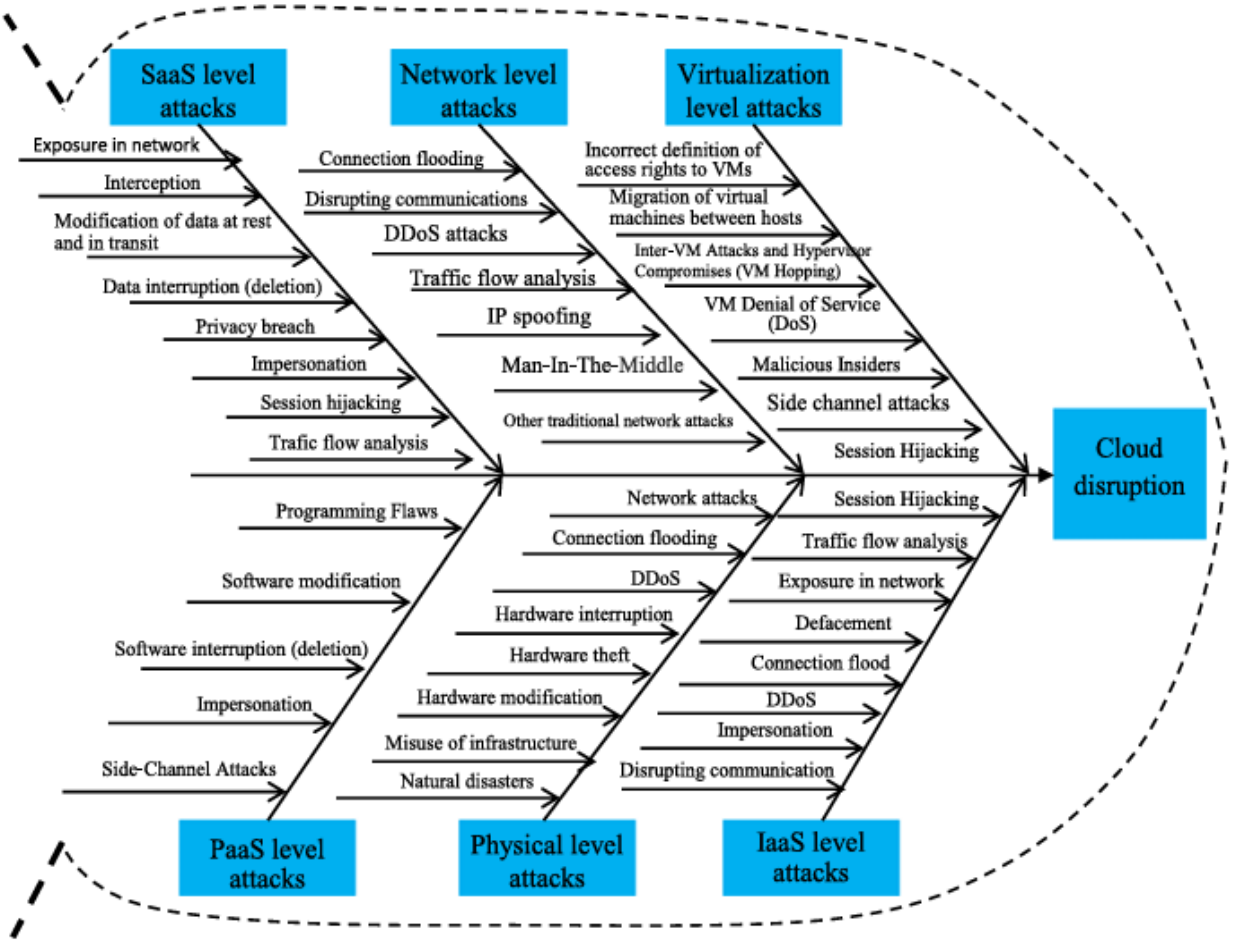


Figure 3. Most common Cyber-attack model for cloud system.

3. Risk assessment method for cloud computing environments

When organizations manage cloud services in the same manner as traditional on premise infrastructure, they risk facing serious security challenges that can potentially impact their entire business operations [18]. Therefore, it is crucial not to underestimate the importance of governing cloud service security, particularly in relation to the organization's IT environment. The first step in this process should be a thorough analysis of the existing IT environment to identify critical security gaps or vulnerabilities [19].

One of the most common and effective methods for this is risk assessment, which forms a core component of the broader risk management framework [20]. Risk assessment is essential for identifying, prioritizing, and mitigating risks to an acceptable level, thereby ensuring business stability. Organizations that neglect risk identification and management expose themselves to the possibility of exploited vulnerabilities, which could severely disrupt their operations. Risk management is defined as "the company-wide measurement and supervision of all business risks." A comprehensive standard for this process is provided by the International Organization for Standardization through ISO/IEC 27005:2018, titled Information technology – Security techniques – Information security risk management. This standard offers managerial guidance for implementing effective risk management, and an overview of its defined process is illustrated in Figure 4.

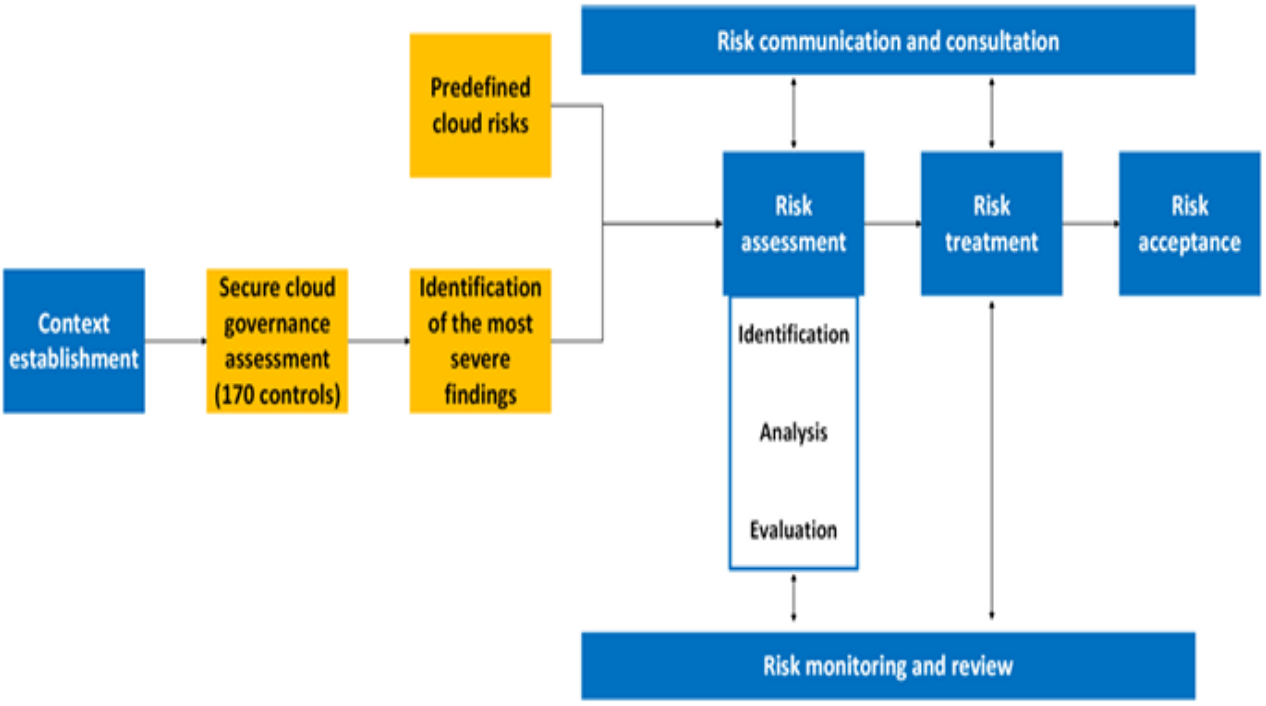


Figure 4. Risk management process based on the ISO/IEC 27005 standard.

According to ISO/IEC 27005, the risk management process consists of six main components, as illustrated in Figure 5. The first phase, context establishment, involves identifying both external and internal factors relevant to risk management. This includes defining the purpose, scope, and boundaries of the risk assessment, as well as determining the organization's risk appetite and the criteria for risk evaluation and acceptance [21]. The second phase, risk assessment, is further divided into three sub-phases: risk identification, risk analysis, and risk evaluation. In the risk identification stage, analysts identify potential sources of harm, including assets, threats, vulnerabilities, existing controls, and possible consequences. The risk analysis phase involves selecting an analysis method—qualitative or quantitative—and assessing the likelihood of incidents along with their potential impact to determine risk levels. Next, in the risk evaluation phase, the calculated risk levels are compared against the previously defined evaluation and acceptance criteria to determine their significance. The risk treatment phase follows, in which appropriate controls and countermeasures are developed to address the identified risks. These risks, along with their severity and proposed mitigation strategies, are then presented to stakeholders, who collaborate to decide which risks should be addressed and how. Common treatment strategies include risk reduction, risk retention (acceptance), risk avoidance, and risk sharing [22].

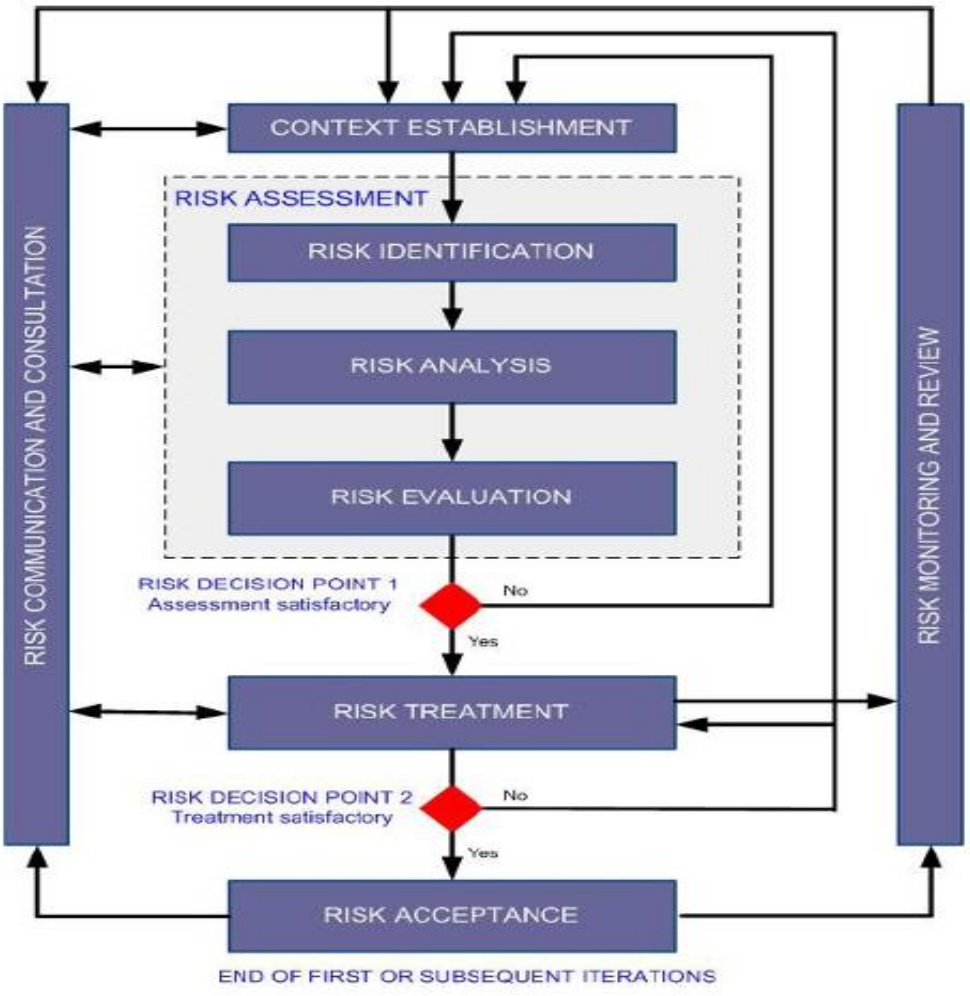


Figure 5. Risk management process based on ISO/IEC 27005

3.1 Service models of cloud computing

Cloud computing architecture is generally divided into two main components: the front end, which is the user-facing interface for interacting with cloud services, and the back end, which encompasses the infrastructure and service models that deliver those services. The back end is comprised of three primary cloud service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [23]. Each model serves different types of users and organizational needs, offering distinct functionalities and benefits.

IaaS (Infrastructure as a Service) provides access to fundamental computing resources such as virtual machines, storage, servers, and networking infrastructure. While IaaS offers scalability and flexibility, it also poses specific security challenges, such as securing virtual machine instances and hypervisors, protecting against unauthorized access, and ensuring data isolation in multi-tenant environments. A key concern is the potential misalignment between the security policies of cloud providers and clients, particularly regarding data retention and destruction. Additionally, the use of outdated or legacy code by clients can introduce vulnerabilities into the system.

PaaS (Platform as a Service) delivers platforms for application development and deployment, offering tools and services that simplify the software development lifecycle. However, it introduces its own security issues, including interoperability risks, vulnerabilities in platform components, and the need for secure authorization and authentication mechanisms. Ensuring the protection of sensitive data processed by platform services and guarding against flaws in custom-developed applications are also critical concerns.

SaaS (Software as a Service) eliminates the need for local installations by providing software applications over the internet. While SaaS offers convenience and ease of access, it comes with security risks related to data privacy, compliance in shared environments, account hijacking, and unauthorized access. Security management in SaaS includes implementing robust authentication and authorization, ensuring data encryption and availability, and managing the overall security of data handled by the service provider. Figure 6 illustrates the types of users associated with each service model along with real-world application examples, helping to clarify the practical use and security implications of each model within the cloud ecosystem [24].

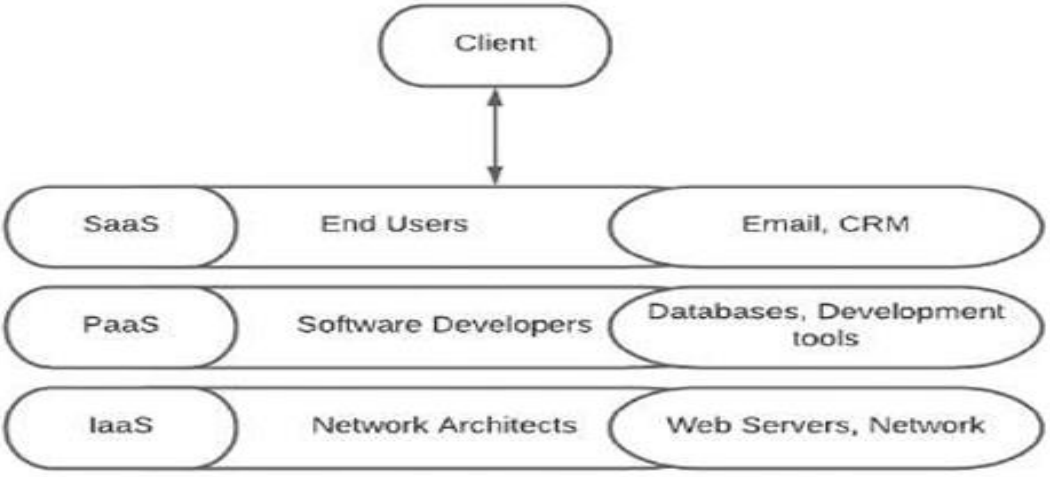


Figure 6. Cloud Service Model

4. Analysis and results

4.1 Classification of threats for each service model

Table 1 presents a classification of common cyber threats associated with the Platform as a Service (PaaS) model in cloud computing. It outlines five major threat categories, each accompanied by a brief description and relevant examples. Cloud Service Abuse refers to the misuse of cloud resources for fraudulent or malicious activities, often resulting from unidentified or unauthorized logins, leading to service downtime and reduced trust. Insecure Interface highlights risks arising from improper authentication and authorization during data transmission, which can lead to data breaches, unauthorized access, and privacy violations. Malicious Insiders involve threats posed by users with privileged access who may intentionally or unintentionally compromise system resources, causing productivity losses and reputational harm. Data Leakage pertains to the unauthorized exposure or theft of sensitive information, typically due to insecure interfaces or poor data handling practices. Lastly, Platform Vulnerabilities stem from misconfigurations or outdated security settings in the platform infrastructure, potentially leading to application compromises, data manipulation, and service outages. This classification emphasizes the importance of robust security practices in managing PaaS environments.

Table 1. Classification of cyber threats in PaaS.

Threats	Description	Example
Cloud Service Abuse	Abuse of cloud services including validation loss, fraud, and attacks due to unidentified logins.	• Fraudulent activities • misuse of services • downtime affecting trust
Insecure Interface	Improper authorization and authentication during data transmission.	• Data breaches • unauthorized access

		• privacy violations
Malicious Insiders	Infiltration of resources by privileged users.	• Productivity losses • operational impacts • reputational damage
Data Leakage	Unauthorized access to or theft of confidential data.	• Exposure through poorly secured interfaces • employee mismanagement
Platform Vulnerabilities	Misconfigurations or outdated platform security settings.	• Compromised applications • data manipulation • outages

Table 2 outlines key cyber threats associated with the Software as a Service (SaaS) model in cloud computing, highlighting the nature of each threat and providing practical examples. Data Breaches involve unauthorized access to or exposure of sensitive data stored in SaaS environments, potentially resulting in confidentiality loss, legal consequences, and erosion of customer trust. Account Hijacking occurs when attackers gain control over user accounts through stolen credentials, leading to data loss, resource misuse, and unauthorized system access. Denial of Service (DoS) attacks target SaaS endpoints with excessive traffic, disrupting service availability and causing outages, customer dissatisfaction, and revenue loss. Vendor Lock-in refers to the difficulty of migrating services due to dependence on a particular provider, which can reduce flexibility, increase operational costs, and lead to service disruptions during provider transitions. Lastly, Social Engineering includes phishing and similar tactics aimed at deceiving users into revealing credentials or installing malware, granting attackers' unauthorized access to sensitive resources. This classification emphasizes the importance of robust user awareness, access control, and incident response measures in securing SaaS environments.

Table 2. Classification of cyber threats in SaaS.

Threat	Description	Example
Data Breaches	Unauthorized access or exposure of sensitive SaaS-hosted data.	• Loss of confidentiality • legal penalties • customer distrust
Account Hijacking	Illegal control of accounts by unauthorized users.	• Stolen credentials leading to data loss and resource misuse.
Denial of Service (DoS)	Overloading SaaS endpoints with excessive requests to disrupt service availability.	• Service outages • dissatisfied customers • revenue loss
Vendor Lock-in	Dependence on specific providers, making migration difficult.	• Reduced flexibility • increased costs • service disruption during provider changes
Social Engineering	Phishing attacks targeting SaaS users to steal credentials.	• Unauthorized access to sensitive resources • malware installation

Table 3 provides a classification of major cyber threats specific to the Infrastructure as a Service (IaaS) model in cloud computing, describing each threat along with relevant examples. Malware refers to malicious software that targets virtual machines and servers, such as Trojans and ransomware, which can cause data breaches and prolonged system downtime. Infrastructure Weaknesses include vulnerabilities in the physical or virtual components of the infrastructure, often leading to unauthorized access and data theft. Advanced Persistent Threats (APTs) are long-term, targeted attacks where intruders stealthily exploit the IaaS environment over extended periods for continuous data theft, espionage, and financial damage. Physical Infrastructure Attacks involve direct attacks on the hardware or data centers that support the cloud infrastructure, resulting in hardware damage, data loss, and extended service outages. Finally, Unauthorized Access stems from weak authentication mechanisms or insecure management interfaces, allowing attackers to take control of cloud resources and cause significant operational disruptions. This classification highlights the critical need for strong access control, infrastructure hardening, and continuous monitoring in securing IaaS environments.

Table 3. Classification of cyber threats in IaaS.

Threat	Description	Example
Malware	Malicious software affecting virtual machines and servers.	• Trojans • Ransomware leading to data breaches and system downtime.
Infrastructure Weaknesses	Vulnerabilities in the underlying physical or virtual infrastructure.	• Unauthorized access to resources • Data theft.
Advanced Persistent Threats (APTs)	Long-term, targeted attacks exploiting IaaS environments.	• Persistent data theft • Espionage • financial loss
Physical Infrastructure Attacks	Direct attacks on servers or data centers.	• Hardware damage • data loss • prolonged outages
Unauthorized Access	Weak authentication or insecure management interfaces.	• Gaining control of cloud resources, leading to operational disruption.

4.2 Classification of vulnerabilities for each service model

Table 4 outlines key cyber vulnerabilities commonly found in Platform as a Service (PaaS) environments, highlighting the areas where security weaknesses may arise. Unsecured APIs refer to application programming interfaces that lack proper access controls or input validation, making them prime targets for exploitation by attackers. Misconfigured Security involves improperly set permissions, exposed databases, or overly permissive access configurations, all of which can lead to unauthorized access and data exposure. Lack of Security Baselines points to the absence of standardized security configurations, resulting in inconsistent and potentially insecure resource deployments. Platform Layer Vulnerabilities arise from flaws or misconfigurations in middleware or operating systems, which can serve as entry points for attackers. Finally, Shared Responsibility Gaps highlight confusion or lack of clarity in defining which security tasks are handled by the cloud provider versus the customer, often leading to overlooked vulnerabilities. These findings underscore the need for clear security guidelines, regular configuration audits, and a well-defined shared responsibility model in PaaS environments.

Table 4. Classification of cyber vulnerabilities in PaaS.

Vulnerability	Description
Unsecured APIs	APIs without proper access controls or input validation, making them susceptible to exploitation.
Misconfigured Security	Incorrect permissions, exposed databases, or overly permissive access settings.
Lack of Security Baselines	Absence of predefined security controls for configuring resources securely.
Platform Layer Vulnerabilities	Errors or misconfigurations in middleware or operating systems.
Shared Responsibility Gaps	Unclear division of responsibilities between cloud provider and the customer.

Table 5 presents a classification of common cyber vulnerabilities within the Software as a Service (SaaS) model, focusing on areas that can compromise the security of cloud-hosted applications. Weak Authentication refers to the use of insufficient login protections, such as the absence of multi-factor authentication (MFA) and reliance on weak password policies, which can easily be exploited by attackers. Vendor Dependency highlights the risks of placing too much trust in cloud service providers without properly assessing their security practices, potentially leaving organizations exposed to vulnerabilities beyond their control. Data Breaches result from unauthorized access to sensitive information hosted on SaaS platforms, often due to poor security controls. Limited Monitoring and Logging denotes the lack of effective logging and monitoring mechanisms, which can delay or prevent the detection of security incidents. Insecure Data Storage involves improperly configured storage systems, such as publicly accessible storage buckets with inadequate access restrictions,

leading to data exposure. These vulnerabilities emphasize the need for strong authentication practices, thorough vendor evaluation, and robust monitoring and data protection measures in SaaS environments.

Table 5. Classification of cyber vulnerabilities in SaaS.

Vulnerability	Description
Weak Authentication	Lack of multi-factor authentication (MFA) and weak password policies.
Vendor Dependency	Over-reliance on cloud vendors without evaluating security practices.
Data Breaches	Unauthorized access to or exposure of sensitive SaaS-hosted data.
Limited Monitoring and Logging	Absence of comprehensive logging configurations to detect security breaches.
Insecure Data Storage	Improperly configured storage buckets with weak access control.

Table 6 identifies and classifies critical cyber vulnerabilities in Infrastructure as a Service (IaaS) environments, focusing on weaknesses that can compromise the security and integrity of cloud infrastructure. Outdated Software refers to the use of unpatched or unsupported software versions that contain known vulnerabilities, increasing the risk of exploitation. Infrastructure Layer Vulnerabilities encompass weaknesses within core components such as virtualization platforms, storage systems, and network infrastructure, which can be targeted to gain unauthorized access or disrupt services. Management Interface Vulnerabilities involve poor access control mechanisms for administrative interfaces, potentially allowing attackers to take over cloud resources. Browser Vulnerabilities arise when attackers exploit flaws in client browsers to hijack user sessions or steal sensitive data during interactions with IaaS platforms. Inadequate Encryption points to the use of weak or absent encryption protocols for data in storage or during transmission, leaving sensitive information exposed to interception or theft. These vulnerabilities underline the importance of regular software updates, strong access controls, secure encryption practices, and continuous monitoring in IaaS security management.

Table 6. Classification of cyber vulnerabilities in IaaS.

Vulnerability	Description
Outdated Software	Using software with known vulnerabilities due to lack of timely updates.
Infrastructure Layer Vulnerabilities	Vulnerabilities in virtualization, storage, and networking components.
Management Interface Vulnerabilities	Weak access controls for administrative consoles.
Browser Vulnerabilities	Exploitation of client browser flaws to hijack sessions or steal data.
Inadequate Encryption	Lack of strong encryption protocols during data storage or transmission.

4.3 Classification of countermeasures for each service model

Table 7 outlines the most critical security countermeasures for protecting Platform as a Service (PaaS) environments, emphasizing practices that address common vulnerabilities and enhance overall platform security. API Security Measures involve securing APIs through the use of access controls, API gateways, input validation, and secure token-based authentication to prevent unauthorized access and exploitation. SSL/TLS Encryption ensures that data transmitted between applications and endpoints remains confidential and protected from interception. Penetration Testing is used to simulate real-world cyberattacks, helping to uncover potential security flaws within the platform before they can be exploited. Service Integrity Checks are conducted to verify that any integrated or injected services do not contain malicious code or compromise the platform's functionality. Finally, Multi-layered Authentication strengthens access control by implementing additional verification methods, such as multi-factor authentication (MFA), to prevent unauthorized access. These countermeasures collectively contribute to building a secure and resilient PaaS environment.

Table 7. Classification of the most critical security countermeasures for PaaS.

Countermeasure	Description
API Security Measures	Implements access controls, API gateways, input validation, and secure token authentication.
SSL/TLS Encryption	Protects data during transmission between applications and endpoints.
Penetration Testing	Simulates attacks to identify vulnerabilities in the platform.
Service Integrity Checks	Validates that injected services do not introduce malicious functionalities.
Multi-layered Authentication	Enhances security with additional verification layers such as MFA.

Table 8 highlights the most essential security countermeasures for safeguarding Software as a Service (SaaS) environments, focusing on strategies that protect data, ensure compliance, and reduce human-related risks. Multi-Factor Authentication (MFA) enhances account security by requiring multiple forms of identity verification, thereby reducing the risk of unauthorized access. Data Loss Prevention (DLP) solutions monitor and control the movement of sensitive data to prevent unauthorized sharing or leakage. Compliance Audits are conducted to verify that the SaaS environment adheres to legal and regulatory standards such as GDPR and HIPAA, helping to avoid penalties and maintain customer trust. Backup and Disaster Recovery ensures data availability and business continuity by regularly backing up critical data and implementing effective recovery protocols in the event of system failures or attacks. Lastly, Training Programs aim to raise awareness among employees about cyber threats, such as phishing, and promote best practices in data security and compliance. These countermeasures play a vital role in maintaining the security, reliability, and regulatory alignment of SaaS services.

Table 8. Classification of the most critical security countermeasures for SaaS.

Countermeasure	Description
Multi-Factor Authentication (MFA)	Requires additional layers of identity verification to prevent unauthorized access.
Data Loss Prevention (DLP)	Tools to restrict unauthorized data sharing and monitor sensitive data transfers.
Compliance Audits	Ensures adherence to data protection regulations and standards such as GDPR and HIPAA.
Backup and Disaster Recovery	Maintains regular data backups and recovery protocols to ensure data availability.
Training Programs	Educates staff on phishing prevention, data security practices, and compliance requirements.

Table 9 presents the most critical security countermeasures essential for securing Infrastructure as a Service (IaaS) environments, targeting the protection of virtual infrastructure and network integrity. VM Isolation is a foundational control that ensures virtual machines (VMs) are properly segregated, preventing unauthorized access between tenants in a shared environment. Intrusion Detection Systems (IDS) are used to monitor network traffic and detect suspicious or unauthorized activities, enabling rapid response to potential threats. Regular Patching involves the continuous updating of virtual machines and associated software to fix known vulnerabilities and reduce exposure to exploits. Network Segmentation divides the cloud infrastructure into distinct segments, isolating sensitive data and systems from general or public access, thus minimizing the attack surface. Rootkit Detection focuses on identifying and eliminating malicious rootkits that could

compromise hypervisors or the underlying system integrity. Together, these countermeasures are vital for maintaining the security, performance, and trustworthiness of IaaS platforms.

Table 9. Classification of the most critical security countermeasures for IaaS.

Countermeasure	Description
VM Isolation	Ensures that virtual machines are segregated to prevent unauthorized cross-access.
Intrusion Detection Systems (IDS)	Monitors network traffic to detect and prevent unauthorized activities.
Regular Patching	Keeps virtual machines and software updated to address known vulnerabilities.
Network Segmentation	Divides cloud networks into segments to isolate sensitive data from general access.
Rootkit Detection	Identifies malicious rootkits within hypervisors to secure the system integrity.

Table 10 provides a mapping of appropriate security countermeasures to address common threats within Infrastructure as a Service (IaaS) environments. For Malware, recommended controls include regular software updates, the deployment of Endpoint Protection Software (EPS), and the use of antivirus/antimalware tools to detect and neutralize malicious code. To mitigate Infrastructure Weaknesses, organizations should perform regular vulnerability assessments, enforce secure configurations, and implement robust monitoring tools to detect anomalies. Advanced Persistent Threats (APTs) require continuous monitoring, the use of Intrusion Detection Systems (IDS), and well-defined incident response plans to identify and respond to stealthy, long-term attacks. Physical Infrastructure Attacks can be countered with strong physical security measures, reliable backup systems, and redundant infrastructure to ensure continuity in the event of hardware compromise. Finally, to prevent Unauthorized Access, it is essential to implement strong authentication protocols, comprehensive Identity and Access Management (IAM), and role-based access controls (RBAC) to enforce proper user privileges and restrict access. This table highlights the importance of aligning security controls with specific threat types to effectively safeguard IaaS environments.

Table 10. Mapping the suitable countermeasures with against threats in IaaS (Infrastructure as a Service).

Threat	Control Measures
Malware	• Regular software updates • Endpoint Protection Software (EPS) • Antivirus/Antimalware tools
Infrastructure Weaknesses	• Regular vulnerability assessments • secure configurations • monitoring tools
Advanced Persistent Threats (APTs)	• Continuous monitoring • intrusion detection systems (IDS) • incident response planning
Physical Infrastructure Attacks	• Physical security measures • backup systems • redundant infrastructure
Unauthorized Access	• Strong authentication protocols • Identity and Access Management (IAM) • role-based access controls (RBAC)

Table 11 outlines effective countermeasures tailored to specific cyber threats within Platform as a Service (PaaS) environments. For Cloud Service Abuse, key controls include implementing API security measures, using SSL/TLS encryption to protect data in transit, and conducting service integrity checks to detect unauthorized or malicious modifications. To address Insecure Interfaces, the use of secure APIs, multi-layered authentication mechanisms, and thorough input validation helps prevent unauthorized access and data breaches. Against Malicious Insiders, organizations should enforce Role-Based Access Control (RBAC), maintain detailed logging and auditing of user activities, and apply the principle of least privilege to minimize internal risks. Data Leakage can be mitigated through strong encryption for both data at rest and in transit, regular compliance audits to ensure adherence to data protection standards, and Data Loss Prevention (DLP) tools to monitor and restrict unauthorized data transfers. Finally, to counter Platform Vulnerabilities, regular penetration testing, service integrity checks, and secure communication protocols like SSL/TLS are essential for identifying and mitigating weaknesses in the platform layer. This mapping underscores the importance of targeted, layered security strategies to protect PaaS environments.

Table 11. Mapping the suitable countermeasures with against threats in PaaS (Platform as a Service).

Threat	Control Measures
Cloud Service Abuse	• API security measures • SSL/TLS encryption • service integrity checks
Insecure Interface	• API security measures • multi-layered authentication • input validation
Malicious Insiders	• Role-based access control (RBAC) • logging and auditing • least privilege principle
Data Leakage	• Data encryption (at rest and in transit) • regular compliance audits • data loss prevention (DLP)
Platform Vulnerabilities	• Regular penetration testing • service integrity checks • SSL/TLS encryption

Table 12 presents a mapping of appropriate security countermeasures to mitigate key threats in Software as a Service (SaaS) environments. To protect against Data Breaches, essential measures include encrypting data both at rest and during transmission, conducting regular compliance audits, and implementing strong Identity and Access Management (IAM) systems. For Account Hijacking, multi-factor authentication (MFA), user education and training, and the enforcement of strong password policies help prevent unauthorized account access. Denial of Service (DoS) attacks can be mitigated through Distributed Denial of Service (DDoS) protection tools, load balancing to distribute traffic evenly, and traffic filtering to block malicious requests. To address Vendor Lock-in, strategies such as adopting hybrid cloud models, evaluating service level agreements (SLAs) carefully, and implementing multi-cloud approaches provide greater flexibility and reduce dependency on a single provider. Finally, Social Engineering threats can be countered through phishing awareness training, email filtering solutions to block suspicious content, and robust incident response planning to quickly contain and address attacks. This table emphasizes the need for proactive and layered defenses tailored to the unique challenges of SaaS environments.

Table 12. Mapping the suitable countermeasures with against threats in SaaS (Software as a Service)

Threat	Control Measures
Data Breaches	• Data encryption (at rest and in transit) • compliance audits • Identity and Access Management (IAM)
Account Hijacking	• Multi-factor authentication (MFA) • user education/training

	• strong password policies
Denial of Service (DoS)	• Distributed Denial of Service (DDoS) protection • load balancing • traffic filtering
Vendor Lock-in	• Hybrid cloud strategies • careful SLA evaluation • multi-cloud adoption
Social Engineering	• Phishing awareness training • email filtering • incident response planning

5. Conclusion

This study provides a comprehensive exploration of cloud computing, its architectural models, service delivery frameworks (SaaS, PaaS, and IaaS), and the unique security challenges associated with each. While cloud computing offers scalable, flexible, and cost-effective solutions for modern businesses, it also introduces critical vulnerabilities, especially in multi-tenant environments. Through a detailed examination of cyber threats—including data breaches, deception attacks, DoS attacks, and insider threats—and associated vulnerabilities such as weak authentication, misconfigured security settings, and insecure APIs, the article emphasizes the importance of adopting a layered and model-specific security approach. The research highlights the vital role of risk assessment and risk management based on established standards like ISO/IEC 27005:2018, which guide organizations in identifying, evaluating, and mitigating threats across cloud environments. By classifying and mapping threats and vulnerabilities to suitable countermeasures for each service model, the article presents a practical framework for strengthening cloud security. Key countermeasures such as multi-factor authentication, intrusion detection systems, encryption, data loss prevention, and secure API practices are shown to be essential in defending against both external and internal threats. Ultimately, this study underscores that securing cloud systems is not a one-size-fits-all solution. Instead, it requires a thorough understanding of the architecture, shared responsibility models, and unique characteristics of each service type. Organizations must adopt proactive security strategies, regularly assess their risk posture, and align with best practices and standards to build trust, ensure compliance, and maintain the integrity and availability of their cloud-based services.

6. Implications of the research

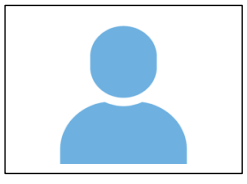
The findings of this research have several important implications for both academic and practical domains within the field of cloud computing security. Firstly, the study reinforces the necessity of adopting a service-model-specific approach to cloud security. By distinguishing between the security needs of SaaS, PaaS, and IaaS, the research helps cloud consumers and providers allocate responsibilities more effectively and implement tailored security measures aligned with the shared responsibility model. This enhances the overall security posture of organizations utilizing cloud technologies. Secondly, the classification and mapping of threats, vulnerabilities, and countermeasures serve as a valuable framework for cybersecurity professionals, offering a structured methodology for identifying potential risks and applying relevant controls. Organizations can use this framework to design more effective risk assessment and mitigation strategies, leading to better-informed decisions about cloud adoption, architecture, and vendor selection. Thirdly, by integrating the ISO/IEC 27005:2018 risk management standard into the analysis, the study emphasizes the importance of standardized practices in achieving regulatory compliance and improving resilience to evolving cyber threats. This is especially significant for industries dealing with sensitive data and facing strict data protection laws such as GDPR and HIPAA.

Furthermore, the research highlights the need for continuous security awareness and training across all levels of an organization, especially in SaaS environments where user behavior plays a crucial role in maintaining security. The insights also support future research directions, such as the development of intelligent threat detection systems, automated risk assessment tools, and advanced encryption techniques tailored for dynamic cloud environments. Overall, this research provides a solid foundation for enhancing strategic decision-making, policy development, and technical implementations related to cloud security, offering both preventive and responsive solutions to the complex challenges posed by modern cloud infrastructures.

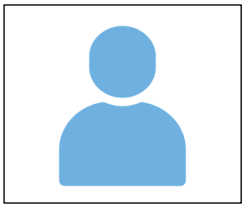
References

[1] Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and security of cloud computing: a complete guideline. Symmetry, 15(11), 1981.
[2] Zbořil, M. (2022). Risk Assessment Method of Cloud Environment. Computing and Informatics, 41(5), 1186-1206.
[3] Shajan, A., & Rangaswamy, S. (2021). Survey of security threats and countermeasures in cloud computing. United International Journal for Research & Technology, 2(7), 201-207.
[4] Hashim, W., & Hussein, N. A. H. K. (2024). Securing Cloud Computing Environments: An Analysis of Multi-Tenancy Vulnerabilities and Countermeasures. SHIFRA, 2024, 9-17
[5] Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., ... & Kim, K. I. (2021). A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures, and challenges. Electronics, 10(15), 1811.
[6] Kumar, A., & Kumar, K. A. (2022). A Survey on Cloud Computing Security Threats, Attacks and Countermeasures: A Review. International Journal of Human Computations & Intelligence, 1(3), 13-18
[7] Abdullayeva, F. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. Results in Control and Optimization, 12, 100268.
[8] Fadhil, I. S. M., Nizar, N. B. M., & Rostam, R. J. (2023). Security and privacy issues in cloud computing. Authorea Preprints.
[9] Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber security threats in cloud: Literature review. In 2021 international conference on information technology (ICIT) (pp. 779-786). IEEE
[10] Journal of Computers and Applications, 46(5), 348-361.Rani, P., Singh, S., & Singh, K. (2024). Cloud computing security: a taxonomy, threat detection and mitigation techniques. International Journal of Computers and Applications, 46(5), 348-361.
[11] Pericherla, S. S. (2023). Cloud Computing Threats, Vulnerabilities and Countermeasures: A State-of-the-Art. ISC Int. J. Inf. Secur., 15(1), 1-5.
[12] Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2024). Information security risk assessment methods in cloud computing: Comprehensive review. Journal of Computer Information Systems, 1-28.
[13] Wang, Y., Zhu, M., Yuan, J., Wang, G., & Zhou, H. (2024). The intelligent prediction and assessment of financial information risk in the cloud computing model. arXiv preprint arXiv:2404.09322.
[14] Yanamala, A. K. Y. (2024). Emerging challenges in cloud computing security: A comprehensive review. International Journal of Advanced Engineering Technologies and Innovations, 1(4), 448-479.
[15] Devi, T. A., & Jain, A. (2024, May). Enhancing Cloud Security with Deep Learning-Based Intrusion Detection in Cloud Computing Environments. In 2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT) (pp. 541-546). IEEE.
[16] Sanagana, D. P. R., & Tummalachervu, C. K. (2024, May). Securing Cloud Computing Environment via Optimal Deep Learning-based Intrusion Detection Systems. In 2024 Second International Conference on Data Science and Information System (ICDSIS) (pp. 1-6). IEEE.
[17] Aljuaid, W. A. H., & Alshamrani, S. S. (2024). A deep learning approach for intrusion detection systems in cloud computing environments. Applied Sciences, 14(13), 5381.
[18] Alsadie, D. (2024). Artificial intelligence techniques for securing fog computing environments: trends, challenges, and future directions. IEEE Access.
[19] Alam, M., Shahid, M., & Mustajab, S. (2024). Security challenges for workflow allocation model in cloud computing environment: a comprehensive survey, framework, taxonomy, open issues, and future directions. The Journal of Supercomputing, 80(8), 11491-11555.
[20] Prakash, S., Malaiyappan, J. N. A., Thirunavukkarasu, K., & Devan, M. (2024). Achieving regulatory compliance in cloud computing through ML. AIJMR-Advanced International Journal of Multidisciplinary Research, 2(2).
[21] Awan, I. A., Sumra, I. A., Mahmood, K., Akram, M., Mujahid, S. K., & Zaman, M. I. (2024). A Reliable Approach For Data Security Framework In Cloud Computing Network. Migration Letters, 21(S11), 923-934.
[22] Hassan, O. F., Fatai, F. O., Aderibigbe, O., Akinde, A. O., Onasanya, T., Sanusi, M. A., & Odukoya, O. (2024). Enhancing Cybersecurity through Cloud Computing Solutions in the United States. Intelligent Information Management, 16(4), 176-193.
[23] Kirti, M., Maurya, A. K., & Yadav, R. S. (2024). Fault-tolerance approaches for distributed and cloud computing environments: A systematic review, taxonomy and future directions. Concurrency and Computation: Practice and Experience, 36(13), e8081.

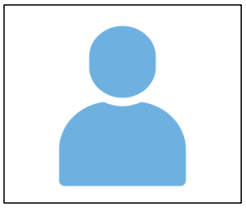
Biographies



Rasha Almanasir in Cybersecurity program from the University of Jordan, Jordan. Her research interests include cybersecurity, cybersecurity risk assessment and cryptographic.



Deyaa Al-solomon in Cybersecurity program from the University of Jordan, Jordan. Her research interests include cybersecurity, cybersecurity risk assessment and cryptographic.



Saif Indrawes in Cybersecurity program from the University of Jordan, Jordan. Her research interests include cybersecurity, cybersecurity risk assessment and cryptographic.

Dr. Mohammed Almaiah is an Associate Professor in the Department of Computer Science at University of Jordan. Almaiah is among the top 2% scientists in the world from 2020 up to now. He is working as Editor in Chief for the International Journal of Cybersecurity and Risk Assessment. He has published over 115 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain.

Dr. Umar Islam is from Pakistan and he received his Master in Computer Science degree from COMSATS University in 2018. He is a Ph.D. scholar and currently working as a lecturer at IQRA National University, Swat campus. He has several research projects and articles on IoT, machine learning, and cybersecurity. His research interests include Machine Learning, Federated Learning, cybersecurity, the Internet of Things, and Artificial Intelligence.

Dr. Marwan Alshar'e is an Assistant Professor of Computer Science at Sohar University, Oman. With over 15 years of academic and research experience across international institutions, his expertise spans cybersecurity, information systems design, artificial intelligence, and e-learning. He has led and contributed to several funded research projects and published extensively in Scopus-indexed journals. Dr. Alshar'e also serves on multiple editorial boards and research committees and is actively involved in program coordination and academic development initiatives at his institution.