STAP
Smart Technologies Academic Press

Jordanian Journal of Informatics and Computing
https://jjic.thestap.com/

Risk Assessment for Identifying Threats, vulnerabilities and countermeasures in Cloud Computing

Santosh Reddy Addula[1], Sajedeh Norozpour[2], Mohammed Amin[3]

[1]*Department of Information Technology, University of the Cumberlands, United States, USA*

[2] *Istanbul Gelişim University. Istanbul, Türkiye*

[3] *King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan*

ARTICLE INFO

Article History

Received 10-01-2025
Revised 23-04-2025
Accepted 05-06-2025
Published 07-06-2025

Academic Editor:

Dr. Shahed Almobydeen

Vol.2025, No.1

DOI:
https://doi.org/10.63180/jjic.thestap.2025.1.5

ABSTRACT

The main objective of this study is to conduct a comprehensive analysis of cyber risks in cloud computing, including classifying threats, vulnerabilities, impacts, and countermeasures. This classification helps to identify suitable security controls to mitigate cyber risks for each type of threat. Additionally, this study aims to explore the main vulnerabilities in terms of infrastructure, service and platform in cloud computing. This study uses the content analysis technique to collect, analyze, and classify data in terms of types of threats, vulnerabilities, and countermeasures. The methodology comprises four primary stages: (1) identifying key components, (2) threat identification, (3) vulnerability identification, and (4) countermeasure identification. The results indicate that DoS attacks and account hijacking attacks were the most prevalent infrastructure vulnerabilities in cloud computing, each accounting for 14% and 10% of incidents. The results found that unpatched software and weak access controls were classified as the most critical threats in the service level in cloud computing, comprising 17% and 12% of incidents, respectively. The results also indicated that encryption methods, access controls mechanisms and firewall malware protection are the most significant and effective countermeasures for protecting the infrastructure, service and platform in cloud computing environment. The findings of this study provides valuable recommendations for academic research in classifying the different types of cyber threats and understanding the significant security controls against cyber-attacks in cloud computing.

Keywords: Risk Assessment, Cloud Computing, Cybersecurity, Cyber Threats, Countermeasures.

How to cite the article

Addula, S. R., Norozpour, S., Amin, M., & . (2025). Risk Assessment for Identifying Threats, vulnerabilities and countermeasures in Cloud Computing. Jordanian Journal of Informatics and Computing, 2025(1), 38–48. https://doi.org/10.63180/jjic.thestap.2025.1.5

*Corresponding author. Email: saddula5840@ucumberlands.edu

1. Introduction

Cloud computing is a broad term that describes the move to the cloud and a mobile workforce, which has brought new security risks [1]. Cloud account takeover, data oversharing, and usage of unapproved cloud applications present considerable challenges to security teams. Cloud security encompasses the technologies, applications, controls, and policies that protect people, data, and infrastructure from cyber-attacks and compliance risks on cloud computing platforms [2]. It involves a comprehensive set of security measures designed to address both external and internal security threats to organizations, including controlling security, compliance, and other usage risks of cloud computing and data storage. By guarding data and assets, cloud security services provide a critical safety net for organizations that rely on cloud-based solutions. It establishes increased reliability and availability of information, reduces upfront and ongoing costs related to data protection, enables easier scalability, and provides improved protection against sophisticated attacks on people and systems [3][4].

Cloud computing may give organizations agility, but it can also open up vulnerabilities for organizations that lack the internal knowledge and skills to understand security challenges in the cloud effectively [5][6]. Poor planning can manifest itself in misunderstanding the implications of the shared responsibility model, which lays out the security duties of the cloud provider and the user. Traditional data center security models are not suitable for the cloud. Administrators must learn new strategies and skills specific to cloud computing. This misunderstanding could lead to the exploitation of unintentional security holes in cloud computing environment. All organizations face security risks, threats, and challenges every day [7][8]. For instance, an API endpoint hosted in the cloud and exposed to the public Internet is a risk, the attacker who tries to access sensitive data using that API is the threat, and organization's challenge is effectively protecting public APIs while keeping them available for legitimate users or customers who need them. Therefore, understanding these threats and risks will help security analysts better protect your cloud assets.

Previous studies have highlighted several security issues in cloud computing, including misconfiguration, insecure interfaces, unmanaged attack surface and human errors [9][10][11]. These vulnerabilities may lead to data breaches, unauthorized access, and service interruptions. Cyber criminals often exploit vulnerabilities and weaknesses in cloud security to gain access to valuable data and assets. Once attackers' access cloud account credentials, they impersonate legitimate users. They can trick your people into wiring money to them or releasing corporate data. They can also hijack email accounts to distribute spam and phishing emails. Recent years have witnessed numerous cybersecurity attacks on cloud computing. For example, a study of over 1,000 cloud service tenants with over 20 million user accounts found over 15 million unauthorized login attempts in the first half of 2019 alone. More than 400,000 of these attempts resulted in successful logins. About 85% of tenants were targeted by cyber-attacks, and 45% had at least one compromised account in their environment. Therefore, understanding potential threats is crucial in risk assessment and should be considered when developing a robust security strategy to prevent data breaches. Security risk assessment plays a vital role in identifying potential threats, implementing proactive security measures, and mitigating the likelihood of successful attacks. Cybersecurity risk assessment for cloud computing is an ongoing process rather than a one-time task. By identifying and classifying risks, implementing appropriate security controls, and evaluating their effectiveness, organizations can significantly reduce potential threats and risks in cloud computing. Consequently, the study purpose to achieve the following objectives: (1) To determine the critical cybersecurity threats in cloud computing, (2) To determine the critical cybersecurity vulnerabilities in cloud computing and (3) To determine the critical cybersecurity countermeasures in cloud computing.

2. Related works

[12] Discussed the potential vulnerabilities in smart cities networks, the types of cyber- attacks they may face, and the impact of these attacks on the safety and functionality of autonomous vehicles. [13], the study focused on the advantages and disadvantages of using the cloud for information security management, outlining the importance of enterprises of using cloud computing which is important for protecting sensitive data, cyber threats and the services that the cloud computing provides which are Software-as- a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS). Another study by [14] focused on the advantages and disadvantages of using the cloud for information security management, outlining the importance of enterprises of using cloud computing which is important for protecting sensitive data, cyber threats and the services that the cloud computing provides which are Software-as- a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS). [15] Presented in this study provided the main cloud security requirements, identified threats, vulnerabilities, and countermeasures. In addition, this work identified a unified requirements for security threats, vulnerabilities and countermeasures in cloud computing. In the same way, [16] discussed the maintenance of the cloud computing security, the baseline security requirements within an enterprise to manage risks according to this article confidentiality and privacy, data

infringement obligations, and third- party commitments in cloud computing arrangements. If a risk has already gone undetected and is under way in the cloud one of the first steps to be taken is to have risk evaluation, it's usually done by pinpointing the whereabouts of the risk monitoring it, and analyzing its criticalness. [17] Conducted a systematic review of the critical challenges and vulnerabilities in cloud computing, with a particular emphasis on security and privacy issues. The work evaluated potential threats ranging from data breaches to unauthorized access, and it evaluates the repercussions of these challenges on user trust and data integrity within cloud infrastructure. The Cloud Security Alliance has published a report titled "Top Threats on Cloud Computing 2024" as shown in Table 1.

Table 1. Top Threats on Cloud Computing 2024

No.	Top Threats on Cloud Computing
1.	Misconfiguration and inadequate change control
2.	Identity and Access Management
3.	Insecure interfaces and APIs
4.	Inadequate selection/implementation of cloud security strategy
5.	Insecure third-party resources
6.	Insecure software development
7.	Accidental cloud disclosure
8.	System vulnerabilities
9.	Limited cloud visibility/observability
10.	Unauthenticated resource sharing
11.	Advanced Persistent Threats

3. Research design and methodology

This section outlines the research design for proposing a risk assessment methodology for cloud computing. The methodology comprises four primary stages: (1) identifying key components, (2) threat identification, (3) vulnerability identification, and (4) countermeasure identification. Each stage is informed by the findings from the literature review. The primary objective of this risk assessment framework is to provide a robust and comprehensive approach for addressing all types of threats, vulnerabilities, and countermeasures in cloud computing. Figure 1 illustrates the main stages of the risk assessment framework.

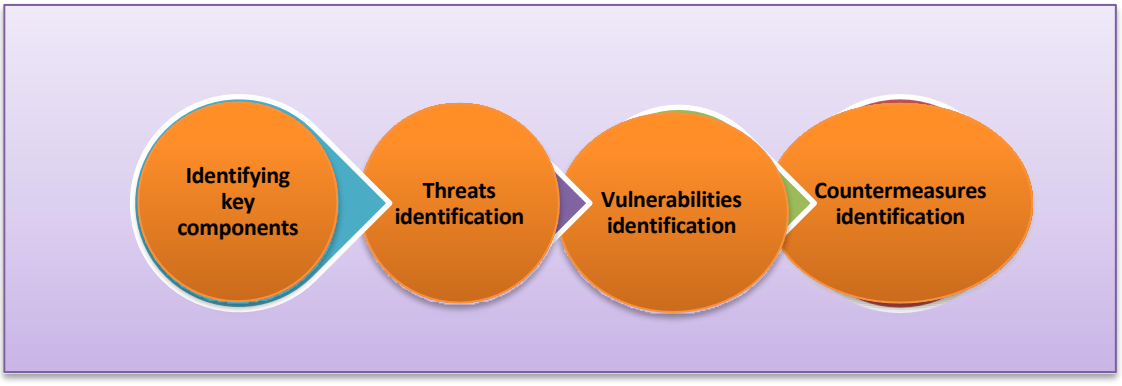

Figure 1. The Main Stages of Methodology.

3.1 Stage One: Identifying key components

The initial phase of the risk assessment framework involves compiling data from literature review findings to establish the dataset for this study. This process entails a comprehensive examination of existing studies, models, frameworks, and literature in the field of cloud computing. The collected data encompasses threat types, vulnerability categories, and countermeasure methodologies. The information gathered during this stage will undergo analysis in subsequent phases.

3.2 Stage Two: Threats identification

Following data collection in the first stage, the subsequent phase involves analyzing the gathered information to identify and categorize existing cybersecurity threats in cloud computing. This stage encompasses a comprehensive and systematic process that identifies various types of threats with the potential to exploit vulnerabilities in database systems, potentially resulting in compromised systems.

3.3 Stage Three: Vulnerabilities identification

In the third stage, following data collection, an analysis is conducted to identify existing technical security vulnerabilities that could potentially compromise cloud computing. This stage of the risk assessment framework incorporates a comprehensive systematic review to determine critical vulnerability types that may be exploited to breach cloud computing.

3.4 Stage Four: Countermeasures identification

The final phase of the risk assessment framework involves identifying and categorizing effective countermeasures to address potential cybersecurity threats and vulnerabilities in cloud computing. The identification of these countermeasures is directly linked to all types of threats and vulnerabilities identified in the previous stages' findings. Consequently, this stage provides solutions to mitigate potential threats that could compromise the integrity of cloud computing.

This sections illustrates the primary components of the research methodology. The methodology comprises three main steps: (1) threat identification, (2) vulnerability identification, and (3) countermeasure identification. The following subsections will provide detailed explanations of each step within the methodology.

4. Threats Identification

The threat classification is categorized into three main groups: (1) Infrastructure threats, (2) Service threats and (3) Platform threats. Infrastructure threats encompass malware types that exploit security weaknesses in the IT infrastructure of cloud computing, such as data breaches, cloud service abuse and hijacking. Service threats include service delivery threats and insecure interface threats. Platform threats include two types are malicious insiders and identity theft. The classification analysis is based on multiple dimensions, including threat characteristics, behaviors, and their impacts. Each threat type is described with an explanation of its potential impact on cloud computing. The subsequent subsections provide a detailed threats classification on cloud computing.

Table 2. Classification of cyber threats based on infrastructure, services and platforms.

Area	Threats	Problems	Affected services	Solutions
Infrastructure threats	Data breaches	Unauthorized access or retrievalof data, application, or service	IaaS, SaaS, and PaaS	Encryption of data, proofs of storage, server-aided secure computation
	Cloud service abuse	loss of validation service fraud and more vigorous attacks dueto unidentified login	PaaS and IaaS	Monitor network status and provide robust registration and authentication
	Hijacking	Illegal control of certain authorized services by unauthorized users. Stolen user account credentials	IaaS, SaaS, and PaaS	Adopt a robust authentication mechanism, security policies, and a secure communication channel

Service threats	Service delivery	loss of control of cloud infrastructure	IaaS, SaaS, and PaaS	Offer services that monitor and control cloud infrastructure
	Insecure interface	Improper authorization and incorrect authentication transmission of content	IaaS, SaaS, and PaaS	Transmission of data is encrypted, and there are authentication mechanisms
Platform threats	Malicious insiders	Infiltration of organizational resources, destruction of asset productivity losses, and impact on operations	IaaS, SaaS, and PaaS	Security and management processes that use protocol reports and breach notifications
	Identity theft	An attacker could gain the identity of a valid user to access the usage resources	IaaS, SaaS, and PaaS	Use strong multilayer passwords and authentication mechanisms

4.1 Classification of Infrastructure Threats

As discussed in the preceding section, we categorize cyber threats in cloud computing into infrastructure threats, as illustrated in Table 3. Infrastructure threats encompass malware types that exploit security weaknesses in the IT infrastructure of cloud computing, such as data breaches, cloud service abuse and hijacking. According to Table 3, data breaches, it happens when a cybercriminal successfully infiltrates a data source and extracts sensitive information. Data loss is another type of threats, which happens human mistake, hard drive failure, power outage, or malware infection. Denial of service (DoS) is one of the critical threats in cloud computing, where the attacker sends many requests to the system, the system gets overwhelmed and down. In addition, account hijacking is another threat, through the act of stealing the login credentials for unethical reasons. Advanced persistent threats, it is happened when the attacker infiltrates networks to worm their way into an organization's cloud- based systems and steal sensitive information. As outlined in Table 3, security attacks on passwords can be categorized into different types:

1. Intelligent Brute-Force Attacks: Brute-force attacks are a trial-and-error technique in which the attacker submits many username and password combinations until something works. What makes such attacks intelligent is using automated tools to expose multiple combinations of usernames with passwords in large credential dumps.
2. Advanced Phishing Campaigns: Otherwise known as "credential phishing," these targeted and well-crafted campaigns come in various forms and deceive people into revealing their authentication credentials. Attackers usually carry out phishing via socially engineered emails.
3. Password Recycling: This common cloud security threat is characterized by the same password used across multiple accounts. If an attacker gets their hands on an account's credentials from an unrelated data breach, they can leverage password recycling to breach other sensitive accounts and data.
4. Data Loss and IP Theft: On any typical business day, people share information with colleagues, partners, and others via cloud-based collaboration or messaging tools. However, a lack of employee training on cloud security or worker malice could result in sharing sensitive data with those who shouldn't be able to see it.
5. Malicious File Shares: Phishing links, credential stealers, and downloaders are typically used in these types of attacks. Threat actors also distribute malware via cloud services such as Dropbox.
6. Data Breaches: One of the most significant risks associated with cloud security is the potential for a data breach. Hackers can gain access to cloud-based systems and steal sensitive information, such as financial data, personal information, or intellectual property.

Table 3. Classification of infrastructure threats in cloud computing

Threat	Impact	Vulnerabilities	Countermeasures
Data breaches	Disclosure of sensitive information to unauthorized parties	Target attack, simple human Errors, application vulnerabilities.	Encryption, regular Audits.
Data loss	the unavailability of data	Simple human error, natural disasters, hard drive failures, power failures, malware infection.	Data backup, disaster recovery plans, redundant storage.
Denial of service (DoS)	system or service is inaccessible to the legitimate users	Weak network architecture, insecure network protocol, vulnerable application.	Rate limiting, traffic filtering.
Vulnerable systems an APIs	compromise of the subsystem or the entire system	Weak API credentials, key management, operating system bugs, hypervisor bugs, unpatched software.	Patching, API security
Weak authentication and identity management	circumvention of the system security measures	Malware infection, social engineering attacks, man-in-the-middle attack.	Multi-factor authentication, strong password policies.
Account hijacking	Stolen credentials of cloud users or operators may allow illegitimate users to use the cloud resources for nefarious purpose	Malware infection, social engineering attacks, man-in-the-middle attack.	Multi-factor authentication
Shared technology vulnerabilities	virtual machines and hypervisor might allow the attacker to compromise all the users sharing the resources	Hypervisor bugs, virtual machine vulnerabilities, third-party and software vulnerabilities.	Hypervisor security.
Lacking due diligence	A cloud consumer must periodically review the accreditations and standards followed by the cloud service provider	No auditing, service levelagreement.	Service legal agreements.
Lack of responsibility	lead to service unavailability or a data breach	Service level agreement, human negligence.	Employee training, security policies.

4.2 Classification of Service cloud threats

Service cloud threats encompass Insecure APIs vulnerabilities that can be used to access cloud-based services can be vulnerable to attacks, such as injection or man-in-the-middle attacks. Another threat called Advanced Persistent Threats (APTs): These sophisticated, long-term cyber-attacks are characterized by their discreet, persistent nature. APTs commonly target large, high-value organizations and are frequently backed by well-funded, state-sponsored groups or highly skilled threat actors. Service delivery threat which happened when loss of control of cloud infrastructure. Insecure interface threat also happened when an improper authorization and incorrect authentication transmission of content. Table 4 presents the main threats under the service cloud.

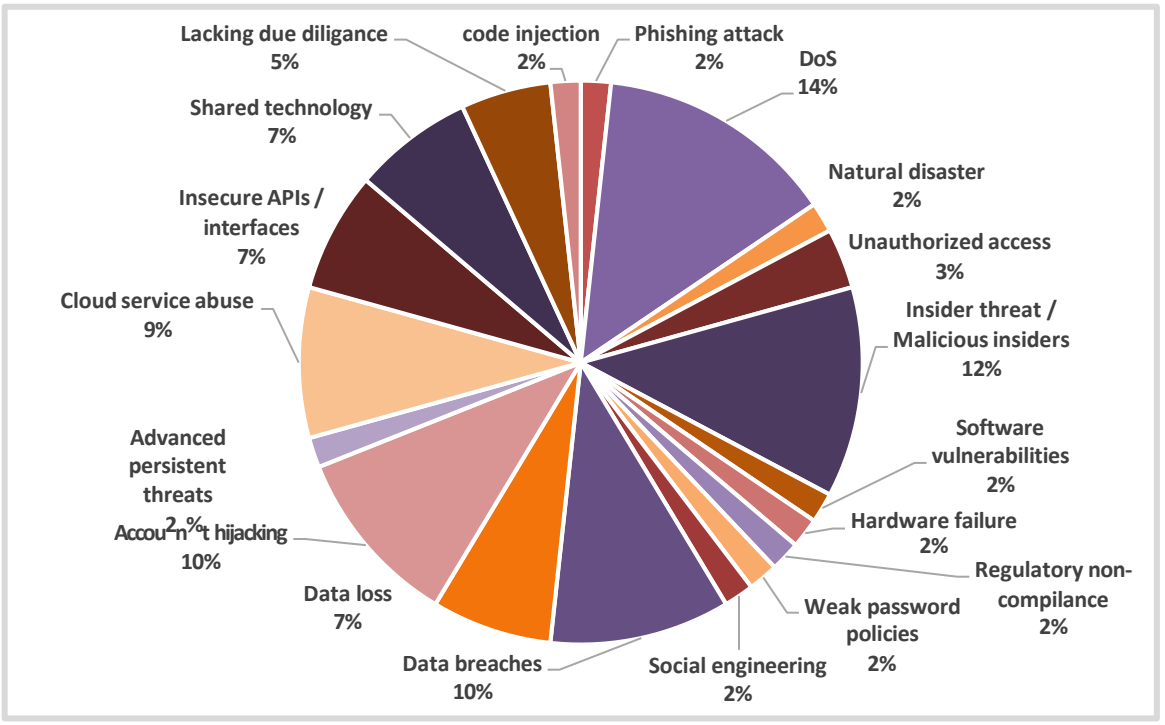

Figure 2. Analysis of classifications of Infrastructure vulnerabilities.

Table 4. Classification of service threats in cloud computing

Threats	Description	Countermeasures
Vulnerability in API Security	Despite the usefulness of APIs in protecting cloud services, their efficacycould be compromised due to the accessibility of few cloud services. Consequently, openly accessible cloud services are susceptible tounauthorized access, heightening the risk of hacking by malicious actors.	Robust API authentication Model
Unintended Data Exposure	Improper access control of object storage buckets and data stores is a significant contributing factor to cloud data breaches, potentially resulting in unauthorized viewing, alteration,or removal of private data.	Secure Data Transmission
Code injection threat	These virtual attacks involve illegal SQL injection on a computer, which exploits unreliable interfaces to execute unauthorized SQL statements. Theobjective of such attacks is to gain unauthorized access to personal information, thereby compromising individuals' privacy.	Input validation & parametrized queries includingprepared statements
Service delivery threat	Service delivery threat which happened when loss of control of cloud infrastructure.	
Insecure interface threat	Insecure interface threat also happened when an improper authorization and incorrect authentication transmission of content	

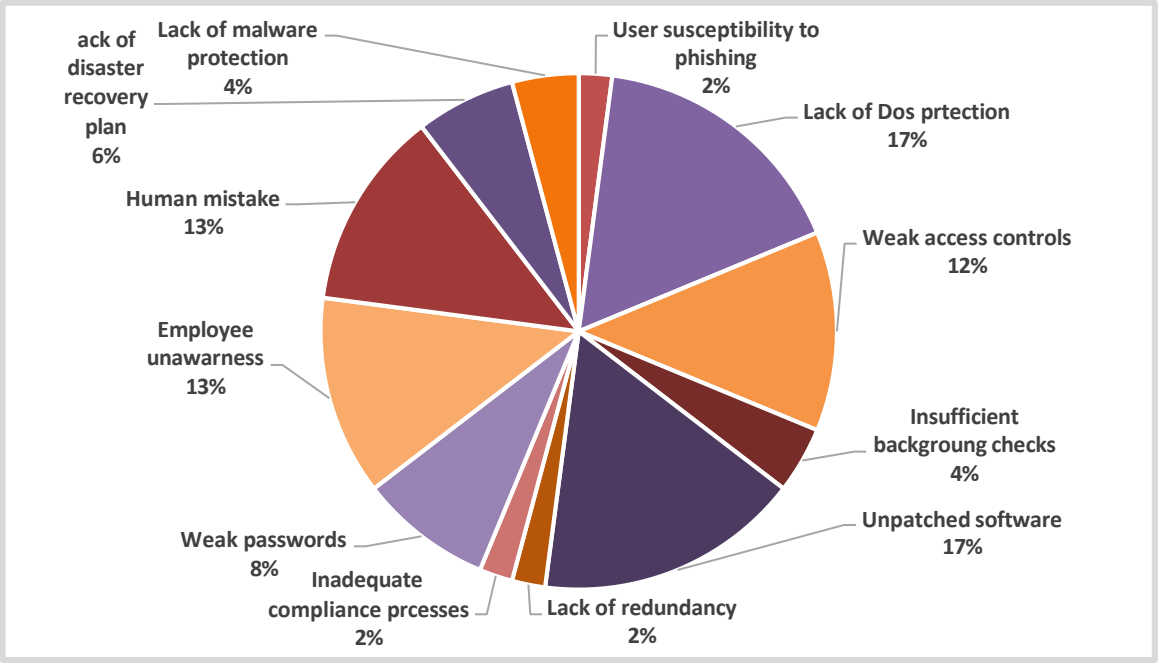

Figure 3. Analysis of classifications of Service threats.

5. Vulnerabilities Identification

The second step of the methodology aims to identify the technical security vulnerabilities that could be exploited to compromise the cloud computing' assets. These vulnerabilities may be associated with either single or multiple operational or cyber security threats. Vulnerability scans and assessments are crucial steps in the risk assessment process to identify critical technical vulnerabilities. In this study, the classification of vulnerabilities is divided into twenty main categories: weak authentication, untrusted third-party, unnecessary third-party granted access, software bugs, unpatched database, insecure coding practices, weak security controls, weak audit trail, limited security expertise and education, unmanaged sensitive data, insecure network, password misuse, platform vulnerabilities, integration challenges, management complexity, weak encryption practices, weak data masking, multiple usage of an account, weak security awareness, and ineffective key management. Table 5 summarizes the main technical vulnerabilities in cloud computing, describing these vulnerabilities and their impacts.

Table 5. Classification of technical vulnerabilities in cloud computing.

Vulnerabilities	Description and Impact
Weak Authentication [6] [7]	Users using weak authentication leads to attackers easily guessing the credentials. Lack of proper training or understanding of company policies can lead to catastrophic loss to an organization.
Untrusted third-party [7]	Third-party systems may not have the same level of security as the enterprise's internal systems, and they may not be updated or maintained regularly.
Third-party unnecessary granted access [4]	Granting unnecessary access to a third-party admin to a database allows the admin to use this vulnerability to harm the system by modifying, stealing data, or even shutting the system down.
Software Bugs [5]	A bug is a problem within software that causes it to work in an improper way, which means it might perform functions while it is not supposed to or not perform other functions it is supposed to.

Unpatched Database [1] [5]	An incorrect configuration of a system puts it at risk by exposing the system's sensitive data and code. As organizations take months to patch databases, the attackers have more time to exploit the vulnerabilities and launch their attacks.
Insecure Coding Practices [3] [5]	A vulnerability in databases with a lack of secure coding practices makes the system insecure, causing breaches and loss of data and information. Improper implementation or management of encryption can result in vulnerabilities that can expose data to attackers.
Weak Security Controls [5]	Security threats are malicious attacks that affect a system and cause harm to it. In databases, a threat involves SQL and non-SQL to inject malicious code into a system.
Weak Audit Trail [1] [3]	Main vulnerabilities of audit trail: 1. Information overload: large batches of data can lead to overwhelming security terms making it difficult to identify. 2. False positive: lead to alert fatigue and potential oversight of critical incidents. 3. High costs: implementing and maintaining auditing and monitoring systems can be expensive, involving costs for tools and storage.
Limited Security Expertise and Education [1]	Many organizations struggle to keep up with data growth and are prepared for security breaches. The lack of expertise is the main cause, so they don't handle incidents properly.
Unmanaged Sensitive Data [1]	Sensitive data in databases will be exposed to threats if the required controls and permissions are not implemented.
Insecure network [3]	Passwords transmitted over insecure networks can be intercepted by hackers.
Passwords misusage [3]	Using weak passwords or using the same password for many accounts allows the attacker to guess the password easily and access all accounts that use it.
Platform Vulnerabilities [4]	Unauthorized entry, data corruption, or service denial can result from flaws in underlying working frameworks and extra services installed on a database server.
Integration challenges [3]	Complex integration means that integrating monitoring tools with existing systems can create gaps in coverage.
Management complexity [3]	Configuration challenges because complex setup and management can lead to ineffective threat detection.
Weak Encryption practices [3]	Poor key management can compromise encryption. If encryption keys are not securely stored, rotated, or managed, encrypted data can become vulnerable to unauthorized access.
Weak Data Masking [3]	Poorly implemented data masking can lead to decreased protection of sensitive data and complexity of permission management to the overall access control system.
Multiple usage of an account [1] [3]	When numerous people use the same account, it's more difficult to determine who is responsible for any given action.
Weak security awareness [1]	Database users make the database vulnerable by creating attack points that may be exploited by attackers such as setting weak password and not modifying the default password.
Ineffective key management [3]	Poor key management can compromise encryption. If encryption keys are not securely stored, rotated, or managed, encrypted data can become vulnerable to unauthorized access.

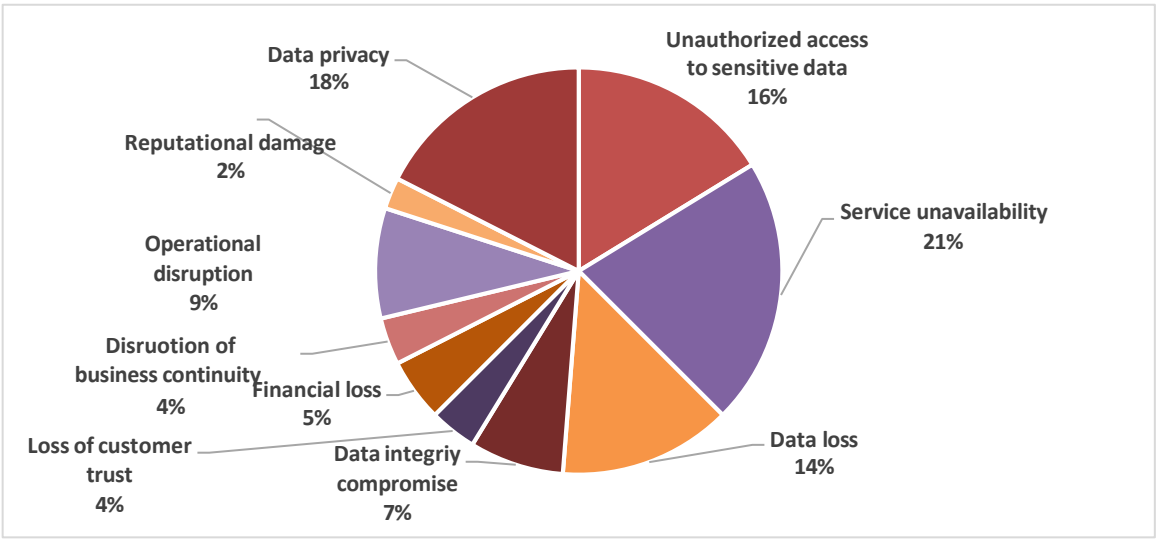

Figure 4. Analysis of classifications of the main impacts of vulnerabilities in cloud computing.

6. Countermeasures Identification

In this phase, we conduct a comprehensive analysis of essential countermeasures aimed at reducing and mitigating the impact of vulnerabilities associated with cyber threats. Our study identified a range of security controls designed to enhance cloud computing system security against cyber-attacks. These measures include data encryption, access control, authentication, firewalls, data backup, behavior detection, spam detection, security audits, anomaly detection methods, and others, as illustrated in Table 4. Security controls and countermeasures are mechanisms and tools developed to protect cloud computing from cyber threats and attacks.

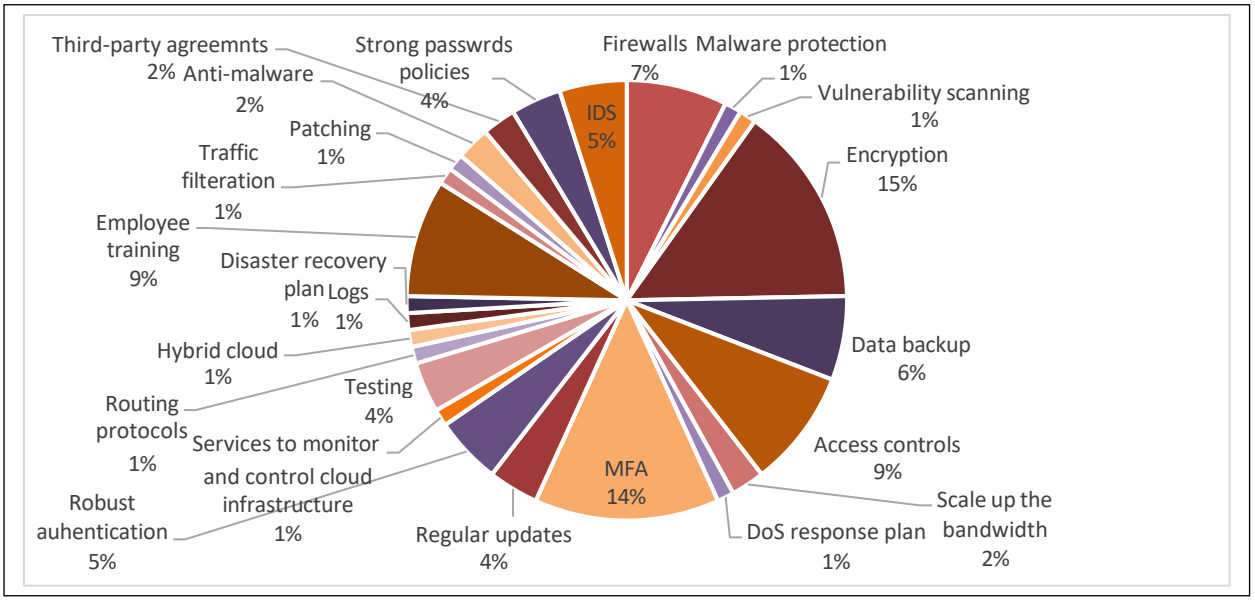

Figure 5. Analysis of classifications of the main countermeasures in cloud computing.

These countermeasures are crucial for maintaining data integrity and safeguarding database systems from unauthorized access. They can be categorized into several types based on their functions, usage, effectiveness, and importance. As shown in Figure 4 encryption methods are considered one of the most powerful technical security controls for database systems, protecting sensitive data and preventing unauthorized access. Multi-factor authentication is also a robust technique for preventing unauthorized access to sensitive data and database systems. Firewalls offer monitoring capabilities for databases

and defend them against attacks. Using the logs they maintain, they can audit and monitor all database access. Firewalls provide a level of control over network traffic and prevent unauthorized access to sensitive data. Network segmentation helps restrict the spread of cyberattacks throughout the network and isolate vital resources and assets. IDPS is designed to detect and respond to new and advanced attacks. IDS evaluate data using network traffic, database operations, SQL queries, system logs, and other sources. When an attack is identified, IPS stop them by disabling connections, blacklisting IP addresses, or modifying firewall settings. IDPS combine signature-based and behavioral detection approaches, which help identify zero-day attacks. Figure 6 represents the most common countermeasures in database systems.

7. Conclusion

In the recent years, cybersecurity-threats are the most critical challenges facing cloud computing as well as increasing the number of cyber-attacks on cloud computing systems and becoming more sophisticated. Cyber-attacks in the cloud computing systems can cause a huge impact, including data loss, reputation damage, and failure of the system. Thus, it is necessary to understand the behavior of cyber threats on cloud computing systems and identify the suitable countermeasures to mitigate their impacts. Therefore, cyber-risk classifications and assessment play a prime role in risk management and establish a significant framework for determining and responding to cyber-threats. Risk assessment helps for understanding the impact of cyber-threats and develops appropriate security controls to mitigate the risk. This study provided a comprehensive analysis of cyber risks in the cloud computing systems, including classifying threats, attacks, impact and countermeasures. This classification assists to understand the suitable security controls to mitigate the cyber risks for each kind of threat. The results indicate that DoS attacks and account hijacking attacks were the most prevalent infrastructure vulnerabilities in cloud computing, each accounting for 14% and 10% of incidents. The results found that unpatched software and weak access controls were classified as the most critical threats in the service level in cloud computing, comprising 17% and 12% of incidents, respectively. The results also indicated that encryption methods, access controls mechanisms and firewall malware protection are the most significant and effective countermeasures for protecting the infrastructure, service and platform in cloud computing environment. The findings of this study provides valuable recommendations for academic research in classifying the different types of cyber threats and understanding the significant security controls against cyber-attacks in cloud computing.

Funding

No funding.

Author contributions

Conceptualization, S.R.A.; methodology; S.N; formal analysis, M.A; investigation, S.R.A.; resources, S.N.; writing original draft preparation, M.A.; writing—review and editing, S.R.A., S.N and M.A. All authors have read and agreed to the published version of the manuscript.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Use of Generative Artificial Intelligence

The authors declare that no generative artificial intelligence tools were used in the preparation of this manuscript.

References

[1] 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.

[2] Dutta, A., Peng, G. C. A., & Choudhary, A. (2013). Risks in enterprise cloud computing: the perspective of IT experts. *Journal of Computer Information Systems*, *53*(4), 39-48.

[3] 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.

[4] Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review, 33, 1-48.

[5] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of internet services and applications*, *4*(1), 5.
[6] Tsai, C. L., Lin, U. C., Chang, A. Y., & Chen, C. J. (2010, August). Information security issue of enterprises adopting the application of cloud computing. In *The 6th International Conference on Networked Computing and Advanced Information Management* (pp. 645-649). IEEE.
[7] Sasubilli, M. K., & Venkateswarlu, R. (2021, January). Cloud computing security challenges, threats and vulnerabilities. In *2021 6th international conference on inventive computation technologies (ICICT)* (pp. 476-480). IEEE.
[8] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), 583-592.
[9] El Kafhali, S., El Mir, I., & Hanini, M. (2022). Security threats, defense mechanisms, challenges, and future directions in cloud computing. *Archives of Computational Methods in Engineering*, *29*(1), 223-246.
[10] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. *Electronics*, *11*(20), 3330.
[11] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.
[12] 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.
[13] Peng, G. C. A., Dutta, A., & Choudhary, A. (2013, October). Exploring critical risks associated with enterprise cloud computing. In *International Conference on Cloud Computing* (pp. 132-141). Cham: Springer International Publishing.
[14] 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.
[15] Verma, A., & Kaushal, S. (2011, July). Cloud computing security issues and challenges: a survey. In *International conference on advances in computing and communications* (pp. 445-454). Berlin, Heidelberg: Springer Berlin Heidelberg.

Biographies

Dr. Santosh Reddy Addula, SMIEEE, currently works as a researcher at the Department of Information Technology at the University of the Cumberlands. His research focuses on Artificial Intelligence, Machine Learning, IoT, Cybersecurity, Blockchain, Cloud Computing, Automation and Robotics, Finance, IT Healthcare and Supply Chain Management. Santosh is dedicated to advancing knowledge and developing innovative solutions in these fields. He has demonstrated expertise across multiple domains. Santosh is an innovator with a strong portfolio of patents and has significantly contributed to academic research through his articles as an author and co-author. Additionally, he serves as a reviewer for esteemed journals, reflecting his dedication to advancing knowledge and ensuring the quality of scholarly publications in his field. saddula5840@ucumberlands.edu

Dr Sajedeh Norozpour, Assistant Prof, Istanbul Gelisim University, Istanbul, Turkiye. snorozpour@gelisim.edu.tr

Dr. Mohammed Amin 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. M.almaiah@ju.edu.jo