EXAMINING CLOUD SECURITY: IDENTIFYING RISKS AND THE IMPLEMENTED MITIGATION STRATEGIES

EMAN AL-QTIEMAT[1] , ZEYAD AL-ODAT[2]

[1]Full Time Lecturer, Tafila Technical University, Department of Computer Science, Tafila, Jordan

[2]Assistant Professor. Tafila Technical University, Department of Computer and Communications Engineering, Tafila, Jordan

E-mail: [1]eman.alqtiemat@ttu.edu.jo, [2]zeyad.alodat@ttu.edu.jo

ABSTRACT

Cloud computing is critical for modern enterprises, because of its scalability, cost-effectiveness, and adaptability. However, these benefits are offset by security risks and obstacles, which makes cloud computing a two-edged sword. Although technology offers many benefits and services, it also puts data and businesses at risk if security threats are not carefully addressed or if security flaws are discovered after the fact. This paper examines the primary security flaws caused by cloud computing and the existing countermeasures for those flaws. The paper examines cloud models, service models, and distinguishes several deployment models. An analysis of security countermeasures for cyber threats is presented. Furthermore, the work investigates the regulatory environment controlling cloud security, considering compliance frameworks and standards that influence the creation and implementation of security solutions. The study contributes to a more nuanced knowledge of the problems and opportunities in cloud security, as well as practical advice for enterprises looking to improve their cloud security posture. In addition, some recommendations for identifying and averting cloud security risks are presented.

Keywords: *Cloud, Cloud Risks, Security, Cyber Threats, Security Countermeasures.*

1. INTRODUCTION

Cloud computing is a technological and service paradigm for delivering computer resources and services via the internet. The fundamental concept of cloud computing is to eliminate the need for physical, on-premises infrastructure by offering on-demand access to a variety of IT resources, such as servers, storage, databases, networking, software, etc... [1].

Cloud computing protects confidential and sensitive information including intellectual property information, financial data, and information related to clients of important companies and institutions. Therefore, it is necessary to ensure the availability and confidentiality of sensitive data, including preventing data access from unauthorized parties [2]. Cloud services provide protection of data from disasters that might happen to institutions such as fires, wars, floods, or any other natural disaster [3]. In addition, using cloud computing reduces the cost by sharing available resources and operational resources [3].

Security of the cloud is still a challenge. Since more and more companies are storing their data in the cloud, it is imperative to protect the cloud from all known threats [4]. By the end of 2025, 100 zettabytes of data will be stored in the cloud. A hundred billion terabytes is that amount [5]. However, the cloud is the source of 45% of data breaches. According to a recent survey, 80% of organizations had at least one cloud security issue in 2022, and 27% of enterprises had experienced a public cloud security event, up 10% from 2022 [6].

Security issues, such as data breaches, may pose a threat to the reputation of organizations and undermine customer confidence. With the development of security attacks and the emergence of new risks that threaten data security, the cloud needs to adapt to developments and develop adequate protection methods against sophisticated vulnerabilities such as ransomware, zero-day vulnerabilities, and advanced persistent threats (APTs) [7].

It appears that worries about security are becoming more and more prevalent, which could endanger data and cloud resources. For instance, when examining an attack such as phishing attack, its associated risk has been escalated by 33% in 2022 compared to 2020 [8].

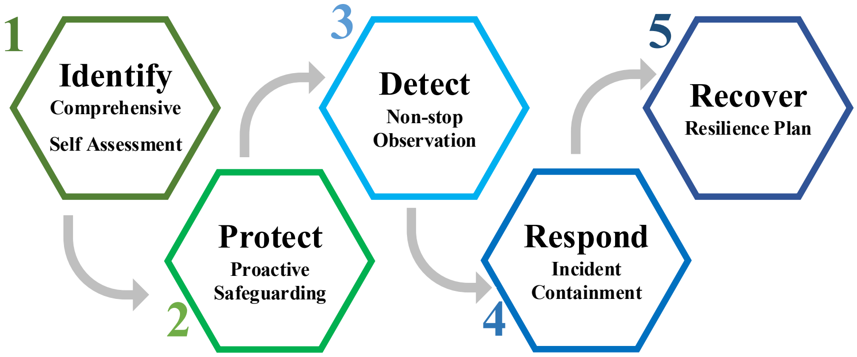

Figure 1: NIST CSF Framework Core Structure

Sharing responsibility of protecting data is the mission and role of institutions alongside the cloud. The institutions must play their role in securing data against security challenges and preserve their reputation and customers' confidence in them [7]. Therefore, working on cloud security is an investment that serves the interests of organizations [7].

The Cybersecurity Framework (CSF), provided by NIST, is a set of guidelines that aid companies and organizations in understanding the cybersecurity risks that may affect their data and work. NIST CSF, Figure 1 shows the core structure that the businesses should flow.

Setting guidelines and providing recommendations to safeguard enterprises against unforeseen risks requires the use of the NIST CSF Framework [9], [10]. The NIST framework's five primary cybersecurity functions are defined as follows:

- Identify: Understand and prioritize assets, risks, and vulnerabilities within the organization.
- Protect: Implement safeguards and measures to protect assets and systems from cyber threats.
- Detect: Develop and implement systems for detecting cybersecurity events and incidents.
- Respond: Have response plans and procedures in place to mitigate the impact of cybersecurity incidents.
- Recover: Develop and implement plans for recovering from cybersecurity incidents and restoring normal operations. The rest of the paper is organized as follows.

This work makes several contributions to the existing literature while also highlighting areas where further research is needed. The contributions are as follow:

- Comprehensive Analysis of Cloud Security Risks: The paper provides a comprehensive analysis of various security risks associated with cloud computing. It covers a wide range of threats including data breaches, access control issues, compliance violations, DDoS attacks, insider threats, misconfigurations, and others.
- Detailed Examination of Security Countermeasures: The paper presents detailed insights into security countermeasures to mitigate cloud security risks. It discusses strategies such as Identity and Access Management (IAM), data encryption, network security, incident response planning, secure coding techniques, and shared responsibility models. This contribution adds value by providing practical guidance on implementing effective security measures in cloud environments, which can help organizations enhance their security posture.
- Emphasis on Shared Responsibility Model: The work emphasizes the shared responsibility model between cloud service providers and customers, particularly in terms of security obligations. It delineates the responsibilities of each party across different types of cloud services (SaaS, PaaS, IaaS). This contribution addresses a critical aspect of cloud security governance and clarifies the roles and responsibilities of stakeholders.
- Focus on Continuous Improvement and Adaptation: the importance of continuous improvement, adaptation, and proactive measures in cloud security. It emphasizes the dynamic nature of security threats and advocates for ongoing updates to security policies and practices.
- Identification of Future Research Directions: The work identifies future research directions,

particularly in the development of novel data security strategies to address outstanding issues in cloud security. This contribution guides researchers towards areas where further investigation is warranted, such as the integration of emerging technologies (e.g., artificial intelligence, blockchain) into cloud security frameworks, or the exploration of regulatory and compliance challenges in multi-cloud environments.

Despite the growing employment of cloud computing, security remains a major concern for organizations. Existing literature provides insights into various security risks and countermeasures in cloud environments. However, there are gaps in understanding the effectiveness of security countermeasures, the implications of emerging technologies, and the complexities of compliance in multi-cloud environments. As a result, there is a need for further research to address these gaps and enhance the security posture of cloud-based systems [11], [12].

The rest of the paper is organized as follows: An overview of the background is presented in Section 2. Section 3 details the related work.

Section 4 illustrates the security risks in the cloud.

Section 5 illustrates details about security countermeasures of the cloud. Section 6 gives an analysis of cloud security countermeasures. Conclusions and directions for future work are noted in Section 7.

2. BACKGROUND

Cloud computing provides many service deployment models. The cloud services are categorized into four different models. This categorization is not limited to what is mentioned here, but we adopt this type as a generic categorization model. On the other hand, we categorized the cloud deployment into six different models. The following text provides a brief illustration of each model, as shown in Figure 2.

The cloud service models are as follows:

- Software as a Service (SaaS): This model offers software applications over the Internet such as Gmail and Microsoft Office 365, these applications are accessible from anywhere without running or installing them on local devices. Software updates are done regularly by the SaaS providers [13].
- Platform as a Service (PaaS): PaaS offers a platform for developers that consists of the required tools and services to build, manage, and deploy applications. Examples of PaaS are Google App Engine and Microsoft Azure App Service which simplifies the applications' development process [13].
- Infrastructure as a Service (IaaS): IaaS provides virtualized computing resources through the internet, such as storage, virtual machines (VMs), storage, and networking. Amazon Web Services (AWS) EC2, Google Compute Engine, and Microsoft Azure Virtual Machines are examples of IaaS [14].
- Container as a Service (CaaS): It is a cloud service that works on container management. CaaS offers platforms and tools for managing and scaling containerized applications [14], for instance, Kubernetes, Docker Swarm, and Google Kubernetes Engine (GKE) are considered CaaS.

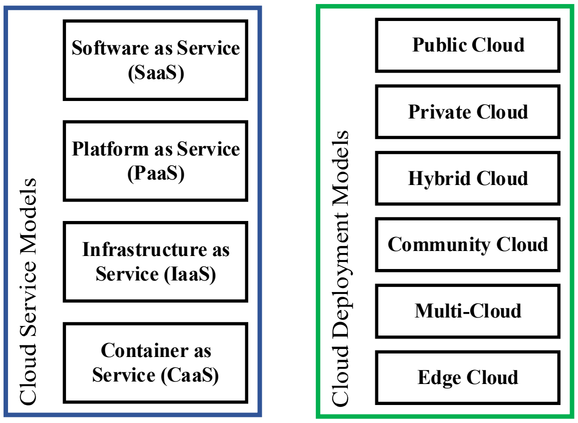

Figure 2: Cloud Models: Service Models and Deployment Models

Organizations usually choose a combination of the four mentioned models to meet their specific requirements and establish a comprehensive cloud strategy.

Availability of resources and services for cloud users requires different approaches supported by different deployment models, as shown in Figure 2. There are several deployment models and use cases for each type as follows:

- Public Cloud: According to this model, the computational resources and services are owned and managed by external service providers. These services are provided based on payment options, either pay as you go or through a subscription [15]. Examples of public cloud are

Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and IBM Cloud. This publishing method is flexible, scalable, and cost-effective.

- Private Cloud: Cloud services and resources are exploited exclusively to serve a single organization by hosting a private cloud locally and are not allowed to be used by the public. This feature makes this type suitable for organizations with special security and compliance requirements [15]. Examples of this deployment model are VMware vCloud and OpenStack.
- Hybrid Cloud: A combination of public cloud elements and other private cloud elements makes up a hybrid cloud. Organizations run their businesses and applications in both private and public clouds, as they can transfer data between the two clouds. This provides flexibility and scalability and maintains control of data and applications [15]. An example of a hybrid cloud is combining Azure with private cloud infrastructure, also integrating an on-premises data center and AWS.
- Community Cloud: This model is used by a group of organizations or communities that have common interests or follow unified industry standards and regulatory requirements [15]. This cloud is a shared cloud structure that provides the general benefits of the cloud in addition to the specific needs of these communities or organizations, for example, financial institutions or healthcare organizations.
- Multi-Cloud: This strategy uses several cloud service providers to serve a specific organization so that the organization benefits from the strengths of multiple service providers to perform different functions and various services [16]. This reduces the problem of restricting vendors, in addition to increasing both flexibility and redundancy. Examples of this model are Using AWS for data analytics, Azure for Windows-based applications, and GCP for machine learning.
- Edge Cloud: To improve application performance and data access speed especially for real-time processing, edge cloud computing is used which deploys cloud resources as close as possible to the network in which data is created, processed, and consumed [17].

Organizations choose the deployment model based on its own requirements and goals.

In the last few years, there has been tremendous growth in finding the optimal configuration of cloud computing that ensures the protection of the data security of business and their clients. Services like integrity, confidentiality, authentication, non-repudiation, and availability are offered for the security of computer networks and information systems. According to NITS, there are five key actors in a cloud computing architecture, as shown in Figure 3.

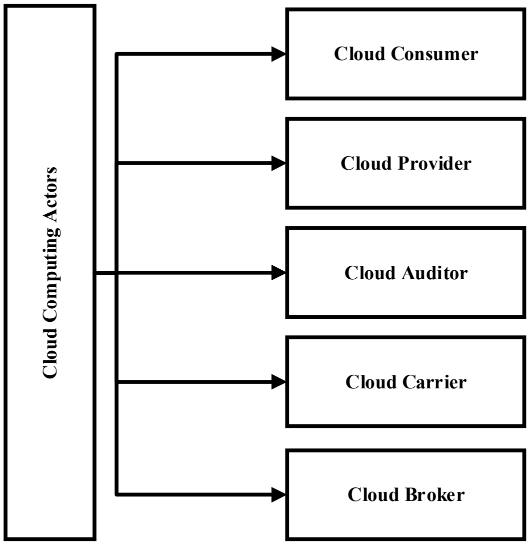

Figure 3: Cloud Computing Actors Framework

These factors are identified as follows:

- Cloud consumer: a person or organization that employs cloud providers' services and keeps a business relationship with them.
- Cloud provider: a person, group, or organization in charge of providing interested parties with a service.
- Cloud auditor: a third party that can conduct an impartial evaluation of the cloud implementation's performance, security, and information system operations.
- Cloud broker: An organization that coordinates the performance, distribution, and use of cloud services as well as the interactions between cloud providers and cloud customers.
- Cloud carrier: a middleman who connects and transfers cloud services between cloud providers and cloud consumers.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. RELATED WORKS

The importance of security in cloud computing cannot be overstated. Due to its many advantages, cloud computing has become a crucial component of contemporary company operations. However, these benefits come with certain security challenges and risks. Here are several studies that work on security challenges and some other surveys that summarize the security challenges. To the best of our knowledge, these are some of the most related states of art in this area of study.

Tabrischi and Rafsanjani reviewed current security frameworks to minimize vulnerabilities and thwart potential assaults. To lower risk and vulnerability and boost confidence in a constantly linked world, they provide several written policies, procedures, and processes that outline the secure management approach in the cloud environment throughout the article. These concerns deal with cloud platform data and service security. the paper classifies security difficulties and conducts a comparative study between security problems and the solutions recommended to address them [18].

Vinoth and Vemula in [19] analyze and assess the biggest threats to cloud systems' network and data security, based on a review of the literature. In addition, this article discusses several cloud usage scenarios and associated security risks in e-commerce and banking.

Sun examines the state of the art in privacy security research as it relates to various cloud computing privacy security protection systems. The author starts by outlining some of the privacy security hazards associated with cloud computing and offering a thorough methodology for protecting privacy. Second, the paper presents and discusses the state of research for several technologies, including multi-tenant, trust, access control, ciphertext policy attribute-based encryption (CP-ABE), key policy attribute-based encryption (KP-ABE), trace mechanism, fine-grain, multi-authority, revocation mechanism, proxy re-encryption (PRE), hierarchical encryption, searchable encryption (SE), and many more. Finally, the proposed paper compares and analyzes the features and range of applications of typical schemes. In addition, the paper addresses open research questions and points out potential future study avenues [20].

The main and most current cloud security risks influencing the development of cloud computing technologies were reviewed in this study [21]. The standard algorithms used for cloud-based authentication and data storage in cloud environments were the focus of this survey. The function of Artificial Neural Networks (ANN) in the cloud environment over the last few years is discussed in this research. Analysis was done on how well the conventional and ANN-based algorithms resisted attacks.
The authors in [22] have examined 3-multi-ranked search strategies in cloud computing and have introduced a novel strategy over obliging but suspicious proxy servers that is the most realistic model to date. Additionally, they specified how to handle various ciphertext sets from each data owner and how to use them to determine the query vector from specified trapdoors. They revamped the GBB-Tree's creation technique to successfully integrate the index trees of several data owners. They showed that, despite requiring more computations than earlier systems, their methodology has a tolerable time cost, which makes the proposed scheme more workable in real-world circumstances.

This paper provides an approach to data protection by employing industry best practices to verify the authenticity and integrity of the data. It covers index builders, Secure Sockets Layer (SSL) encryption, Message Authenticate Codes (MAC), double user authentication (first by the user's owner, then by the cloud), cloud-based digital signature verification, and grouping data into discrete categories. It makes data available by going over solutions for a number of issues, such as data tampering, data leaking, and unauthorized access even from the cloud service provider [23].

4. SECURITY RISKS IN THE CLOUD

The cloud is considered one of the most important technologies in storing, protecting, and processing data, but the cloud is still vulnerable to many security risks that may threaten the stored data. This section summarizes the most common risks to the cloud.

1) ***Data Breaches***.
Which is classified as one of the most serious security problems facing the cloud. Accessing secret data by an unauthorized party can occur due to flaws in cloud configuration or compromised credentials of authorized users [24]. Any unintentional or illegal destruction, loss, alteration, unauthorized disclosure, or access to personal data that is transferred, stored, or processed in any other way can result from a security breach. The global average cost of a data breach in 2023 is $4.45 million, 15%

greater than in 2020, according to the IBM Cost of a Data Breach Report 2023. 51% of businesses want to raise cybersecurity investment this year in response [25].

2) ***Poorly Access Control.***
Poor access control is the failure to manage the access of users who have permissions. These permissions may pose a risk by allowing unauthorized users to access confidential data. Proper procedures for enabling those authorized to enter are of great importance in reducing the severity of expected risks [26].

3) ***Compliance Violations***.
Compliance violation is the failure to comply with cloud regulatory requirements that results in financial and regulatory penalties. Cloud users must adhere to compliance laws and requirements when hosted by the cloud [24].

4) ***Distributed Denial of Service (DDoS) Attacks***.
The cloud is exposed to attacks that cause service disruption to some parties. The seriousness of this issue is based on the sensitivity of the work of the affected organizations. This causes the unavailability of some services for a certain period of time, which is called the denial of service [26].

5) Insider Threat.
Fifth, some employees exploit their knowledge of their organization's weaknesses as called insider threads, they exploit their powers to tamper the cloud data or sell it unethically to competitor organizations [26]. However, some insider attacks happen because of a lack of awareness of some employees or stolen insider's credentials.

6) Lack of Visibility.
The lack of visibility into the infrastructure and lack of knowledge of security configuration makes information security-related incidents difficult to detect, thus increasing the time required to address them [24].

7) Misconfiguration
One more serious security cloud issue is misconfiguration, which refers to security vulnerabilities that arise from improperly configured cloud resources and services. These misconfigurations can cause data breaches, unauthorized access, losing data, and other security incidents. Cloud misconfigurations often occur due to human error or oversight. configurations must be correctly implemented and regularly reviewed [26].

8) ***Third-Party Service Risks***.
Using services or applications from a party outside the cloud requires extreme caution. This may seem positive for saving resources, reducing costs, and facilitating some services, but it may threaten security interests and cause new vulnerabilities that have not been taken into consideration. It is possible that the new external party will implement security controls that are insufficient to deal with the cloud, so choosing a third party is an extremely complex matter and requires study and extreme caution [26].

9) ***Data Encryption***.
Although data encryption has a critical role as a security practice in the cloud, it could also cause certain challenges and risks that organizations need to address. Losing encryption keys, consuming computational resources for encryption and decryption of data, using different encryption mechanisms by the cloud providers, the possibility of key exposure, the high cost required, latency and processing time and many other issues can the data encryption cause [26].

10) Data Fusion.
The data fusion commingling data from different resources, this issue exposes the cloud to security problems, as each source applies a security level that might differ from other sources, this issue threatens the cloud environment and causes non-compliance [27].

11) Government and Legal Risks.
The locations of the data centers of the cloud exist in different regions, each region has its own laws depending on the country it belongs to. This matter may cause conflict or negatively affect data sovereignty or users' privacy [24].

These risks and other related problems must be prevented or mitigated. This responsibility falls on the organizations, which in turn must adopt comprehensive, integrated, and proactive security controls to reduce cloud security problems.
Organized and integrated data protection strategies must also be implemented. The currently available strategies will be discussed in the subsequent section.

5. SECURITY COUNTERMEASURES OF CLOUD

Preserving data and applications in the cloud is extremely important, so the implementation of security measures must be ensured by applying the necessary security strategies. In this section, the most important safeguard security strategies available for the cloud will be discussed.

An essential component of maintaining the security and effectiveness of cloud computing systems is ***Identity and Access Management (IAM)***. IAM is the cornerstone of protecting sensitive data and controlling who can access what resources in the world of cloud computing, where data and applications are stored and remotely accessible. IAM systems enable the establishment and maintenance of user identities, specifying their roles and permissions, and implementing strong authentication and authorization protocols. By lowering the possibility of insider threats, illegal access, and data breaches, this strategy improves security. It also simplifies user provisioning and de-provisioning, guarantees that only authorized users may access cloud resources, and keeps an extensive audit trail for forensic and compliance reasons, all of which contribute to the streamlining of operations [28].

Protecting sensitive data and preserving the integrity and privacy of data stored and transferred across cloud services require the use of ***data encryption***. Encryption works as a shield that protects data against unwanted access and other risks. Encryption is usually implemented by cloud providers in transit, data is being transferred between user devices and cloud servers, and at rest, where the data is saved on the cloud. Most common data encryption techniques used in the cloud [29]:

- Data encryption in Transit:

1) SSL/TLS (Secure Sockets Layer/Transport Layer Security): These encryption protocols protect the security of data transmitted over the Internet, by encrypting the communication line between users and the cloud service to prevent eavesdropping on the transmitted data.

2) IPsec (Internet Protocol Security): IPsec protocols secure communication between devices using the cloud, they use virtual private networks (VPNs) that encrypt data as it travels through the Internet or through untrusted networks.

3) SSH (Secure Shell): This protocol enables devices to communicate with each other, the connection is managed remotely to ensure data is secure when it is transmitted over untrusted networks [29].

- Data Encryption at Rest:

1) Advanced Encryption Standard (AES): It is a widely used symmetric encryption scheme (uses the same key for encryption and decryption processes). AES is a fast and secure technique, making it a great choice for the cloud for encrypting files and other sensitive data.

2) Full Disk Encryption (FDE): This approach encrypts the entire hard disk or Solid-State Drive (SSD). Encrypting the whole drive protected the data stored in the device.

3) File-level Encryption: Some organizations require encryption of some files only; this enables data controlling of files through encryption.

4) Key Management: Some encryption algorithms require an encryption key and a decryption key (Symmetric encryption), other algorithms have one key for both encryption and decryption (Asymmetric). These keys must be kept and managed in a secure way [29].

Many other encryption approaches are used for the security of cloud data, the above mentioned are the most used techniques.

To guarantee the safety of data, apps, and services housed in cloud environments, ***network security*** of the cloud is essential. The traditional network boundary has blurred as more and more businesses go to the cloud, requiring a change in security tactics. Implementing strong defenses against a variety of threats, including distributed denial of service (DDoS) attack, illegal access, and data breaches, is part of cloud network security [30]. The following points explain the most important guarantees for network security of the cloud:

- Firewalls: Applying a firewall plays an important role in filtering and monitoring data traffic according to the organization's previously specified instructions.
- Network Segmentation: Data in the cloud has several levels of importance, so dividing the cloud network into subnetworks or regions can restrict cyberattacks, also this makes it difficult for the attacker to reach the sensitive data.
- Virtual Private Cloud (VPC): Cloud providers offer ways to virtually isolate certain parts of the infrastructure to prevent unauthorized access.

- Intrusion Detection and Prevention Systems (IDS/IPS): IDS and IPS solutions are implemented for detecting and preventing malicious activities within the cloud network. These systems are important in identifying and blocking attacks in real-time.
- Incident Response Plan: develop a procedure to respond to security incidents within a comprehensive security plan. This plan should be tested regularly to make sure it is still efficient [30]. In addition, penetration testing is employed to measure the risk of vulnerabilities in the cloud, this process helps in developing new mitigation procedures. Networks should train the staff to increase their awareness of any cyberattack. Also, cloud providers should have redundant network infrastructure to keep the availability of cloud services.

Regular Auditing and Monitoring plays a critical role in tracking the various activities carried out by users and recording all the work they do. Conduct permanent monitoring of any security incidents and make alerts in case of adoption of suspicious activities [31].

Alternatively, using ***Secure Coding*** techniques is essential for creating software systems that are reliable and robust. They include a collection of methods and ideas meant to stop vulnerabilities and lessen possible dangers all the way through the software development life cycle. These procedures include error management, data encryption, access control, and input validation. Developers can greatly lower the danger of security breaches, including data breaches and unauthorized access, by following secure coding rules. Additionally, they enhance an application's overall credibility and foster a safer online environment for businesses and consumers alike. Secure coding techniques are an essential part of software development in an era where cyber dangers are always changing, guaranteeing that the digital landscape stays as safe as possible [32].

A ***sharing responsibility model*** should be implemented in defending against cyberattacks of the cloud. This model requires a cooperative effort of both the service providers and the cloud customers. Customers have the vital responsibility of protecting their own data and apps in this mutually beneficial relationship, guaranteeing the privacy and accuracy of their digital assets. Meanwhile, it is imperative that the service providers strengthen the underlying infrastructure to make sure it is resistant to outside attacks. Maintaining a balance in sharing of security obligations is crucial, as any disproportion in this mutual commitment may endanger the interests and welfare of users as well as organizations [33]

Within cloud environments, where information and programs are frequently dispersed over multiple locations, the ***Zero Trust Security Model*** offers a strong barrier against potential threats. To make sure that only authorized organizations can access critical resources, it places a strong emphasis on identity and access control, ongoing monitoring, and stringent device and user verification. Organizations may greatly improve their security posture, lower the risk of data breaches, and preserve the confidentiality and integrity of their data even in the face of constantly changing cyber threats by putting this concept into practice in the cloud [20].

On the other hand, the cloud requires securing data from physical threats such as natural disasters, thefts, and data leakage. The latest security measures are used, such as surveillance cameras, imposing tools to control access to data and services, biometric authentication, and other methods that ensure the ***physical security*** of the infrastructure and servers [33].

Moreover, applying the ***vendor security assessment*** evaluates cloud service providers by auditing their security certificates and examining whether the service provider complies with industry standards [33].

In addition, keeping the security strategies up to date and being informed about the security best practices. Continuity of the red team exercises to identify any new security breach that might affect the cloud infrastructure. Moreover, some strategies should be applied for specific organizations, since each organization's security needs may vary based on the role of the cloud services, so security countermeasures should be adapted to some unique requirements. Securing the cloud is constantly changing and requires full knowledge of the new security breaches. Therefore, serious security issues and threats must be monitored and tried to be addressed as quickly as possible.

6. ANALYSIS AND DISCUSSION

To address challenges associated with cloud issues, a multifaceted approach is essential. First, it is imperative to regularly update and modify the cloud infrastructure in response to security vulnerabilities arising from cloud-related issues.

Second, there is a need to innovate and establish new security protocols for data and resources within the cloud, with the objective of enhancing the quality of the existing techniques by integrating multiple security methods.

Third, fast response to incidents is crucial, and there should be a massive focus on conducting ongoing vulnerability assessments to effectively control them, thereby preventing hackers from exploiting any weaknesses.

Fourth, keep track of the regulations pertaining to compliance in your area and industry. Although cloud providers frequently offer information and

Table 1: The Responsibilities of Service Providers and Customers in Applying The Security Strategies of The Cloud

Security Strategy	Public Cloud	Private Cloud
Share responsibility model.	The cloud service provider and customers share responsibility, the service provider's role is securing the infrastructure while securing data and applications is the responsibility of the customers.	Organizations control the cloud infrastructure and are responsible for securing data and applications, but these responsibilities vary depending on the cloud deployment model.
Identity and access management (IAM)	IAM services are offered by cloud providers, these services control the user access and determine their permissions. cloud users are responsible for configuring IAM rules that manage accessing cloud resources	IAM is still important, however, organizations control most of the operations regarding user access since it is the responsibility of organizations to manage the cloud infrastructure.
Data Encryption	Data encryption services are provided by public cloud providers, while enabling and configuring the encryption settings are done by customers.	Managing encryption keys, making sure data is fully protected, and implementing encryption mechanisms are the responsibility of the organizations.
Network Security	Configuration of firewalls, virtual private networks (VPNs), and security groups are done by customers to protect their cloud resources.	In a private cloud, network security is controlled by organizations that should manage and configure the network security measures such as firewalls and IDSs.
Compliance and regulations	It is the responsibility of customers to comply with industry regulations and compliance-related services provided by public cloud service providers.	The responsibility for ensuring compliance in the private cloud lies on organizations, and this is a difficult matter due to the multiple responsibilities required from organizations.
Security Monitoring and Logging	Public cloud providers provide monitoring and logging services, while customers must set up and manage the tracking tools and security issues.	Implementation of the monitoring and logging strategies are the responsibility of organizations since these strategies are specially designed for the organization's specific requirements.
Third-Party Security Solutions	To improve security, customers can utilize a variety of third-party security strategies from the cloud marketplace.	organizations may have to select and integrate third-party security products to handle certain security demands.
Scalability and Elasticity	The flexibility and scalability of public cloud environments enable the dynamic modification of resources to satisfy security requirements.	Depending on the architecture and resource provisioning, the scalability and elasticity of a private cloud may be more constrained.

tools to aid in compliance, it is ultimately the user's obligation to guarantee compliance.

Fifth, human mistakes frequently play a role in security incidents and awareness training is essential. Education and updating the team members on the most recent security risks and recommended procedures is crucial.

Sixth, solutions for cloud security issues can be developed using artificial intelligence, for instance training a machine that can detect security vulnerabilities and breaches.

Finally, Intensive efforts and cooperation are required between users and service providers in a way that ensures the successful application of security mechanisms. Table 1 illustrates the responsibilities of institutions, service providers, and customers in implementing information security protection strategies for both public and private clouds. The table illustrates that in the public cloud, the responsibility is generally on the cloud service provider and the customer to implement and control the security technique, while the responsibility of implementing and monitoring the security mechanism in the private cloud is the organization's role [34].

In accordance with the three different types of cloud services; software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), the shared responsibility model explains the security obligations of cloud providers and clients.

Table 2 illustrates the vendor and user responsibilities in the SaaS, PaaS, and IaaS services. As shown in row one, SaaS application security is the responsibility of the vendor, while endpoints and network security is the user's role. Row two shows the PaaS service, where the platform security is the responsibility of the vendor, and the user must secure the applications developed on the platform. Finally, row three illustrates that the vendor should be responsible for the infrastructure components in the IaaS service while the user should take care of each application installed in the infrastructure [35].

In contrast, when it comes to Software as a Service (SaaS), users are in charge of managing endpoints, users, network security, potential misconfigurations, and data-related problems. Vendors, on the other hand, are mainly in charge of application security. Platform as a Service (PaaS) vendors manage hardware and software components of platform security; customers manage endpoints, users, workloads, and network security in addition to securing applications built on the platform. When it comes to Infrastructure as a Service (IaaS), users are responsible for protecting installed applications on the infrastructure, which includes endpoints, users, network security, workloads, and data. Infrastructure component security is managed by providers. The requirement of precise boundaries and cooperation between providers and users to preserve strong security postures in cloud settings is highlighted by this shared responsibility paradigm.

Table 2: Shared Responsibility by Cloud Service Type

Service Type	Vendor Responsibility	User Responsibility
SaaS	Application security	Endpoints, user, and network security. Misconfigurations, workloads, and data.
PaaS	Platform security, including all hardware and software	Security of applications developed on the platform. Endpoints, user and network security, and workloads
IaaS	Security of all infrastructure components	Security of any application installed on the infrastructure (e.g., OS, applications, middleware). Endpoints, user and network security, workloads, and data.

Figure 1 shows the four primary components of a cloud security system: risk assessment and security.

countermeasures, monitoring and auditing, and awareness training. To identify the assets, we want to safeguard the primary vulnerabilities that could compromise those assets, the risk assessment stage begins with the identification of assets, vulnerabilities, and threats. Second, assess each risk's possible impact and likelihood before prioritizing it according to its likelihood and severity. Lastly, documentation of the results and recommendations is necessary.

The next stage is security countermeasures, based on the risks identified, choose appropriate security procedures or controls, then develop a plan to implement the chosen countermeasures. In the testing countermeasure sub-stage, the identified countermeasures are validated to effectively mitigate or reduce the identified risks. Several countermeasures cloud be applied.

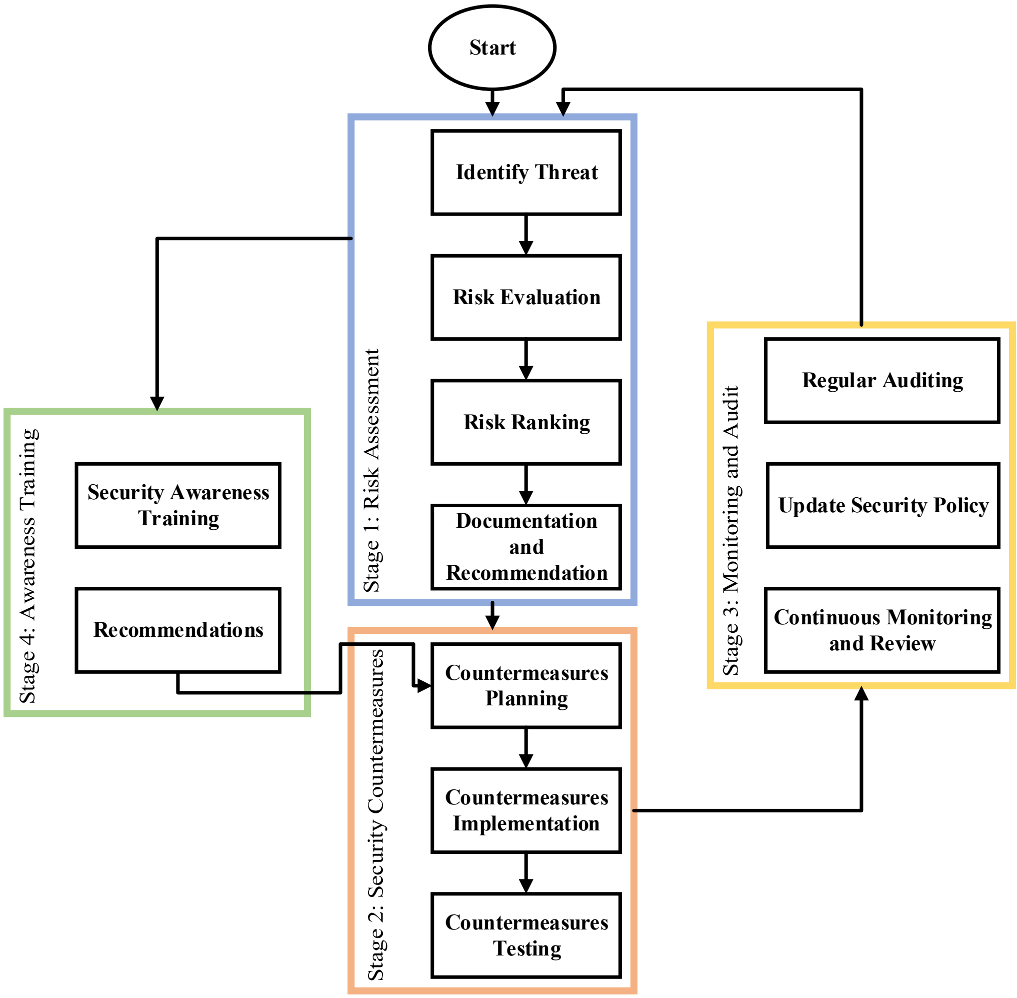
Start
Stage 1: Risk Assessment
Identify Threat
Risk Evaluation
Risk Ranking
Documentation and Recommendation
Stage 2: Security Countermeasures
Countermeasures Planning
Countermeasures Implementation
Countermeasures Testing
Stage 3: Monitoring and Audit
Regular Auditing
Update Security Policy
Continuous Monitoring and Review
Stage 4: Awareness Training
Security Awareness Training
Recommendations

Figure 4: Flowchart of The Primary Components of a Cloud Security System.

Stage three is security monitoring and auditing, monitoring the security posture for identifying new risks continuously and updating some security policies if required. If there is a new risk, we go back to identify the threat in stage one.

Each time a new thread is detected, security awareness training is proposed, which could result in a proposition of new or updated countermeasures or other recommendations in stage four.

A comparative summary of the study and recent pertinent work in the subject of cloud security is given in Table 3. It draws attention to important elements such the research's novelty and relevance, the technique used, the findings' consistency and reliability, the research's effect and contribution, and the results' generalizability and contextualization. The table provides insights into the study's strengths and weaknesses as well as its alignment with accepted knowledge and practices in cloud security by contrasting the research findings with existing literature. This comparative study helps to provide a nuanced view of the research's contributions and consequences by placing it within the larger framework of cloud security scholarship.

7. OPEN RESEARCH ISSUES

In the following we presents some of the open research issues in the field of cloud security:

- Empirical Validation: There is a lack of empirical support for many suggested security remedies and cloud security best practices. Conducting empirical studies and case studies to evaluate the efficacy of these metrics in actual cloud settings should be the focus of future study.
- Comprehensive Scope: The present plethora of research on cloud security may be narrowly

Table 3: A Comparison of Research Findings with Current Relevant Work

Aspect	Research Findings	Current Relevant Work
Relevance and Novelty	Addresses gaps in cloud security Offers new insights and approaches	Builds upon existing literature. Expands on established knowledge
Methodology	Employs robust research methodologies. Incorporates rigorous data analysis	Utilizes various research approaches. Applies statistical techniques
Consistency and Replicability	Findings are consistent with literature	Aligns with existing research findings
Impact and Contribution	Offers practical implications for practitioners. Contributes to policy recommendations	Advances theoretical understanding. Proposes technological advancements
Generalizability and Contextualization	Applicable across different contexts	Relevant to specific settings

focused, missing significant facets or new developments. Research on a wider range of subjects, such as emerging risks, weaknesses, and security remedies in cloud computing, is necessary.

- Theoretical Framework: Although helpful suggestions for practice are important, there aren't many compelling theoretical frameworks that steer cloud security research. Future research should aim to create and employ theoretical frameworks that offer a greater comprehension of the fundamental ideas and dynamics of cloud security.

- Integration of newly emerging Technologies: There are advantages and disadvantages to cloud security frameworks integrating emerging technologies like edge computing, blockchain, and artificial intelligence. How these technologies might be combined to improve threat detection, data security, and access control in cloud systems requires more investigation.

- Regulatory Compliance Challenges such as Cloud security regulations are subject to a complicated and dynamic regulatory environment. To ensure adherence to pertinent regulations while utilizing cloud services, research should concentrate on addressing regulatory compliance difficulties in multi-cloud systems.

- Privacy and Data Protection: Research on creative methods for protecting sensitive data in the cloud is needed, as worries about privacy and data protection grow. This covers privacy-preserving technology designed for cloud environments, data anonymization strategies, and encryption approaches.

- Threat intelligence and information sharing: To effectively counteract changing cyberthreats, stakeholders must collaborate and share information. In the cloud security sector, future research should concentrate on creating frameworks and platforms for sharing threat intelligence and cooperating.

By studying these open research questions, we can enhance our knowledge of the difficulties associated with cloud security and provide more reliable and efficient security solutions for cloud computing systems.

8. CONCLUSION

Protecting the cloud from cyber threats is a crucial concern that requires constant planning, especially with the increase of businesses using cloud storage. The frequency and evolving nature of cyber-attacks need ongoing updates and adjustments to security policies that add a higher level of security. This study outlines the key security challenges in our current landscape, presents the challenging solutions to mitigate these issues, and analyzes the roles of service providers, organizations, and cloud users in protecting the cloud from security issues. Moreover, this paper illustrates the main path guidelines to increase the security of the cloud. In the future, novel data security strategies will be the focus of efforts to address the outstanding issues for which there are currently no optimal solutions. Through the validation of current procedures, strategy refinement, compliance mechanism fine-tuning, and shared responsibility model optimization, the work gradually contributes. Enhancing the entire security posture of cloud-based systems and furthering the field of cloud security benefit from both aspects.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Eman Al-Qtiemat and Zeyad Al-Odat conducted the research and analyzed the data; Eman Al-Qtiemat wrote the paper; Zeyad Al-Odat provided the graphs and table according to the template ...; all authors had approved the final version.

REFERENCES

[1] L. Alhenaki, A. Alwatban, B. Alahmri, and N. Alarifi, “Security in cloud computing: a survey,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 17, no. 4, 2019.

[2] J. Hassan *et al.*, “The rise of cloud computing: data protection, privacy, and open research challenges—a systematic literature review (SLR),” *Comput. Intell. Neurosci.*, vol. 2022, 2022.

[3] S. S. Vellela, R. Balamanigandan, S. P. Praveen, and others, “Strategic Survey on Security and Privacy Methods of Cloud Computing Environment,” *J. Next Gener. Technol.*, vol. 2, no. 1, 2022.

[4] L. Golightly, V. Chang, Q. A. Xu, X. Gao, and B. S. C. Liu, “Adoption of cloud computing as innovation in the organization,” *Int. J. Eng. Bus. Manag.*, vol. 14, p. 18479790221093990, 2022.

[5] S. Basu, “68 Cloud Security Statistics to Be Aware of in 2023.” 2022.

[6] C. Jones, “50 Cloud Security Stats You Should Know In 2023.” 2023.

[7] M. Saratchandra and A. Shrestha, “The role of cloud computing in knowledge management for small and medium enterprises: a systematic literature review,” *J. Knowl. Manag.*, vol. 26, no. 10, pp. 2668–2698, 2022.

[8] D. H. Stipp, “Most common cloud security incidents worldwide in 2020 and 2022.” 2023.

[9] D. P. F. Möller, “NIST Cybersecurity Framework and MITRE Cybersecurity Criteria,” in *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*, Springer, 2023, pp. 231–271.

[10] U. Saritac, X. Liu, and R. Wang, “Assessment of Cybersecurity Framework in Critical Infrastructures,” in *2022 IEEE Delhi Section Conference (DELCON)*, 2022, pp. 1–4.

[11] Z. Al-Odat and S. Khan, “An Efficient Cloud Auditing Scheme for Data Integrity and Identity-Privacy of Multiple Uploaders,” in *2019 IEEE Cloud Summit*, 2019, pp. 8–13.

[12] Z. A. Al-Odat and S. U. Khan, “Anonymous privacy-preserving scheme for big data over the cloud,” in *2019 IEEE International Conference on Big Data (Big Data)*, 2019, pp. 5711–5717.

[13] F. Nadeem, “Evaluating and ranking cloud IaaS, PaaS and SaaS models based on functional and non-functional key performance indicators,” *IEEE Access*, vol. 10, pp. 63245–63257, 2022.

[14] V. Liagkou, G. Fragiadakis, E. Filiopoulou, V. Kyriakidou, C. Michalakelis, and M. Nikolaidou, “Comparing the Cost of IaaS and CaaS Services,” *Int. J. Technol. Diffus.*, vol. 13, no. 1, pp. 1–11, 2022.

[15] M. Ravend and K. Upadhyay, “Reasearch in Cloud Computing Security,” *www.irjmets.com @International Res. J. Mod. Eng.*, vol. 395, no. 01, pp. 395–401, 2023, [Online]. Available: www.irjmets.com.

[16] S. Achar, “Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape,” *Int. J. Comput. Syst. Eng.*, vol. 16, no. 9, pp. 379–384, 2022.

[17] J. Yao *et al.*, “Edge-cloud polarization and collaboration: A comprehensive survey for ai,” *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 7, pp. 6866–6886, 2022.

[18] H. Tabrizchi and M. Kuchaki Rafsanjani, “A survey on security challenges in cloud computing: issues, threats, and solutions,” *J. Supercomput.*, vol. 76, no. 12, pp. 9493–9532, 2020.

[19] S. Vinoth, H. L. Vemula, B. Haralayya, P. Mamgain, M. F. Hasan, and M. Naved, “Application of cloud computing in banking and e-commerce and related security threats,” *Mater. Today Proc.*, vol. 51, pp. 2172–2175, 2022.

[20] P. Sun, “Security and privacy protection in cloud computing: Discussions and challenges,” *J. Netw. Comput. Appl.*, vol. 160, p. 102642, 2020.

[21] S. A. Sheik and A. P. Muniyandi, “Secure authentication schemes in cloud computing with glimpse of artificial neural networks: A review,” *Cyber Secur. Appl.*, vol. 1, p. 100002, 2023.

[22] Y. Kim, J. Son, R. M. Parizi, G. Srivastava, and H. Oh, “3-multi ranked encryption with enhanced security in cloud computing,” *Digit. Commun. Networks*, vol. 9, no. 2, pp. 313–326, 2023.

[23] K. I. Jones and R. Suchithra, “Information Security: A Coordinated Strategy to Guarantee

Data Security in Cloud Computing," *Int. J. Data Informatics Intell. Comput.*, vol. 2, no. 1, pp. 11–31, 2023.

[24] R. A. Khan, S. U. Khan, H. U. Khan, and M. Ilyas, "Systematic literature review on security risks and its practices in secure software development," *ieee Access*, vol. 10, pp. 5456–5481, 2022.

[25] BITSIGHT, "What's the cost of a data breach?" 2023.

[26] T. Hidayat and R. Mahardiko, "A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing," *Int. J. Artif. Intell. Res.*, vol. 4, no. 1, pp. 49–57, 2020.

[27] R. Krishnamurthi, A. Kumar, D. Gopinathan, A. Nayyar, and B. Qureshi, "An overview of IoT sensor data processing, fusion, and analysis techniques," *Sensors*, vol. 20, no. 21, p. 6076, 2020.

[28] A. Alsirhani, M. Ezz, and A. M. Mostafa, "Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing.," *Comput. Syst. Sci. \& Eng.*, vol. 43, no. 3, 2022.

[29] D. Ulybyshev, "Data Protection in Transit and at Rest with Leakage Detection," Purdue University, 2019.

[30] M. Ozer, S. Varlioglu, B. Gonen, V. Adewopo, N. Elsayed, and S. Zengin, "Cloud incident response: Challenges and opportunities," in *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2020, pp. 49–54.

[31] T. P. Hedley and O. Ben-Chorin, "Auditing and monitoring activities help uncover fraud and assess control effectiveness," *CPA J.*, vol. 81, no. 6, p. 68, 2011.

[32] C. Anglano, R. Gaeta, and M. Grangetto, "Securing coding-based cloud storage against pollution attacks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 5, pp. 1457–1469, 2016.

[33] K. W. Bennett and J. Robertson, "Security in the Cloud: understanding your responsibility," in *Cyber Sensing 2019*, 2019, vol. 11011, p. 1101106.

[34] H. Akbar, M. Zubair, and M. S. Malik, "The Security Issues and challenges in Cloud Computing," *Int. J. Electron. Crime Investig.*, vol. 7, no. 1, pp. 13–32, 2023.

[35] A. Sunyaev and A. Sunyaev, "Cloud computing," *Internet Comput. Princ. Distrib. Syst. Emerg. Internet-Based Technol.*, pp. 195–236, 2020.