PROJECT

ADAVANCED TATICS CLOUD COMPUTING IN SECURITY

Techonology stack : AI FOR CYBERSECURITY WITH IBM QRADAR

Project Title : ADVANCED TATICS IN CLOUD COMPUTING SECURITY

Team Leader : BAMMIDI ANKITHA

Team no : LTVIP2024TMIDI13822

Team members : 5

1. Bammidi Ankitha
2. Bammidi Akshitha
3. Uppala Dakshayani
4. Mammidi Vanaja
5. Rayavarapu Girija

COLLEGE : SRI BALAJI DEGREE COLLEGE

INDEX

What is cloud computing?

PDFRSS

Cloud computing is the on-demand delivery of compute power, database, storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing. Whether you are running applications that share photos to millions of mobile users or you're supporting the critical operations of your business, a cloud services platform provides rapid access to flexible and low-cost IT resources. With cloud computing, you don't need to make large upfront investments in hardware and spend a lot of time on the heavy lifting of managing that hardware. Instead, you can provision exactly the right type and size of computing resources you need to power your newest bright idea or operate your IT department.

Cloud computing provides a simple way to access servers, storage, databases and a broad set of application services over the internet. A cloud services platform such as Amazon Web Services owns and maintains the network-connected hardware required for these application services, while you provision and use what you need via a web application.

Introduction

Cloud Computing is a technological innovation that provides a centralized reservoir of resources for configurable and outsourced computing services. This approach delivers computing services comparable to common utility services like water and electricity. The transition to cloud computing has numerous advantages, including faster development times, reduced production costs, and increased dependability.[Citation1] Customers in search of reliable and high-performing computer services now have access to alternatives that are more cost-effective than ever in the form of cloud services, which include web services, e-mail services, and instant messaging services.[Citation2]

In the study conducted by Khan et al.[Citation3] it is mentioned that according to the 2022 State of the Cloud Report, 94% of those polled are currently employing Cloud Computing, with 91% using public cloud and 72% using private cloud. Cloud Computing's appealing qualities may clarify this extensive popularity. Users

can select from four deployment modes, private, community, public, or hybrid, along with various standards like software as a service and infrastructure as service, enabling them to tailor their cloud computing solutions to meet specific needs and requirements.[Citation4] Moreover, Cloud Computing offers network-accessible services with virtually limitless computing resources, available on-demand without requiring technical expertise or maintenance

Greater resource flexibility and efficiency is a significant advantage of cloud computing. The ability to run many virtual machines (VMs) on a physical server is crucial to cloud computing, achieved through virtualization. The fact that VMs may be easily transferred between different hosts only adds to the advantages of virtualization. This offers numerous benefits, including hardware utilization, remote access, resource protection, and isolation: Virtualization, along with other cloud-related technologies, presents security challenges. With the emergence of new risks and hazards within the infrastructure of these technologies, the issue of cloud security remains a concern. According to Szalay et al.,[Citation7] in 2021, 76% and 79% of respondents identified security as a challenge. Others argue that research should concentrate on different activities such as encryption, authentication, data integration, and access issues, whereas some cloud computing consumers prioritize data protection and privacy.[Citation8–11] As mentioned in the given statement, these are considered to be the crucial areas of study,[Citation5,Citation6] researchers continue to pursue a comprehensive approach to classifying and organizing cloud security.

Traditional approaches to information security risk assessment are relied on to assess the potential dangers posed by cloud computing environments. This involves identifying key evaluation indicators, assigning values to these indicators, and employing various methodologies to calculate the final risk rating. In their research, Tariq[Citation12] described the assessment process involved several vital components, including establishing a risk assessment index system, introducing a multi-level fuzzy comprehensive assessment model, and constructing a cloud computing-based information security risk assessment model specifically for power grids, utilizing gray correlation analysis. However, Nonetheless, it is essential to consider the unique attributes of cloud-based systems during these procedures.[Citation13]

In their work Li et al.[Citation13] illustrated the execution of information security risk assessment from both the client's and server's perspectives by integrating the three tiers of cloud computing architecture. During the assessment process, this technique considers the cloud system's design; however, it does not consider how the system risks interact with the factual application circumstances. This implies that risks originating in one part of the system might propagate to other system components.

A security scenario quantification approach was suggested in another research that was mentioned by Tian.[Citation14] This method was based on the likelihood of threat propagation. Graph theory was used for the modeling process in this approach, which targeted the intricate network structure present in the Energy Internet. Nevertheless, this approach only considers scenarios in which risks or threats propagate along a specific channel. The current situation does not align with the fact that risks within a single system component can pose a threat to the overall network resources to varying extents. Moreover, it is crucial to evaluate the permission links between system resources thoroughly. This examination is vital as it impacts the extent to which risk can be transmitted from one resource to another.[Citation13]

Hosting in the cloud has become an essential strategic orientation for companies such as Amazon, Microsoft, and Google.[Citation15] It offers numerous advantages to businesses of all sizes, such as expansion flexibility and minimal effort. Services such as storage and computational power capacity expansion, business owners and top management find 24/7 support, high service availability, adherence to security standards, and effective business continuity strategies are appealing. However, cloud hosting has disadvantages, such as losing control over infrastructure and data. Regulators in the local financial sector are aware of the need for standardization to encourage the widespread use of technology enablers like cloud hosting and computing. Nevertheless, certain governments continue to restrict the transfer of data from local infrastructure to cloud hosting due to apprehensions about security and privacy.[Citation15] A strong security model is essential to ensure secure cloud hosting, is capable of adapting to the environment, involving the right resources, and effectively managing risks. Multiple security models are available, including ISO27005, NIST SP 800–30, CRAMM, CORAS, OCTAVE Allegro, and COBIT 5. The information must be protected, whether hosted in the cloud or locally. Cloud hosting with an appropriate security technique that satisfies all requirements and challenges for maintaining the information's security ensures that the information system is always safeguarded.[Citation15]

As more businesses use cloud computing, there will be an even more significant need for practical information security management in these environments. The increase in cloud computing has substantially raised the possibility that exposed data would be compromised because of the increasing complexity of information security risks and attacks. Iqbal et al.[Citation16] Padmaja and Seshadri[Citation17] conducted research that recorded real-time threats in specific sectors such as healthcare, retail, and banking applications in the cloud and assaults on cloud service providers. These investigations highlight the ever-changing and dynamic nature of cybersecurity concerns in cloud systems. These occurrences emphasize the urgent need for a proactive information security management system, as detailed in this paper, to efficiently reduce such developing threats and safeguard sensitive data in cloud computing. Therefore, implementing a developed and proactive information security management system is models, and involved.

ABSTRACT

Cloud computing faces more security threats, requiring better security measures. This paper examines the various classification and categorization schemes for cloud computing security issues, including the widely known CIA trinity (confidentiality, integrity, and availability), by considering critical aspects of the cloud, such as service models, deployment models, and involved parties. A comprehensive comparison of cloud security classifications constructs an exhaustive taxonomy. ISO27005, NIST SP 800–30, CRAMM, CORAS, OCTAVE Allegro, and COBIT 5 are rigorously compared based on their applicability, adaptability, and suitability within a cloud-based hosting methodology. The findings of this research recommend OCTAVE Allegro as the preferred cloud hosting paradigm. With many security models available in management studies, it is imperative to identify those suitable for the rapidly expanding and dynamically evolving cloud environment. This study underscores the significant methods for securing data on cloud-hosting platforms, thereby contributing to establishing a robust cloud security taxonomy and hosting methodology.

KEYWORDS:

- Cloud computing
- risk assessment method
- cloud security taxonomy
- security model methodologies

Information security threat and attack landscape

The aim of managing information security in cloud computing is to safeguard the infrastructure, data, and applications.[Citation47] Cloud computing security is enforced through a variety of measures, including controls, policies, technologies, and approaches that adhere to security management regulations. The result is increased data privacy, integrity, and availability. The domain of data protection covers a heterogeneous array of solutions aimed at minimizing a spectrum of threats. The hazards discussed include several categories of sensitive information, such as trade secrets, e-mail scams, medical data, and corporate papers, all of which are vulnerable to potential compromise. In cloud computing, these security measures are utilized for safeguarding data, promoting regulatory compliance, upholding customer privacy, and establishing authentication procedures for users and devices.[Citation47]

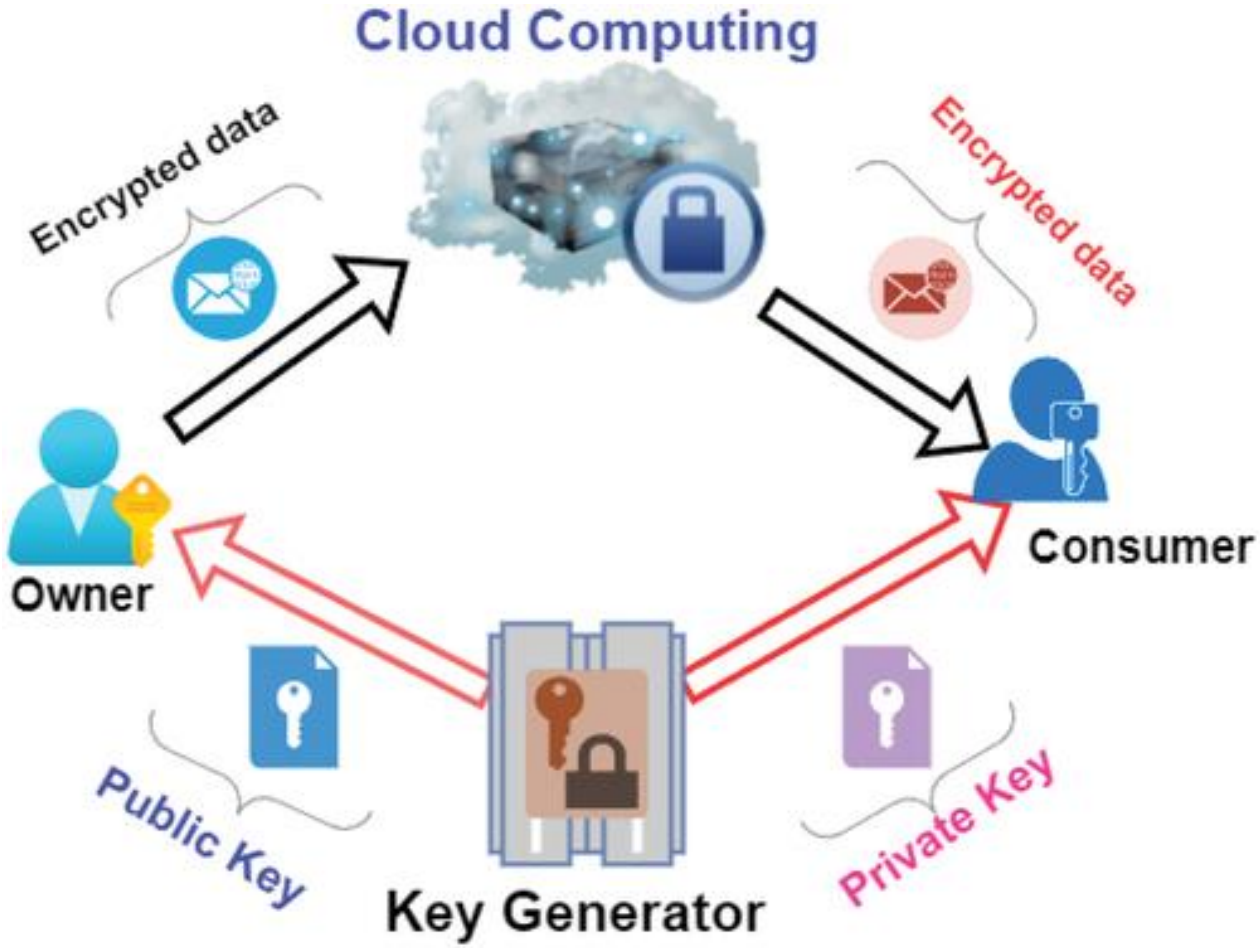
Furthermore, the implementation of cloud protection measures must be shared among both service providers and data owners. The incorporation of a fundamental secure layer in cloud computing is derived from the practices of most cloud service providers.[Citation48] Additionally, this study forecasts a substantial surge in the

worldwide market for public cloud services by the end of 2021, signifying a swift adoption of such services.The security team and IT experts encounter difficulties when it comes to developing effective methods to safeguard sensitive information and dealing with problems related to cloud computing that hinder the secure transfer of data and applications. The main concern revolves around the potential vulnerability of sensitive data and intellectual property, which can be initially targeted either through unintentional information leaks or advanced cyber attacks. The domain of cloud computing presents significant security obstacles, specifically concerning the process of choosing secure keys using resilient algorithms. Ensuring secure and uninterrupted access to cloud storage is a crucial responsibility for developers. The verification of large amounts of data can be achieved using an algebraic signature-based approach, as demonstrated in the previously cited source.[Citation49] As previously demonstrated by Chen[Citation49] in their study, the method eliminates the requirement for the original data. In addition, cloud providers offer auditing services to enhance data integrity. The service, as mentioned above, needs to demonstrate more measures of security methodology concerning the three fundamental indicators of security performance, specifically Availability, Confidentiality, and Integrity (CIA).[Citation50]

Thereby recommended that Cloud Service Providers (CSPs) establish a public service for Third-Party (TPA) auditing to enhance their auditing practises. Implementing this solution would facilitate the provision of analytical services to verify data integrity in cloud-based systems.[Citation51]

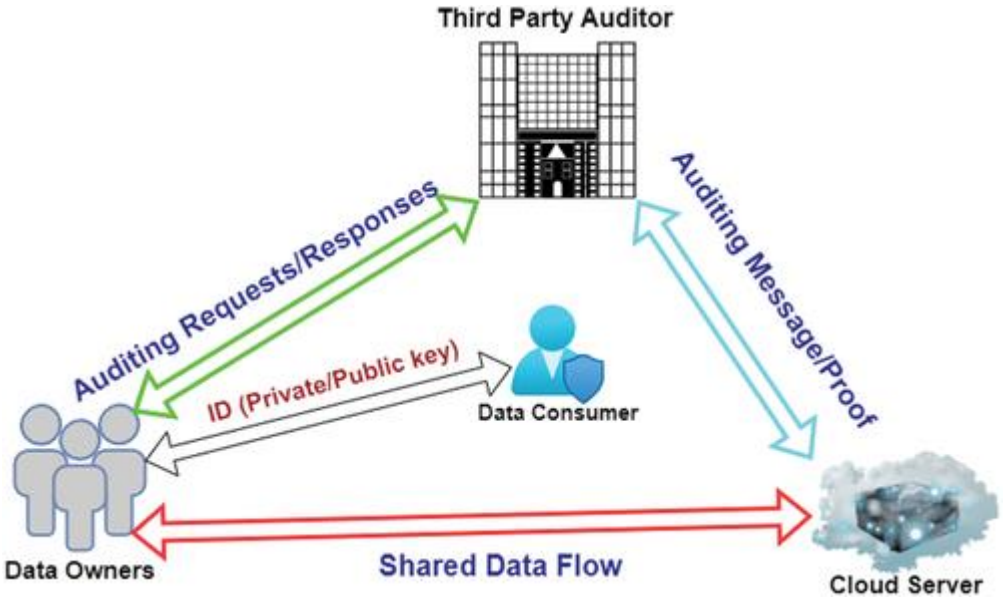
There exist three distinct categories of users who participate in the domain of cloud computing, namely: users, hackers, and cloud managers. The potential risk to data integrity poses a significant concern in the relationship between users and cloud service providers. This is due to the possibility of unauthorized access by hackers who may remotely replace or delete data, which can have significant consequences for the original users. This issue has been documented in previous research.[Citation52] Figure 1 depicts the verification process utilizing cryptographic techniques. There exist numerous techniques to safeguard data from interception during communication or local data exchange. Algorithms serve as the initial line of defense in safeguarding personal data against potential security breaches. Algorithms, such as symmetric and asymmetric cryptographic techniques, including popular ones like RSA, DES, or AES, and their hybrids, are utilized in cloud computing, exemplified by Verma et al.[Citation53]

Figure 1. Cryptography techniques in cloud computing.



Yu et al.[Citation54] suggested approach utilizing Remote Data Integrity Checking (RDIC) is presented, which facilitates the verification of cloud storage by a designated verifier. The predominant portion of a currently existing Research, Development, Innovation, and Commercialisation project is centered on utilizing the RSA algorithm and critical Public Key Infrastructure. (PKI) The abovementioned approach is denoted in Figure 2.

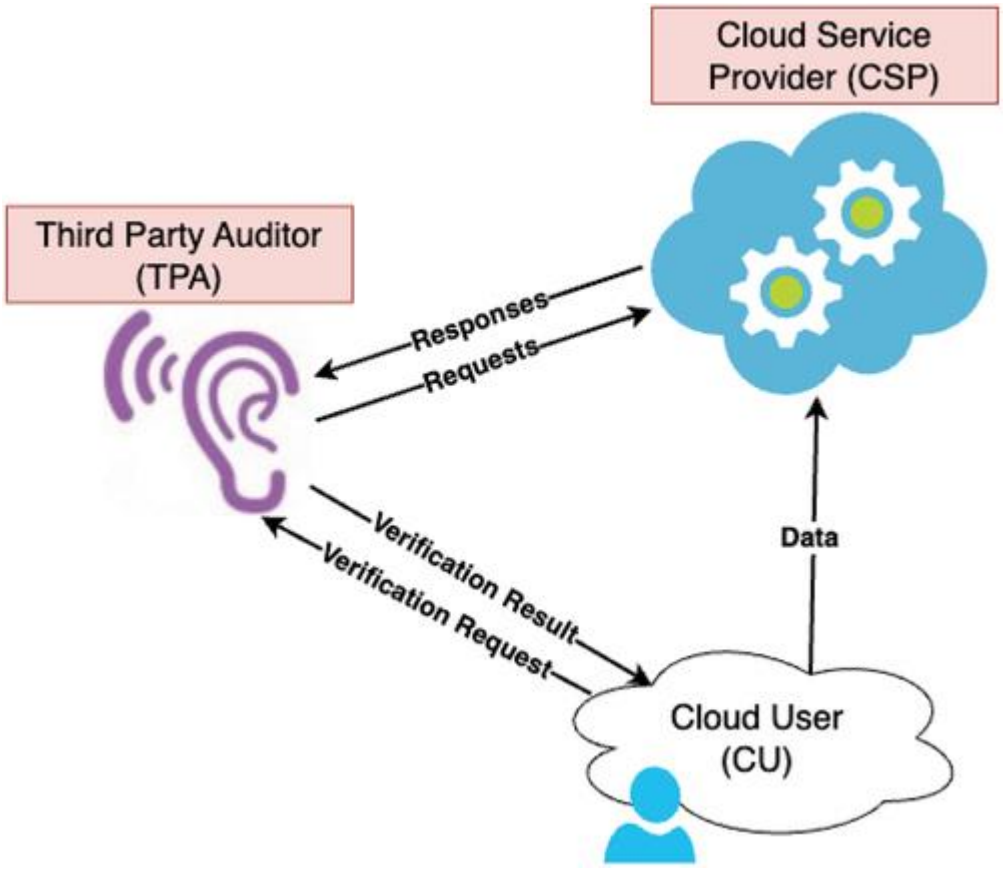
Figure 2. Remote data integrity checking (RDIC).



In a Cloud Computing Environment (CCE), the implementation of public auditing ensures data integrity by leveraging the involvement of a Trusted Third Party Auditor(TPA). This approach addresses the challenge of verifying data accuracy, which can be arduous and costly for cloud users. Nevertheless, this process may violate data confidentiality, one of the three factors of information security management that must be controlled.[Citation55] In certain instances, users may be compelled to disclose personal information that they consider unnecessary, resulting in a breach of confidentiality. The cloud service provider provides strategies for safeguarding a user's sensitive data, as per.[Citation55] The solution presented in the study by More and Chaudhari,[Citation56] as depicted in this diagram demonstrates the participation of three main entities: the data owner, TPA, and

cloud server. This passage describes the responsibilities of the owner, which include dividing the file into separate blocks, encrypting each block, and generating a signature value for the encrypted blocks. Subsequently, the Trusted TPA receives encrypted blocks and signatures from both the cloud server and the user. The TPA applies signatures to available blocks and provides the resulting output. As depicted in Figure 3, this procedure ensures the preservation of confidentiality and integrity.

Figure 3. Third party auditor (TPA) signatures.



In contemporary times, many enterprise organizations have transitioned to cloud-based services, enabling them to offer a pay-as-you-go model.[Citation57] The foremost concern that necessitates attention pertains to the accessibility of resources susceptible to various attacks, including Denial of Services (DoS), worms, malware, and brute force attacks.[Citation46,Citation58] Kurosawa and Ohtaki[Citation59] proposed a solution that enhances data privacy and availability by utilizing algorithms that enable users to detect fraudulent servers, particularly during the execution of data manipulation operations such as updates, deletions, and additions.

Threats and attacks

The dispersed geographical locations of data centers operated by cloud service providers present security challenges and risks, resulting in cloud computing customers needing to be made aware of the specific whereabouts of their confidential data. The increasing proliferation of threats in virtualized environments diminishes the effectiveness of conventional security measures such as firewalls, host-based antivirus software, and intrusion detection systems in providing adequate protection for virtualized systems.[Citation27,Citation60,Citation61]

Data integrity

The absence of confidence in cloud computing is a significant obstacle attributed to data privacy concerns and the frequency of security threats and attacks. Ensuring data integrity monitoring is highly important to prevent any potential data tampering or data corruption within cloud service providers. Data consistency and reliability maintenance are facilitated by data integrity, which also contributes to the preservation of data authenticity.[Citation47,Citation58] Maintaining data integrity is an essential concept that ensures any modifications to the data are executed with the user's awareness and permission.In the event of an intrusion or unauthorized access, the security of protected information may be impaired, potentially resulting in a breach of confidentiality. Various methods that can be employed to compromise user data encompass data alteration, tag forging, and data leakage attacks. Various measures are employed to prevent data integrity attacks in cloud environments. An example of a security measure is cooperative provable data possession, which combines hash indexing hierarchy with homomorphic verifiable responses.[Citation47,Citation58]

Data trust

The primary concern pertains to trust, which is prone to deterioration if two key issues are not adequately resolved: a dearth of lucidity and an infringement upon security and confidentiality. The notion of trust is multifaceted and contingent upon the conduct or demeanor of another individual.[Citation47,Citation58] The flexibility provided by cloud service providers is a key factor that attracts customers to their services; however, this may also expose their sensitive data to potential security risks. Consumers' need for more awareness regarding the technologies employed and the data control process can be attributed to their dependence on contracts and the trust mechanism. According to Al-Hashimi et al.[Citation62] adhering to legal security standards requires meeting several fundamental security criteria, including but not limited to authentication, integrity, transparency, confidentiality, availability, and audits.

Multi-tenancy

Figure 4 depicts various additional challenges in cloud computing that are specifically associated with cloud security. Creating a secure multi-tenant environment requires taking into account several factors, including access policies, application deployment, and data access and protection, as suggested by sources.[Citation63–65] Poor and unrecorded implementation of access control and change management protocols may subject an organization to risks from both internal and external sources, in addition to negative publicity and legal repercussions.[Citation25]

Figure 4. Cloud computing threats and attacks.

Risk management and audits

Evaluating potential risks is a crucial aspect of effectively managing cloud computing resources. The emergence of cloud computing has posed a new challenge in information security management, with significant implications for cloud security. Enhancing the Risk Assessment (RA) for security methodologies is imperative to achieve improvement. In contemporary times, specific concerns have been brought to the forefront within both academic and industrial spheres.[Citation66] Nevertheless, effective risk management frameworks must address the dynamic nature of changes. According to Petraşcu,[Citation67] Risk management can be defined as identifying and assessing potential uncertainties that may result in adverse outcomes for an organization.[Citation66]

Furthermore, there exists a risk that may harm the feasibility of cloud services.[Citation68] Hence, risk management refers to the actions undertaken to guide and oversee individuals and organizations.[Citation69] Information security risk management serves various objectives, among which the three primary purposes can be identified.

Cloud computing offers significant advantages for individuals and organizations but also presents a substantial number of risks and vulnerabilities. According to the author Singh et al.,[Citation70] security policies are typically categorized into five distinct groups. Table 1 displays the prominent policies that are utilized.

When adopting cloud hosting, which offers more significant risks and threats, Irsheid et al.[Citation15] emphasize the need for a reliable Security Model to handle hazards and maximize environmental security effectively. In order to guarantee that the chosen frameworks are current and in line with the changing cloud security environment, steps are taken to evaluate safe proofs created by cryptographic evaluators and give confidence levels to them before picking a distributed framework.[Citation71] Furthermore, architects may get knowledge related to crucial factors for choosing security frameworks from internet platforms such as GitHub, which can assist them in making well-informed judgments.[Citation72] The evaluation of hybrid methodologies and individual algorithms is also conducted to ascertain the optimal outcomes concerning fulfilling user specifications.[Citation73] These procedures provide confidentiality, privacy, and protection in cloud systems while accommodating the evolving security needs and metrics offered by new frameworks in the cloud environment.[Citation74] In addition, the paper underlines the significance of using an appropriate security model in an environment that is rapidly expanding and constantly changing, such as the cloud, to safeguard information successfully. The research evaluates and contrasts six security models of risk assessment methodologies: ISO27005, NIST SP 800–30, CRAMM, CORAS, OCTAVE Allegro, and COBIT 5. The evaluation of the models is based on their suitability, flexibility, and engagement in an approach to cloud-based

hosting. Based on these evaluations, OCTAVE Allegro is recommended as the standard for cloud hosting, with COBIT 5 and CORAS serving as viable options with some tuning.[Citation15]

The research conducted by Ismail and Islam[Citation75] offers useful insights into the integration of effective security processes and procedures that go beyond just implementing frameworks. The authors highlight the need of a cohesive framework for cloud security transparency and audit, which beyond the mere deployment of fundamental security principles. They contend that while frameworks are necessary, they are insufficient in isolation to guarantee strong security in cloud computing. The paper explores the intricacies of cloud security and emphasizes the need of openness and audit methods that may provide a full perspective on security policies. The authors emphasize the need of surpassing frameworks and prioritizing comprehensive methods that include transparency and audit functions to improve security procedures in cloud computing settings.

Establishing rules and procedures is crucial to ensure the CIA of information throughout the entire process of inputting, transmitting, and storing it.[Citation76] Companies that host their information systems in any environment are now legally required to have sufficient security strategies and practices to ensure that the CIA Triad can continue to function as intended.[Citation76] Although an on-premise setup may give businesses increased control over their information technology infrastructure, Additionally, it is important to have secure backups and clear visibility into all system components, it does come with its own unique set of challenges, such as the high cost of maintaining information availability and the responsibility for managing the infrastructure falling directly on the shoulders of the IT staff.[Citation77] In addition, upgrading hardware and software, expanding the capacity of servers, and setting up a data center may all provide substantial obstacles to the company and affect the organization’s income, reputation, and credibility.[Citation78]

Examining the cloud security categories is essential for dealing with the possibility of prejudice or subjectivity in the evaluation procedure. Narang[Citation72] emphasizes the recognition and examination of common cloud security concerns, which is crucial for comprehending the scope of possible prejudices or subjectivity in security evaluations. In addition, Ismail and Islam[Citation75] provide a consolidated framework for enhancing transparency and auditability in cloud security. This framework facilitates the standardization of the evaluation process and reduces the influence of subjective interpretations. Furthermore, Jamshidi et al.[Citation79] highlight the significance of doing quality evaluation in systematic literature reviews, specifically in addressing the potential bias in the results. This is important because it emphasizes the need for thorough review techniques to prevent possible biases in cloud security classifications. The technique used to assess and evaluate cloud security categories is a crucial factor in guaranteeing the dependability and accuracy of the results to guarantee the reliability of the

comparison. Using suitable assessment metrics and considering contextual aspects in this situation is crucial. The research offers valuable insights into the dynamic security metric framework, which tackles crucial elements that affect the overall security of a system from several perspectives.[Citation80] This paradigm is especially pertinent since it highlights the need to consider contextual elements that might substantially impact cloud security classifications. The paper thoroughly overviews the assessment metrics used in systems security by examining the current metrics and their strengths and weaknesses. It is essential to guarantee that the approach used to compare cloud security categories is thorough.

ISO27005

Kure et al.[Citation81] comply with the requirements of the ISO 27,005 standard Figure 5 and Table 3, and businesses are required to set up a technical security team to formulate an all-encompassing security strategy. The standard offers a methodical and organized approach to the management of risks, outlining a series of activities that companies and other organizations should carry out.[Citation81]

Figure 5. ISO27005 risk management process.

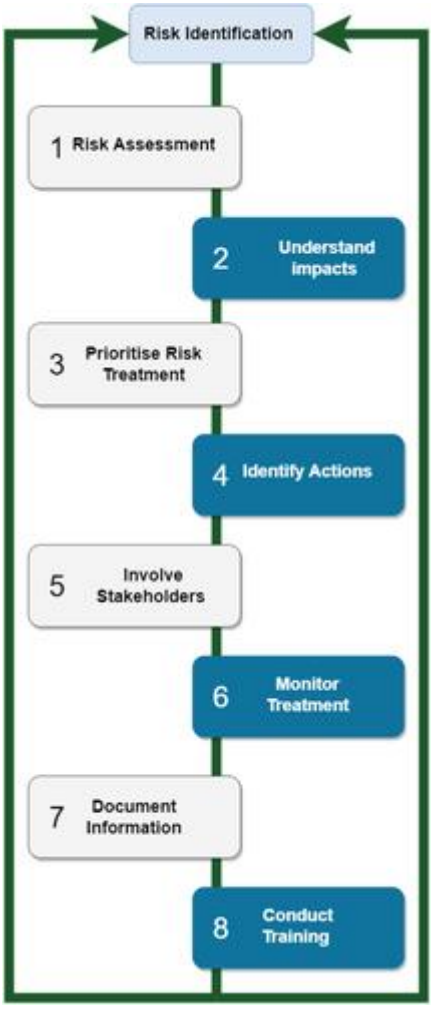


Table 3. ISO27005 risk management process.

The technique that is utilized in ISO 27,005 entails identifying the organization's assets, the risks that those assets are up against, any weaknesses or vulnerabilities, the controls that are already in place, the chance of an event happening, and the repercussions that will arise from it.[Citation82]

NIST SP 800–30

The NIST SP 800–30 methodology Figure 6 and Table 4 is one of the risk management methodologies used most often nowadays. It assists businesses in improving their capacity to thwart, identify, and react to cyber-attacks. This strategy is often used to reduce risk exposure. The process of risk management using NIST SP 800–30 encompasses several sequential steps.[Citation83]

Figure 6. NIST SP 800–30 risk management process.

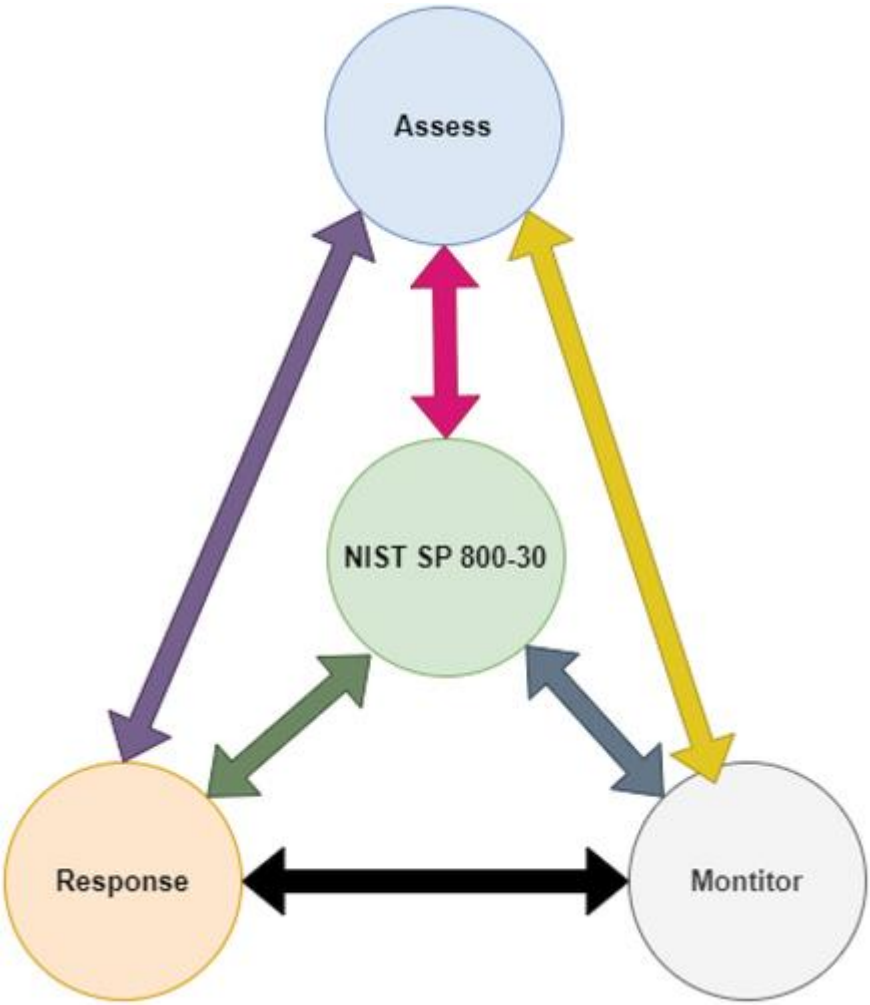


Table 4. Steps for developing NIST SP 800–30 risk management plan.

OCTAVE

The United States Department of Defense (DOD) designed the model known as OCTAVE Figure 7 and Table 5. Its purpose is to facilitate the alignment of an organization's goals and objectives with its information security strategies. The approach emphasizes the protection of an organization's information assets by focusing on identifying possible threats and vulnerabilities that might put the safety of the systems at risk.[Citation84] The OCTAVE model may be broken down into four distinct phases, each contributing to the overall execution of the process.[Citation85,Citation86]

Figure 7. OCTAVE model stages and steps.

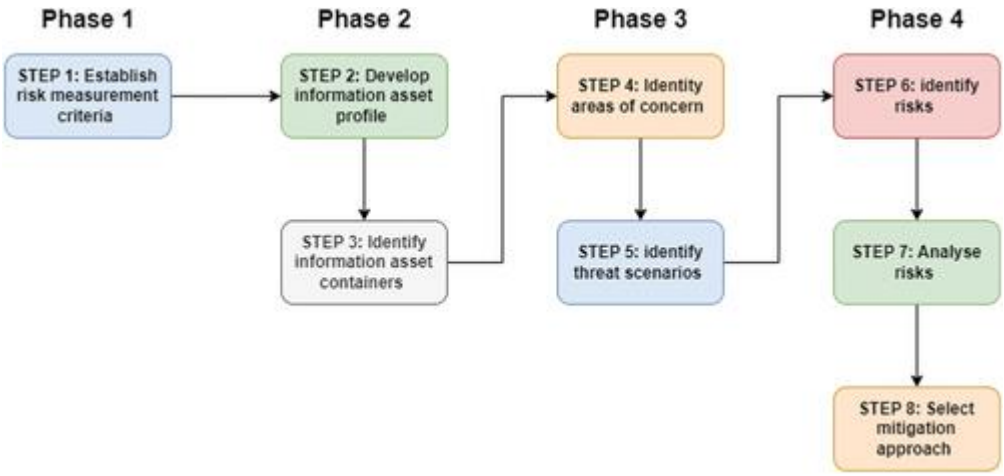


Table 5. OCTAVE model stages and steps.

OCTAVE recommendation

The recommendation of OCTAVE Allegro as the preferred cloud hosting model effectively tackles the risk of oversimplifying or generalizing results by prioritizing the identification of crucial assets and hazards.[Citation87] OCTAVE Allegro utilizes systematic risk assessment techniques, avoiding general assumptions and ensuring a detailed comprehension of the organization's own risk environment. The methodology eliminates the simplicity of security assessments and discourages the generalization of results by prioritizing a customized, risk-based approach. This guarantees that the security suggestions given are tailored to the organization's unique circumstances, reducing the dangers linked to a generic approach and fostering a more efficient and focused security stance in the cloud hosting environment.[Citation87]

CRAMM

The CRAMM methodology Figure 8 and Table 6 The CRAMM methodology, which stands for Central Communication and Telecommunication Agency's Risk Analysis and Management Methodology, is a strategy developed by the British Government's CCTA (Central Communication and Telecommunication Agency) for analyzing and managing risks.[Citation88] The methodology consists of three distinct stages.

Figure 8. CRAMM model stages and steps.

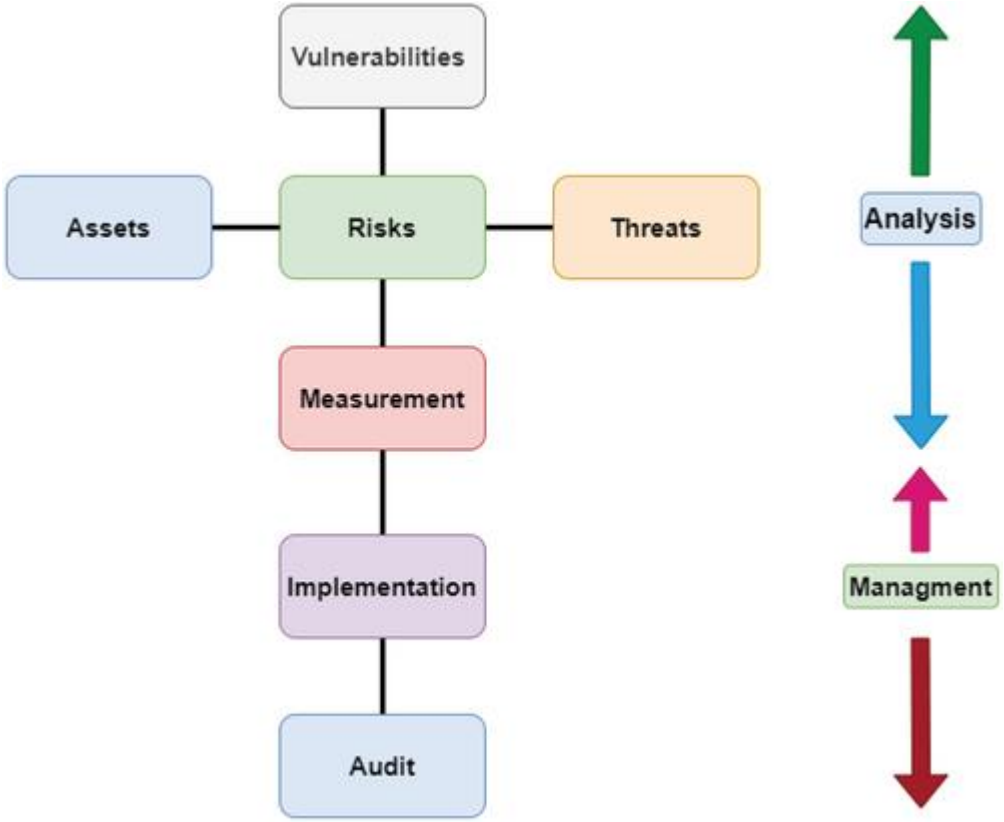


Table 6. Phases of the CRAMM methodology.

CORAS

Between 2001 and 2003, the European Commission was responsible for developing and funding the CORAS methodology, which provides a practical framework for evaluating security risks. It is an eight-step process that is based on a model as shown in the Figure 9 with detail in Table 7, and it is used for doing security analysis.[Citation89] To describe the CORAS method using the Unified Modeling Language (UML), a graphical language is utilized that employs diagrams to illustrate the interactions and relationships between users and their operating environment. Because CORAS models threats to software and

distributed systems, so it is well-suited for deployment in cloud-based environments.[Citation90]

Figure 9. CORAS model stages and steps.

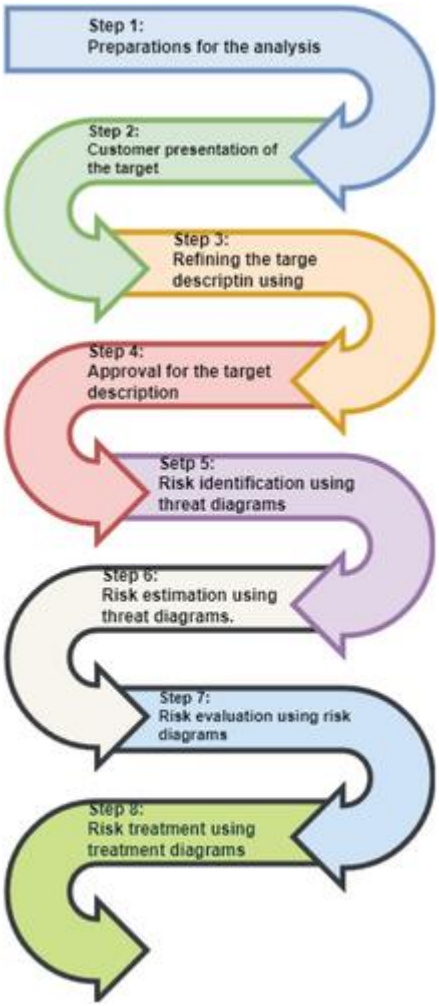


Table 7. CORAS model stages and steps.

COBIT 5

COBIT 5 is a framework of control association developed in 2012 by the Information Systems Audit as shown in Figure 10. Its purpose is to help organizations manage and analyze risks connected to their cloud-based information assets and the consequences these risks have on the organization. COBIT 5 was first introduced in 2012. It relies on a foundation of five fundamental principles as shown in the Table 8 and is supported by seven enablers for effective IT management.[Citation91]

Figure 10. COBIT 5 model stages and steps.

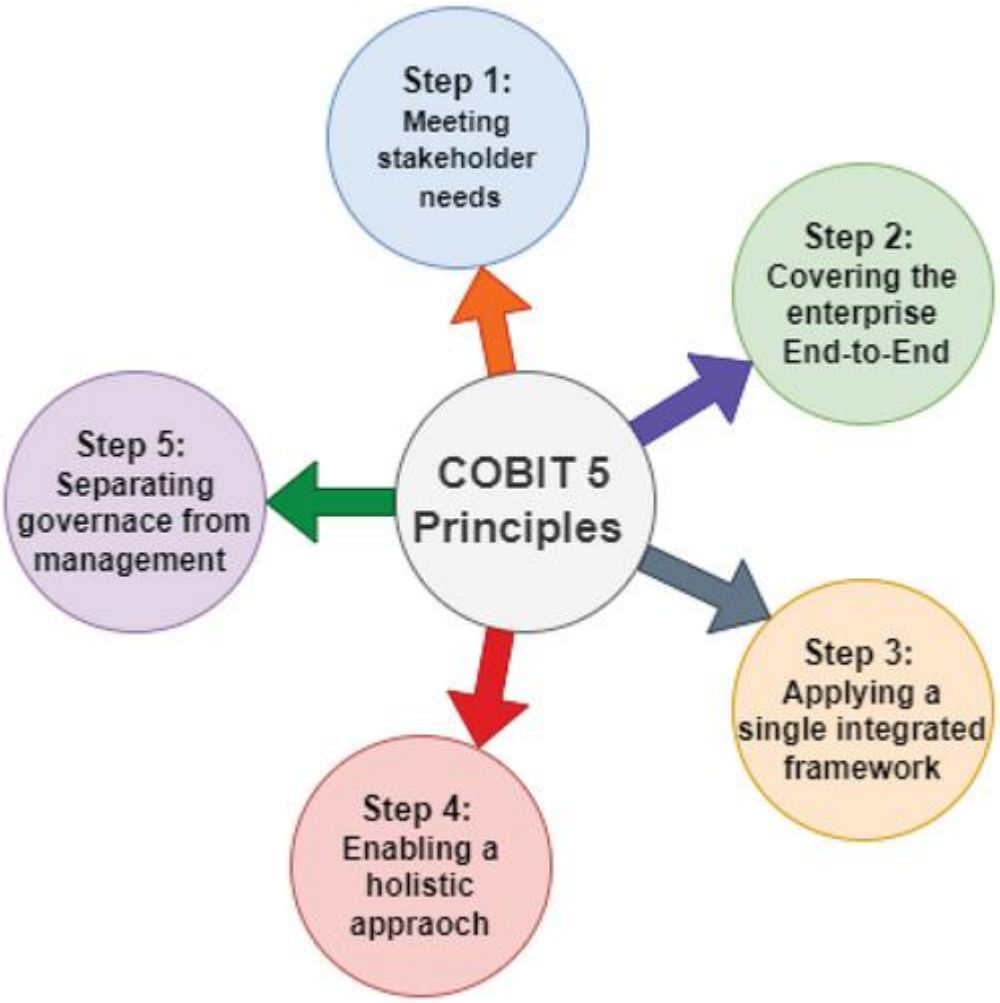


Table 8. COBIT 5 rules.

The suitability of different security models, developed and deployed across different domains, relies on the understanding of the organization's business objectives and risk management framework. After assessing the levels of risk that are deemed acceptable, organizations can pick the risk management strategies that are most suited to achieving their goals, or they may tailor a strategy by selecting components from a variety of frameworks. Both the NIST and ISO security models have a systematic approach. However, the NIST security model includes particular restrictions that might make adapting existing procedures to new cloud infrastructure configurations more difficult. On the other hand, the OCTAVE model emphasizes organizational risks and practises and comes equipped with an automated application to facilitate implementation. In terms of applicability, flexibility, and participation, each model has benefits and limitations; thus, when selecting a model, it is essential to consider the particular requirements of cloud-hosted systems.

Mastering Cloud Security: Protecting Your Company's Digital Assets

In this edition of **TechTrends Translated: Boardroom Edition**, we delve into the vital topic of **Cloud Security**. As we increasingly migrate our businesses to the cloud, understanding how to protect our digital assets becomes paramount. This article aims to demystify cloud security challenges and strategies, ensuring you can confidently navigate the cloud's vast potential while safeguarding your data and applications. I believe this insight will not only enhance your conversations around technology but also equip you with the knowledge to make informed decisions that fortify your company's digital defenses.

Remember, in each **TechTrends Translated: Boardroom Edition** article, we navigate emerging tech with ease and expertise. The goal is to give business leaders like you easy-to-understand insights designed to elevate your boardroom discussions and business decisions.

Understanding Cloud Security Fundamentally

Cloud Security refers to the collection of policies, controls, procedures, and technologies that work together to protect cloud-based systems, data, and infrastructure. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. Essentially, it's a significant aspect of any cloud service that ensures data integrity, confidentiality, and availability.

Think of Cloud Security as the Security System for your Digital Home

Just as you'd secure your physical business premises with locks, alarms, and surveillance, cloud security protects your digital presence in the cloud. It ensures that only authorized users can access your valuable information, much like a key system controls access to your company's building.

Real-World Applications and Examples

To illustrate the practicality of cloud security, let's explore how businesses use it:

- **Data Encryption**: A retail company stores customer payment information in the cloud. By encrypting this data, the company ensures that even if unauthorized access occurs, the information remains unintelligible and secure.
- **Identity and Access Management (IAM)**: A financial institution uses IAM to control who can access its cloud-based data and applications, ensuring that only authorized employees can access sensitive financial records.

- **Security Monitoring and Threat Detection**: E-commerce platforms continuously monitor their cloud environments for unusual activity, quickly identifying and mitigating potential threats to protect customer data and maintain trust.

Pros and Cons of Cloud Security

Pros:

- **Enhanced Security Measures**: Cloud providers invest heavily in security technologies, offering levels of security often beyond what individual companies can achieve on their own. For instance, automatic security updates ensure that defenses stay robust against emerging threats.
- **Scalability**: Cloud security solutions can easily scale up or down based on your business needs, providing flexibility as your business grows or faces seasonal peaks.

Cons:

- **Shared Responsibility Model**: While cloud providers ensure the security of the cloud, security in the cloud is the responsibility of the business. This dual responsibility can lead to gaps in coverage if not properly managed.

Complexity in Control: Migrating to cloud services can sometimes result in a feeling of lost control over certain security aspects, especially for businesses used to on-premises IT environments. Understanding Cloud Security Fundamentally

Cloud Security refers to the collection of policies, controls, procedures, and technologies that work together to protect cloud-based systems, data, and infrastructure. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. Essentially, it's a significant aspect of any cloud service that ensures data integrity, confidentiality, and availability.

Think of Cloud Security as the Security System for your Digital Home

Just as you'd secure your physical business premises with locks, alarms, and surveillance, cloud security protects your digital presence in the cloud. It ensures that only authorized users can access your valuable information, much like a key system controls access to your company's building.

Real-World Applications and Examples

To illustrate the practicality of cloud security, let's explore how businesses use it:

- **Data Encryption**: A retail company stores customer payment information in the cloud. By encrypting this data, the company ensures that even if unauthorized access occurs, the information remains unintelligible and secure.

Cloud Security Testing

1. Improper Identity and Access Management

Improper Identity and Access Management in Cloud is the practice of failing to consider the security of access to cloud resources when making cloud service choices. Poor access management can lead to various security issues, including data loss and theft, security breaches, and the loss of business-critical data and information.

Poor access management is the lack of oversight on the modifications made to an account, including changes made by system administrators.

For example: If a user is granted access to a resource and then leaves the company or is terminated, that access should be removed immediately.

3 Different Approaches to perform Cloud Security Testing

Cloud security testing is performed in three different approaches:

- **Black Box**: No external information about the cloud infrastructure
- **Gray Box**: Limited information about the cloud infrastructure
- **White Box**: Complete information about the cloud infrastructure

The White Box approach may sound the most secure, but this is not always the case. It's the opposite. This is because the White Box testing approach has the advantage of letting admins and security personnel know more about the cloud environment. This means they will know more about the cloud infrastructure and the cloud environment, which does not give hacker-style thinking to the security tester.

In contrast, the Black Box approach is the opposite of this. This approach doesn't let information about the cloud environment be known to anyone. This means that the security team has to compromise their cloud security thinking like a Hacker.

The Gray Box approach is almost like the White Box approach. The only difference is that it tends to be a combination of Black and White Box approaches. This means that some information about the cloud environment is known, but not everything. With this approach, you can have the best of both worlds.

Cloud Security Testing 101

1. Improper Identity and Access Management

Improper Identity and Access Management in Cloud is the practice of failing to consider the security of access to cloud resources when making cloud service choices. Poor access management can lead to various security issues, including data loss and theft, security breaches, and the loss of business-critical data and information.

Poor access management is the lack of oversight on the modifications made to an account, including changes made by system administrators.

For example: If a user is granted access to a resource and then leaves the company or is terminated, that access should be removed immediately.

2. Misconfigured Storage Buckets

Data stored in the cloud storage buckets might be vulnerable. If you have misconfigured your storage bucket, the data stored in it could be accessible via a simple search query. There are many cloud providers out there, but each one comes with its own terms of service.

One such term is that most providers allow you to have a publicly accessible bucket. Your bucket can be accessed by anyone with an internet connection and a simple search query. The result is that you or your company may have some very sensitive data exposed and available to anyone who is curious enough to find it.

3. Missing Multi-Factor Authentication

Almost every enterprise-level cloud deployment these days relies on multi-factor authentication (MFA) to ensure that only authorized users can access their cloud resources. MFA is a great way to ensure that even if your cloud infrastructure is compromised, your most sensitive data will be protected.

However, not all organizations are implementing multi-factor authentication correctly. It’s important to know that MFA isn’t a simple one-size-fits-all solution. This can make the process of implementing MFA complicated and open the door for security misconfigurations.

Do Cloud Services Providers allow cloud security testing?

The cloud services providers, such as Amazon Web Services, Google Cloud Platform, and Microsoft Azure, allow their customers to perform testing, but with some limitations. Above all, these services have their own cloud security providers their security teams that perform testing using various methods.

Keeping our data safe in the cloud is a big concern for companies, no matter their size. Protecting sensitive data, ensuring compliance, and safeguarding against malicious threats have become imperative tasks, especially in cloud environments where the traditional boundaries of networks are blurred.

But there's more to worry about with cloud security testing services. Cloud security testing isn't just an additional layer of defense; it's a strategic imperative that ensures your organization's cloud infrastructure remains resilient against an ever-expanding array of cyber threats.

AWS – Amazon Web Services

AWS allows testing on the following resources only:

- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateways
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments

GCP – Google Cloud Platform

According to Google:

If you plan to evaluate the security of your Cloud Platform infrastructure with penetration testing, you are not required to contact us. You will have to abide by the Cloud Platform Acceptable Use Policy and Terms of Service and ensure that your tests only affect your projects (and not other customers' applications

Challenges in Cloud Security Testing

With most businesses going for the cloud, it has become the need of the hour to test the cloud infrastructure for security. Cloud security testing is necessary to ensure data security, and there is a need to test cloud-based applications continuously.

Cloud security testing is a big challenge for security professionals. Cloud security testing is difficult as it involves various aspects of cloud infrastructure. It is a big challenge as the cloud is used for various purposes, and it is a complex infrastructure. Below mentioned are a few pointers to understand why security testing in a cloud environment is complex.

1. Lack of Information

The biggest challenge for cloud security testing is the lack of information about the cloud provider infrastructure and cloud access. Cloud providers

may not be willing to share the information with the customer. Such information might include security policies, physical locations of the data center, and much more. Without this information, it is difficult for the cloud security testing team to map the cloud provider infrastructure and determine the scope of the security testing.

2. Resource sharing

Resource sharing is a common feature of cloud services and is essential for multi-tenant architecture. However, this commonality can also prove to be a limitation during Cloud security testing. Cloud security testing is a highly challenging task, especially with the rise of IaaS cloud services.

3. Policy restrictions

The policy restrictions of the cloud service provider may limit the scope of security testing. The cloud security testing team may not conduct security testing activities on all the cloud infrastructure components or may not be able to audit the network access controls in place. The different cloud approaches may expose the business to security risks depending on the cloud service providers' approaches and the overall security of the cloud.

Astra's Cloud Security Testing Solution

Astra's Cloud Security Testing Solution is a comprehensive cloud compliance validation program designed to ensure your cloud platform is secure. With the constantly evolving threats, you need to have a complete cloud security solution that can cover all your cloud security needs. We help you meet today's rigorous cloud compliance standards, protect your data in the cloud, and reduce cloud security risk with a one-stop solution.

Astra understands that your data is the most valuable and sensitive asset you have. It's why we design our security testing solutions to proactively protect your cloud environment against threats of all kinds, including insider threats while giving you the flexibility to know what's happening in your environment at all times.

Astra's Holistic Approach to cloud security testing is designed to help you build and maintain a secure cloud environment throughout the entire lifecycle of your cloud workloads. We help you understand your vulnerabilities, risk exposure, and attack surface and then help you remediate those vulnerabilities and reduce your attack surface. This way, you can be confident about your cloud security posture and be ready when a breach happens.

Shield Your Cloud: Essential Practices for Cloud Application Security Testing.

Ready for Free Trial

Cloud computing has become the cornerstone of modern business operations. Organizations across industries are embracing the cloud's agility, scalability, and cost-effectiveness to power their digital transformations.

However, this reliance on cloud-based infrastructure also introduces new security challenges that demand proactive measures to safeguard sensitive data and applications.

Table of Contents

Cyber Threats

Cyber threats are constantly evolving, and cloud environments are prime targets for malicious actors. The dynamic nature of the cloud, with its shared resources and complex configurations, presents a larger attack surface for attackers to exploit.

Data breaches, unauthorized access, and application vulnerabilities are just a few of the threats that can jeopardize cloud security.

Cloud Application Security Testing

Cloud application security testing is a crucial component of a comprehensive cloud security strategy. This process involves identifying and eliminating security vulnerabilities in cloud-based applications before they can be exploited.

By implementing a robust cloud application security testing program, organizations can significantly enhance their cloud security posture and protect their valuable data and applications.

Here are some essential practices for cloud application security testing:

Prioritize Security Throughout the Development Lifecycle:

Integrate security testing into every stage of the development lifecycle, from design to deployment. This approach helps catch vulnerabilities early and reduces the cost of remediation later on.

Implement Automated Security Testing:

Leverage automated tools to perform regular scans and identify potential vulnerabilities. Automated testing can significantly improve efficiency and provide continuous visibility into the security posture of cloud applications.

Focus on Sensitive Data Protection:

Implement robust data protection measures, including encryption at rest and in transit, to safeguard sensitive information from unauthorized access.

Enforce Strict Access Controls:

Implement granular access controls to restrict access to cloud resources and applications to authorized users only. This principle of least privilege ensures that only the right people have access to the right data.

Continuous Monitoring and Threat Intelligence:

Continuously monitor cloud environments for suspicious activity and utilize threat intelligence feeds to stay informed about emerging threats. This proactive approach enables organizations to detect and respond to threats promptly.

According to recent statistics, cloud security incidents are on the rise. A 2023 report by IBM Security found that data breaches in cloud environments increased by 10% in the past year. This underscores the importance of implementing effective cloud application security testing practices.

Industry experts emphasize the need for a comprehensive cloud application security approach that encompasses technology, processes, and people.

They advocate for a shift from reactive to proactive security measures, emphasizing the importance of integrating security into the development lifecycle and continuously testing and monitoring cloud environments.

Cloud application security testing is an ongoing process that requires continuous vigilance and adaptation. By embracing best practices, organizations can shield their cloud infrastructure from evolving threats and protect their valuable data and applications.

businesses, cloud application security is a top priority.

Cloud Application Security and Why Is it Important?

Cloud application security refers to the governance and security controls put in place to protect data across the entire cloud environment.
The evolution of the digital landscape has increased the relevancy of cloud application security. Businesses are rapidly migrating huge stores of their data into cloud infrastructure, increasing the potential of security vulnerabilities ripe for exploitation. Undoubtedly, cyberattacks can levy a major financial and reputational blow to an organization.
Following are the 10 most common — and important — security risks organizations with cloud applications face.

1. Misconfiguration

A leading security risks facing cloud applications and systems, misconfiguration often occurs when users inadvertently enable outbound access to cloud networks, allowing applications and servers that shouldn’t be privileged to have access to data and assets. Attackers can easily exploit those vulnerabilities by stealing the credentials of less secure touchpoints.

2. Insecure data sharing

Storing critical data in either on-prem servers or cloud storage repositories or applications encourages employees to exchange greater volumes of data at a much higher frequency. Without a secure way to handle data-sharing between employees, these exchanges can create cloud vulnerabilities resulting in compromised assets.

3. Account hijacking

Hackers have increased their abilities as technology evolved, turning cloud apps into potential attack vectors. Account hijacking occurs when hackers steal account credentials and use them to gain access to critical systems.

4. Ill-equipped staff

For many companies, tech development, IT system diversification and evolving security threats outpace their ability to manage their security needs. Many enterprises lack the budget to hire qualified personnel or the resources to train on new skills. Lacking these personnel can expose the organization to risk.

5. Insufficient access controls

Insufficient access and identity controls are especially risky when companies hybridize their data infrastructure. Without an adequate governance policy to restrict access to data, sensitive information can be exposed.

6. Compliance risk

There are numerous data compliance frameworks businesses must adhere to, including HIPAA, PCI-DSS, and GDPR. Failing to comply could land companies in serious compliance risk — which is extremely costly. Businesses should ensure they have proper authentication systems in place to keep all data compliant. Additionally, they must have reference documentation frameworks that outline steps to achieve compliance.

7. Data loss

Companies lacking the proper data management controls and protocols can unintentionally cause data loss. That can happen when data is accidentally deleted or irreversibly changed, or encryption keys are altered, rendering fully intact data inaccessible. Data loss can lead to serious problems for enterprises, so routine data backups are critical.

8. Employee negligence

A leading security threat facing cloud applications results from negligent employee behavior. In particular, this is true for account hijacking, as hackers take advantage of employees unintentionally giving away critical personal information.

9. Outdated firewall

As threat actors learn to more effectively exploit increasingly sophisticated systems and applications, security architecture needs to be constantly updated. An

adequate network and cloud firewall should identify security vulnerabilities, giving companies information to patch and prevent future exposure.

10. Unsecure APIs

Customers, partners, and even internal team members interact with cloud apps enabled via APIs, making these a significant attack vector. Any risk management strategy should include API protection and API gateway security.

Cloud Application Security Risk Can Affect Businesses

Data and asset compromise can have a serious financial impact on businesses, with long-lasting and even permanent consequences. Beyond the immediate financial cost, cloud application security exposures can lead to additional reputational damage. Take note of the nonfinancial effects security risks can have on businesses:

Damaged brand image

A successful cyberattack can force business activity offline for days or weeks. When that happens, customers aren't getting the products or services they paid for (or intend to pay for). That can cause serious, lasting damage to an organization's brand.

Lost trust

The advent of mass data sharing in the digital economy means customers entrust companies and organizations with reams of their personal information. If a business suffers a cyberattack, customers may worry their data or assets are not safe with the company.

Organization disruption

In the event of a cybersecurity attack, in most instances more could have been done to prevent the attack. Consequently, this means some team members will be held responsible. This can lead to terminations and replacements, which is disruptive for an organization.

Forced closures

Some security breaches are so damaging that affected organizations never recover. The impacted organization may drastically reduce their operations or close down permanently. These occurrences are rare, but not out of the realm of possibility.

[**Related Reading:** Top 8 Data Security Best Practices]

CLOUD APPLICATION SECURITY BEST PRACTICES

Cybersecurity attacks are on the rise, especially with so many enterprises using cloud applications to streamline their business process and services. Here's what organizations can do to enhance their cloud application security.

Train

employees on password best practices, including using a mix of numbers, symbols and lower- and uppercase letters.

Invest

in a cloud security solution that's capable of identifying any potential attack vectors in the cloud ecosystem.

Conduct

regular security audits to understand who has access to different data, and make adjustments as needs and responsibilities change.

Update

security software regularly to make sure systems are best equipped to protect critical data from the latest threats.

Create

privileged access guidelines to authorize only those teams and individuals who require data to actually use it.

Ensure

compliance with all relevant data security frameworks to protect information and instill confidence in customers and clients.

Automate

security processes to minimize and eliminate the risk of costly mistakes that could lead to data loss.

FORTRA

At Fortra's Alert Logic, we provide unrivaled security for any environment. Learn how managed detection and response (MDR) provides comprehensive coverage to protect against known and unknown threats to your cloud applications.

alertlogic.com/managed-detection-and-response

Security culture

As the prevalence of cloud computing continues to rise, so do the associated security risks. Consequently, organizations must establish a culture of strategic information security that addresses the unique security challenges posed by cloud computing. This paper will propose a strategic information security culture for cloud computing, suggest policies to enforce it and address how to implement and administer these policies effectively.

Strategic Information Security Culture Identification for Cloud Computing: Extensive research was conducted to identify the most pertinent strategic information security culture. The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a recognized approach for addressing cybersecurity risks, including those related to cloud computing. The NIST framework emphasizes five fundamental functions: Identity, Protect, Detect, Respond, and Recover.[Citation97]

Therefore, the proposed strategic information security culture for cloud computing must be based on the NIST Cybersecurity Framework. This framework offers a comprehensive and adaptable approach to resolving cloud computing security risks. By identifying the unique risks associated with cloud computing, organizations can tailor the framework to their particular requirements.

Access control policy

This policy describes the criteria for granting access to cloud-based resources and data as shown in Figure 11. There have been instances in which user data has been leaked, underscoring the necessity for solid security measures.[Citation98,Citation99] Most of the research in cloud computing security is primarily concerned with safeguarding data privacy,[Citation100] the utilization of ciphertext for data retrieval and possession of evidence,[Citation100] and access control,[Citation101] which is essential for preventing unauthorized access to confidential data.

Figure 11. Access control model.

Access control is crucial to safeguard cloud-stored data and has undergone extensive research. Belguith et al.[Citation102] presented the concept of access control, highlighting its key elements such as access control techniques, subjects, and objects. Among the access control methods mentioned is Discretionary Access Control (DAC),[Citation103] which provides complete access authorization to the object owner based on user identification authentication and access rules, but it may contribute to unrestricted access rights and difficulty in administration. DAC is one of the access control methods. The use of a security marking mechanism, which can only accomplish coarse-grained access control, is incorporated into the architecture of the Mandatory Access Control (MAC),[Citation104] the system is designed to meet the confidentiality requirements of the information by implementing the Role-Based Access Control (RBAC) mechanism,[Citation105,Citation106] Initially, access rights are assigned to specific roles, which are subsequently assigned to administrators. However, RBAC might not validate the identification and authorization of network entities. The use of the requester's and the resource's attributes to make access decisions enables adaptable and confidential access.[Citation107] Attribute access control is a technique of access management that is built on attribute encryption.[Citation108]

On the other hand, these access control methods cannot identify unauthorized data access or optimize access control policies promptly. Additionally, A potential solution involves implementing a data protection model that incorporates access control mechanisms utilizing encryption attributes and employs a data access detection algorithm. This integrated approach establishes a closed-loop control system that generates real-time feedback, enabling continuous optimization of data access control strategies. As a result, the overall integrity of data protection is enhanced, providing a robust framework for safeguarding sensitive information.

Data protection policy

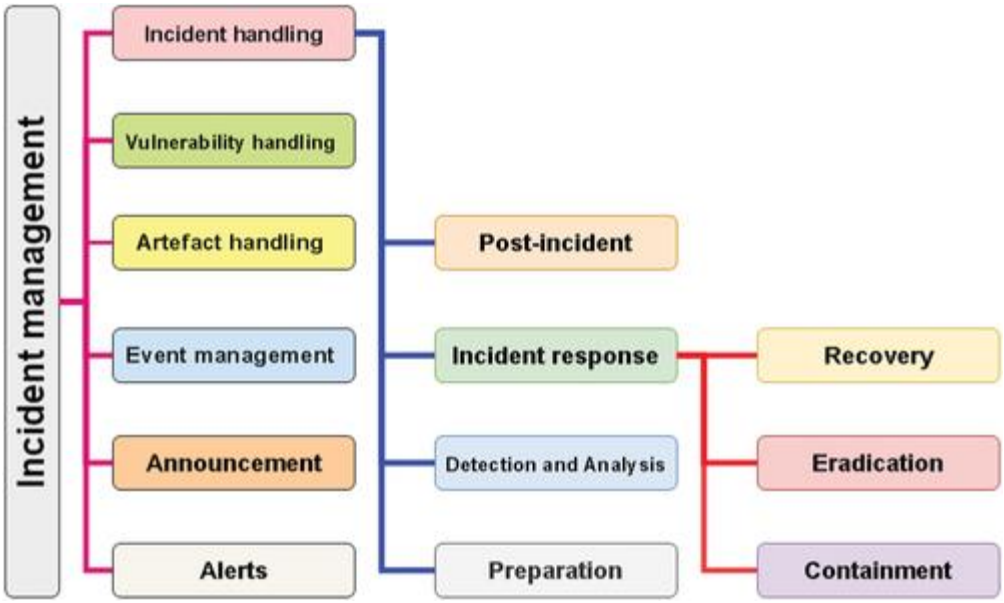
Data protection policy in cloud data protection encompasses the regulations and protocols governing the handling, storage, processing, and sharing of sensitive data within cloud environments. As the utilization of cloud computing services continues to grow, ensuring the security of cloud data has emerged as a paramount concern for businesses and organizations across the globe.[Citation70] Data protection policies in cloud computing place significant importance on encryption.[Citation109] Encryption transforms sensitive data into an unintelligible format that can only be accessed with the corresponding decryption key. Before preserving data in the cloud, encrypting it to prevent unauthorized access is essential. To ensure data security, robust encryption algorithms such as Advanced Encryption Standard (AES) should be utilized. Access management is an additional essential component of a comprehensive data protection strategy for

cloud computing.[Citation110] The term"access control" refers to a method used to safeguard private data kept in the cloud by preventing unauthorized users from gaining access. The process involves allocating rights to users based on their designated roles, the provided duties, and the level of trust they have earned. The implementation of access control rules is vital in ensuring that only authorized personnel are able to access private data that is kept in cloud-based systems. It is important to have established data backup and recovery protocols to guarantee the ability to recover critical data in case of data loss.[Citation111] Regular data backups should be taken, and backup data should be kept secure. Compliance with regulatory standards like GDPR, HIPAA, and PCI DSS is essential for data protection in the cloud.[Citation112] Organizations must ensure that their data protection policies align with these standards to avoid legal and financial repercussions.

Incident response policy

This policy lays out the procedures that are to be followed if there is a security breach. It should include protocols for reporting incidents, limiting the damage, and carrying out post-incident reviews Figure 12.

Figure 12. Incident management.



After an incident has been identified, it is necessary to react appropriately to reduce the adverse effects of the incident. The term"response" was coined by Baskerville et al.[Citation113] to describe an immediate and purposeful reaction to an occurrence. During this period, the emphasis is placed on activities that are reactionary rather than preventative measures. Three critical steps must be taken to effectively respond to an incident: confinement, elimination, and

recuperation.[Citation114] Changing the credentials on infiltrated systems is one example of a confinement and elimination strategy that can be implemented. Other examples include turning off the contaminated system, securing compromised accounts, and stopping incoming network traffic. In addition, the significance of backup and recovery in enhancing performance and procedure and making use of sophisticated technologies, such as online backup and cloud storage, has been highlighted by research efforts in recent years.[Citation114] No technique or strategy is universally applicable when responding to security situations, just as no two criminal scenarios are ever the same. Cichonski et al.[Citation114] suggests considering the following parameters when developing an effective incident response strategy:

- The protection of existing information.
- Availability of services, including network communication and services supplied to third parties and the general public.
- Time and workforce requirements for implementation.
- The approach's effectiveness may include complete or partial confinement of the situation.
- The time that the solution will be in effect, including whether it is a transient or permanent remedy or an emergency alternative that will be eliminated later.

In a perfect world, incident response strategies should be adapted to particular circumstances to deploy them rapidly. This rapid deployment can be achieved through the utilization of automatic tools. One illustrative tool is the Automated Incursion Response System (AIRS), which employs an automated decision-making process to select and implement suitable response options promptly.[Citation115] It has been demonstrated through research carried out by Luo et al.,[Citation116] Anwar et al.[Citation117] that AIRS is effective in reducing the time between detection and response. This leads to the genuine case of complex and multistage attacks, significantly improving incident response rates.

Implement policies effectively

There are various phases of cloud interactions where risk analysis can be conducted.[Citation118] Providers participating in the cloud have security concerns regarding other providers, which can be related to trust, service hazards, or legal issues. Providers may need to evaluate the risk of collaborating with other providers, or they may need to address specific security requirements. Risk assessments can also vary depending on the form of cloud deployment—private, public, or hybrid. Analyzing security concerns in the context of cloud computing reveals that each concern has distinct effects on various assets.[Citation118] Given the circumstances wherein organizations lack resources or expertise to implement and sustain cloud security frameworks effectively, several suggestions can be gleaned from the extant body of literature. According to Chauhan and Shiaeles,[Citation43] acquiring knowledge about diverse cloud security frameworks is

critical to making well-informed choices concerning the choice and execution of appropriate security protocols for cloud-based systems. As a result, organizations should prioritize acquiring knowledge regarding various frameworks to comprehend their particular security needs and make well-informed decisions.

Furthermore, Ismail and Islam[Citation75] put forth a cohesive framework that addresses the transparency and audit of cloud security. Organizations that need to possess strong proficiency in cloud security may find this framework especially advantageous, given that it offers a methodical strategy for augmenting the transparency and audibility of cloud security procedures. By implementing this framework, organizations can establish a more methodical and all-encompassing strategy for safeguarding against cloud threats, even when confronted with limited resources or expertise. When evaluating cloud frameworks, it is essential to carefully analyze their compatibility, flexibility, and applicability in different cloud settings and use cases. Chauhan and Shiaeles[Citation43] highlights the need to thoroughly compare the focal point, extent, methodology, effectiveness, constraints, implementation procedures, and necessary tools in deploying cloud security frameworks. An extensive examination is essential for evaluating the relevance and appropriateness of each framework in various cloud settings and use cases. In addition, Ismail and Islam[Citation75] provide a comprehensive framework for enhancing transparency and auditability in cloud security. This paradigm can potentially provide valuable insights into the effectiveness of security frameworks in various cloud settings. It is crucial to comprehend how these frameworks may be integrated and customized for different cloud settings to assess their flexibility. In addition, Andrikopoulos et al.[Citation119] examine the process of modifying programs for the cloud environment, emphasizing the significance of flexibility in cloud computing. This source offers excellent perspectives on the flexibility of programs, which may also be used for the flexibility of cloud frameworks in many scenarios and settings. Aside from applicability, flexibility, and appropriateness, numerous more considerations should be considered while assessing cloud security classes. The methodical architectural support for adaptability during cloud migration, as emphasized by Jamshidi et al.,[Citation79] is of utmost importance. This highlights the need to consider the architectural elements and support systems to ensure smooth migration and integration of security frameworks across various cloud environments. In addition, Chauhan and Shiaeles[Citation43] highlight the need to consider the risk factors associated with significant cloud security risks and their influence on cloud platforms. This suggests that while evaluating cloud security categories, it is essential to thoroughly analyze the possible risks and threats that impact the efficiency of security frameworks in various cloud settings and use cases.

- Evaluate potential risks and vulnerabilities within the cloud environment by conducting a risk assessment.

- Create a comprehensive plan that outlines how security policies will be implemented and enforced. This plan should also identify who is responsible for implementing and enforcing the policies.
- Regular training and awareness initiatives should be conducted for employees and stakeholders to ensure their familiarity with security policies and to enhance their understanding of their responsibilities in maintaining a secure cloud environment.
- Regularly monitor the adherence to security policies and evaluate their effectiveness in mitigating risks to ensure ongoing compliance and effectiveness.
- Update the security policies as necessary to reflect any changes in the cloud environment or emerging security threats.

Figure 13 demonstrates that there are different phases involved in the methodology of risk mitigation, this including the process encompasses several stages, namely risk identification, risk assessment, risk management, risk planning, risk resolution, and risk monitoring. Throughout these phases, it is crucial to account for potential risks associated with collaborating with other providers and adhere to any specific security requirements.[Citation118]

Figure 13. Implement and manage policies.

As organizations increasingly move their data storage and processing to the cloud, they face a significant threat of having their most valuable information lost, breached, or otherwise compromised.[Citation15] Therefore, a reliable Risk management strategy and models are required to safeguard vital data assets.[Citation120] The first phase in the process of risk management is the recognition and identification of possible hazards or risks. The subsequent phase is formulating solutions to alleviate or counter the identified dangers. The first phase of risk management involves the identification of prospective hazards that may pose a threat to an organization's data and computer infrastructure. Furthermore, an assessment is conducted to determine the potential magnitude of damage that these hazards may inflict upon the organization if they were to materialize.[Citation120] The second step is mitigating those dangers once they have been discovered. El Fray[Citation121] claims that over 200 different security models are in use today due to the rapid development of online services. ISO27005, NIST SP 800–30, CORAS,

CRAMM, OCTAVE, and COBIT are some of the widely-used risk evaluation techniques that can be applied to evaluating and assessing the dangers impacting cloud-based systems and services.[Citation15]

Static mapping

The static mapping model involves matching a predetermined incident alert with a predetermined response. However, this approach presents challenges, including the possibility of an adversary predicting the response.[Citation122]

Dynamic mapping

The dynamic mapping model is a method for selecting response strategies according to incident context.[Citation115] However, diverse strategies have been proposed to reduce response time and balance security and usability. Risk assessment models, such as the Risk Index Model and Response Strategy Model, have been devised to rank incidents according to their severity and likelihood of vulnerability. Machine learning methods, such as the Markov decision model and Hidden Markov Model, have been employed to improve the balance between response accuracy and adaptability. The theory approaches such as Response and Recovery Engines and Dynamic tree-based have been proposed to minimize conflicts of reactions.[Citation122]

Cost-sensitive mapping

The cost-sensitive response model aims to achieve a balance between damage and response costs by minimizing four factors: implementation costs, resource utilization, time efficiency, and costs associated with modifications.[Citation122] The three most important factors are damage, response, and operational costs. Several methods have been proposed to improve cost response and seek trade-offs, including preemptive cost-sensitive response and balancing intrusion damage and response cost. These strategies consider intrusion patterns, available resources, security policies, and system environments to initiate the appropriate response.[Citation123]

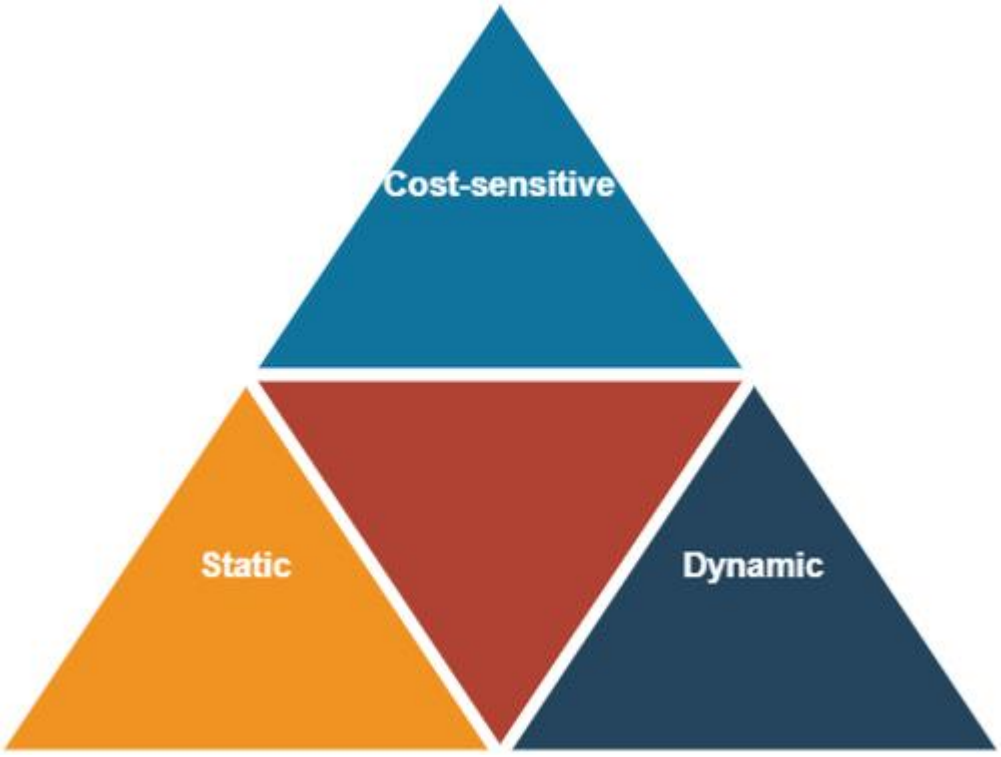
Post-incident

The phase that follows the resolution of an incident is known as the post-incident phase.[Citation122] During this phase, personnel must be highly proactive in identifying and reflecting on new hazards and improving protection mechanisms. During this phase, information and results are compiled to provide feedback to improve incident management. Adaptive incident learning, the process of transmitting knowledge or experience garnered during an incident to future actions, has been identified as a critical post-incident phase component. This ability to learn from and adapt to past experiences is crucial for future incident management.[Citation124]

Even though it plays an essential part, the significance and importance of incident learning receive a different level of attention than the technological elements of incident management.[Citation125] According to Ab Rahman and Choo,[Citation122] the organizational learning theory has been employed as a conceptual framework to explore how organizations can acquire knowledge to guide their practices through various forms, norms, procedures, and strategies. This investigation was carried out using the organizational learning theory. On the other hand, ontology is a method of knowledge management that provides a rigorous specification of computer concepts that can be interpreted across various disciplines and their interrelationships.[Citation124] *Ontology* is a strategy that can be used with other knowledge management methods. It has been hypothesized that this method could facilitate more efficient education provided by the (Computer Security Incident Response Teams) CSIRT to a more extensive population.

The primary objective of the post-incident phase is to collect data from the preceding three phases for learning and development, as demonstrated by Ab Rahman and Choo[Citation122] in their work, as shown in Figure 14. This information is typically documented in a report.[Citation126] Additionally, this stage involves presenting formal reports to higher-level management and suggesting enhancements to incident handling, considering both technical and managerial aspects. Taylor[Citation126] implies that conducting research on generic information content and templates would be beneficial in generating a comprehensive and informative report, particularly when the report is intended for utilization by law enforcement agencies or in a courtroom setting.[Citation122]

Figure 14. Three response models.



Therefore, a strategic information security culture is essential for ensuring data and resources' security and integrity in a cloud computing environment. By implementing and enforcing suitable policies, organizations can proficiently mitigate the risks linked to cloud computing, thereby protecting their data and assets.

Technical security controls

Cloud computing presents various security challenges due to its shared infrastructure, distributed resources, and lack of physical control. To ensure the availability, confidentiality, and integrity of information assets, it is crucial to implement effective technological security measures such as encryption, access control, Multi Factor Authentication (MFA), Intrusion Detection and Prevention Systems (IDPS), and Data Loss Prevention (DLP). By implementing these technical security controls, organizations can effectively thwart unauthorized access, data leakage, and various security incidents. This proactive approach to security significantly strengthens the overall security stance of cloud computing environments, minimizing the risks associated with threats and attacks. It is essential for organizations to thoughtfully choose their security controls, taking into consideration their risk profile, compliance obligations, and security goals.

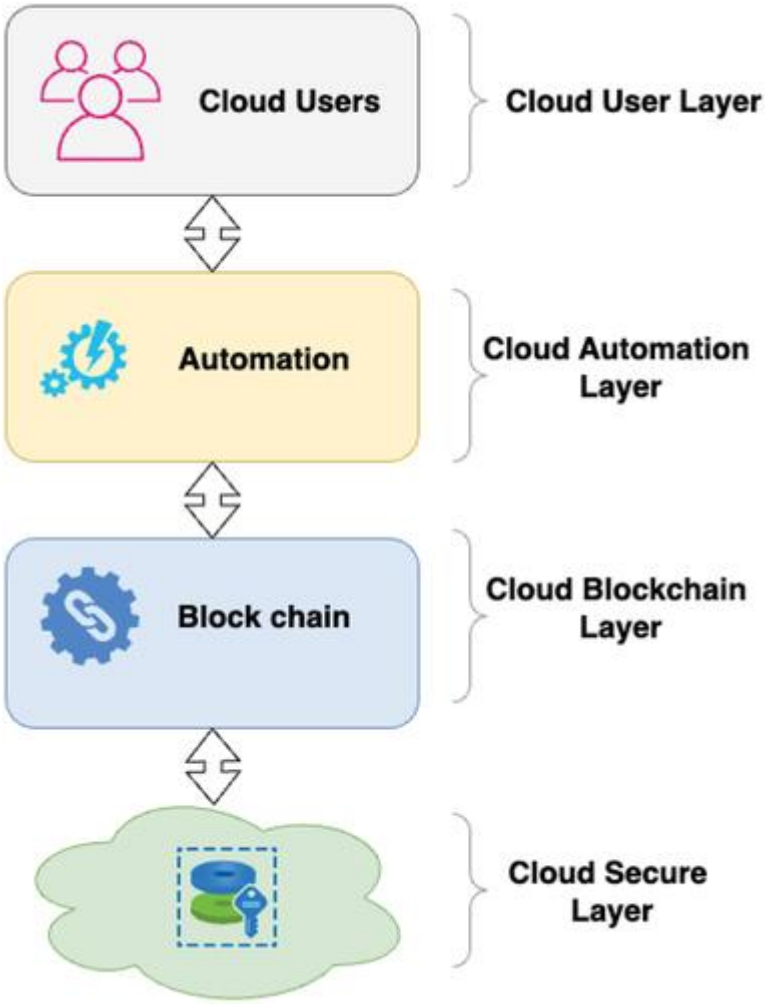
Due to the shared infrastructure and lack of physical control in cloud environments, maintaining confidentiality, integrity, and availability is challenging. Therefore, adequate technical security controls are essential to secure cloud computing environments. This review will critically assess the state-of-the-art technical security controls for cloud computing and recommend the most effective protection mechanisms.

Encryption

Encryption is a cryptographic process that converts data from its original, unencrypted form to ciphertext. This transformation is achieved through a mathematical procedure, ensuring the confidentiality of the data. In Figure 15, encryption is one of the most effective technological safeguards to protect data from unauthorized access during transmission and while at rest. However, the effectiveness of encryption depends on the encryption technique used, key management, and access restrictions. Hence, it is imperative for businesses to meticulously choose encryption algorithms and adopt effective key management practices in order to guarantee the authenticity and confidentiality of their data. Table 10 demonstrates an evaluation of the encryption's strengths, shortcomings, and prospective consequences. For instance, Butt et al.[Citation127] highlights the importance of encryption in cloud computing as it helps protect data from unauthorized access. Pavithran et al.[Citation128] conducted an in-depth analysis of the applications of blockchain technology in cloud storage security from 2010 to 2019. Containerization and virtualization architectures, as well as reliable intrusion detection that uses blockchain, were a few topics covered in Alkadi et al.[Citation29] discussion of collaborative anomalous detection mechanisms for recognizing external and insider assaults from cloud centers. Their article

provided a high-level analysis of cloud infrastructure and recognized potential contemporary security incidents based on the predominance of certain security flaws in various cloud implementation models. They also highlighted how the Network Intrusion Detection System (NIDS) for cloud-based blockchain applications could resolve data protection and confidence management problems. The decentralized and disseminated character of the blockchain process, which guarantees protection specifications and improves cloud storage security, was emphasized in Mughal and Joseph[Citation129]'s proposal for blockchain as a solution for cloud security and storage.

Figure 15. Secure encryption-based cloud framework.



Access control

Access management is vital to ensuring the security of cloud computing, with the goal of preventing unauthorized users from gaining access to sensitive data and resources. Organizations can implement access control via a variety of methods, including Role-Based Access Control (RBAC), Attribute Based Access Control (ABAC), and mandatory access control mechanisms (MAC). RBAC is the most commonly used access control technique, offering the potential to streamline access management and reduce the risk of unauthorized access. Access management has been highlighted as an essential security measure for cloud computing by Mondal et al.[Citation130] This measure can prevent unauthorized access to confidential resources and is one of the most essential security measures.

Cloud computing users can be classified into three groups: malicious users, inadvertent users who experience losses due to organizational errors, and users with a history of successful use. Traditional access control methods become ineffective in cloud computing due to the dynamic nature of resource allocation. This is because the cloud server automatically and in real-time distributes resources based on the application being run by the user. Consequently, in their work Venifa Mini and Angel Viji,[Citation131] introduces the “T-RBAC” model (trust and role-based access control), which uses trust as the basis for user authorization and employs a Markov model to enable dynamic user authorization.

Blaze et al.[Citation132] are credited with being the first person to put forward the idea of confidence as a solution to the problem of insufficient security information in an open system. The T-RBAC paradigm provides for the distribution of varying trust values among users and the distribution of varying authorization to users following their trust values. The authorization procedure is carried out dynamically under the Markov model. This dynamic access control authorization follows the dynamic characteristics of cloud computing users and resource utilization. It allows authorization to be adjusted in real-time, preventing unauthorized access by malevolent users.

The process of access control has progressed through several phases, with the primary areas of emphasis now being access control models, access control founded on cryptography, and virtual machine access control in cloud computing environments.[Citation133,Citation134] These access control mechanisms have been intended to accommodate the enormous, dynamic, and stringent private characteristics of new computing environments such as cloud computing and the

Internet of Things (IoT). Table 10 presents the results of a critical analysis of the access control system.

Multi-factor authentication

According to Bose et al.,[Citation135] Security measures based on Multi Factor Authentication (MFA) necessitate using more than one form of user identification before granting access to protected areas or data (see Table 10). Limiting unauthorized access due to compromised credentials makes this a helpful security technique for cloud computing. One Time Passwords (OTP), smart cards, fingerprint identification, and device authentication can be used to establish MFA in an organization. The use of MFA in cloud computing environments can substantially enhance their security posture and lower the likelihood of unauthorized access. Traditional access control approaches are inadequate because of the unpredictable behavior of cloud computing users and resource distribution.[Citation136]

The cloud administration framework utilizes a multi-factor authentication procedure, which validates activities using a combination of fingerprint, password, and secret essential authentication methods that provide a higher level of protection; the system generates a private key through AES cryptography and incorporates the users' fingerprints and passcode information. When the biometric information a user provides matches the biometric affiliated with the user, the user can access the system. The AES algorithm generates keys based on different fundamental values Table 9, determining the number of repetition rounds for the transformation. Table 9 shows the number of repetition rounds is determined by the size of the key.[Citation26]

Table 9. Number of reiteration cycles for different key sizes in AES[Citation26].

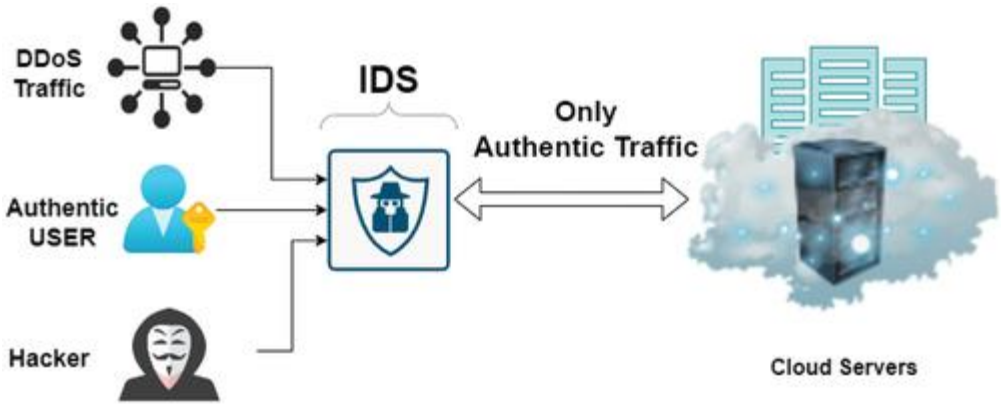
Intrusion detection

According to Nadeem et al.[Citation137] in their study, cloud computing offers advantages such as cost savings, resource accessibility, and improved performance. However, the growing number of cloud computing users increases the risk of attacks. The Intrusion Detection System (IDS) monitors the attack rate of each device on the network. See the Table 10 for details. Intrusion Detection and Prevention Systems (IDPS) are regarded as one of the vital tools for safeguarding the cloud server against attacks 14, which monitors network activity and prevents unauthorized access, data breaches, and other security incidents.[Citation138] Implementing IDPS in cloud computing environments can significantly improve overall security and prevent various security incidents, as pointed out by.[Citation138] Therefore, IDPS is considered a critical security strategy for cloud computing.

Table 10. Technical security controls critical assessme

One of the many approaches to resolving cloud security issues that various solutions can carry out is utilizing an IDS, as shown in Figure 16. According to Basu et al.,[Citation139] keeping data on cloud computing can present several risks, and the primary challenge related to cloud computing revolves around ensuring cloud security and safeguarding against various attacks and breaches. Threats come in many forms, such as those posed by software, inside assaults, a lack of support and standardization, and more. According to Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India. et al.[Citation140] anti-malware and security software by themselves are not enough to safeguard a complete network or to provide protection on their own, so the intrusion detection system, a hardware component, functions upon connection to a network., keeps an eye out for potentially malicious behavior on that network and alerts the administrator when something goes wrong. Aryachandra et al.[Citation141] developed an architecture implemented on a practical utility called snort. An automatic host-based methodology was suggested by Gassais et al.[Citation142] that uses machine learning techniques to identify intrusions coming from smart devices. Mazini et al.[Citation143] leverages machine learning models to enable anomaly-based intrusion detection systems. She also develops a mixed method, uses the AdaBoost algorithm, and discovers enormous exposure charges with an inexpensive determined charge. De La Torre Parra et al.[Citation144] went through several articles and discussed how DOS attacks could occur on cloud platforms, webpages, levels of the OSI model, and other places.

Figure 16. Intrusion detection architecture.



Display full size

Several researchers have conducted numerous studies to make cloud computing secure. Their research entails the design of various algorithms and architectural constructions to keep the cloud secure, as well as the review of numerous publications demonstrating improved detection techniques. It was also proposed to use an intrusion detection system and machine learning algorithms to detect

intrusion from intelligent devices. Nevertheless, further research is needed to explore novel models that can enhance the performance of IDS and address their inherent challenges. Also, it is essential to think about what could cause DOS attacks and take the steps needed to stop them from happening on cloud servers.

Data loss prevention (DLP)

Data Loss Prevention (DLP) serves as a protective mechanism that monitors data transfers and safeguards against data loss, leakage, and unauthorized access as shown in the Table 10. Bucur et al.[Citation145] stress that data loss prevention (DLP) is an essential security measure for cloud computing because it can stop confidential data from exiting the cloud environment. DLP can be network- or host-based, and it can prevent confidential data from exiting an environment hosted in the cloud. DLP has the capacity to considerably improve the general safety condition of cloud computing environments and prevent numerous security breaches.

Several different techniques use pre-defined keywords and regular expressions to locate confidential information. Nevertheless, employing these techniques requires a substantial number of rules, which can result in a decline in detection accuracy due to an increase in false positives.[Citation145] Costante et al.[Citation146] introduced a methodology for the protection of data loss that was based on signature-based methods in addition to anomaly-based methods. A machine learning technique is utilized by the framework in order to conduct an analysis of user behaviors and to develop a collection of malevolent behavior indicators. Using the Named Entity Recognition technique, Gómez-Hidalgo et al.[Citation147] suggested yet another method for preventing data loss, but it cannot safeguard pictures. Ong et al.[Citation148] presented a system that uses deep learning to identify confidential information in documents based on semantic context analysis. However, the application of this system is restricted to identifying sensitive information only in documents. These approaches have some drawbacks, and it is possible that we cannot use them in the real world because they need to work better.

The Cloud Access Security Broker (CASB) is widely recognized as a prominent technology in cloud security,[Citation149] and Gartner has approved this technology. To protect vital information, it functions by utilizing proxy servers developed by various cybersecurity companies such as CipherCloud.[Citation150] The Cloud Access Security Broker functions by installing a gateway server between users and cloud applications. By performing protocol analysis, this intermediary can identify confidential data, intercept it, and encrypt it. The implementation of this strategy, on the other hand, requires the reverse engineering of network protocols for a variety of cloud applications, this process can consume significant time and effort due to its labor-intensive nature. As a result, the adaptability of this methodology to a variety of different applications is constrained.

Song has developed a plug-in for web browsers called ShadowCrypt,[Citation151] that encrypts textual data in preexisting cloud services. However, it cannot handle data items such as binary files or picture files. Mimesis Aegis[Citation152] offers confidential data separation via a conceptual layer for mobile apps but does not offer data file security. CryptDB[Citation153] acts as an intermediary between the database and application servers to secure sensitive user information. This technique protects sensitive information in a database from a nosy database owner. Regrettably, it only works with datasets at the moment. Grubbs et al.[Citation154] is an online application data security solution built on the Meteor JavaScript infrastructure. However, Mylar is compatible with only certain platforms and lacks the ability to support data processing tasks. Virtru[Citation155] it is a web-based solution that provides e-mail encryption and leak prevention capabilities. Although it works well for e-mail systems, it has limited potential for use in cutting-edge software.

Cloud storage services,[Citation156] platforms such as Box, Dropbox, and Salesforce remain widely used in business settings due to their convenience in online collaboration and communication, cost-saving benefits for data storage, and guaranteed data dependability. Despite these advantages, such services are susceptible to exploitation and abuse, which can result in the exposure of confidential information to untrusted environments. Reports indicate security vulnerabilities in Google Drive, Dropbox, and Box, which may grant unintended users access to confidential files and connections to file transfers. Furthermore, the flaws of Amazon S3 have led to the potential disclosure of sensitive medical and military information. As a direct consequence, it is imperative to prevent confidential data from being transferred from on-premises corporate networks to less secure online storage locations.

In conclusion, data loss prevention (DLP) is an essential security measure for cloud computing environments, as a protective measure against the risks of data loss, unauthorized access, and leakage. Numerous methods and approaches can be employed to effectively incorporate DLP into an organization’s security strategy, such as pre-defined keywords and regular expressions, machine learning, and the use of Cloud Access Security Broker (CASB). However, these approaches have their drawbacks and limitations. Various tools such as ShadowCrypt, Mimesis Aegis, CryptDB, Mylar, and Virtru offer data encryption and security but are limited to specific platforms or data types. Cloud storage services are also susceptible to security vulnerabilities, which can lead to the exposure of confidential information. Therefore, it is crucial to prevent confidential data from being transferred to less secure online storage locations.

Conclusion

In summary, cloud computing is a popular technological innovation providing centralized computing services and resources. It offers multiple deployment modes and models, including public, private, community, and hybrid, with infrastructure, platform, and software. Cloud hosting has advantages like expansion flexibility and minimal effort but disadvantages like losing control over infrastructure and data. Cloud computing offers benefits like decreased costs and time, improved performance and dependability, and infinite computing resources on demand. However, security concerns remain significant as cloud computing presents challenges like data security and privacy, authentication, encryption, data integration, and access issues. Critical cloud hosting requires a robust security framework capable of adjusting to the surrounding context, involve the appropriate resources, and effectively manage risks. As businesses transfer their valuable data assets to cloud-based infrastructure, new risks that require a proper approach to risk management, assessment, and governance are associated with this migration. There are multiple methodologies for security risk management and assessment in cloud-based systems. The OCTAVE Allegro, COBIT 5, and CORAS models are recommended for the cloud hosting approach as they address the CIA Triad, emphasizing the storage, processing, and transmission of information. However, the ISO27005, NIST SP 800–30, and CRAMM models, although comprehensive, may not offer specific and accurate guidelines for assessing and evaluating cloud-related risks. The CORAS, OCTAVE and COBIT5 models provide a clear procedure for addressing risks related to both internal and external systems and software resources, including the specific infrastructure of cloud computing. COBIT 5 also encompasses the governance aspect when managing cloud systems. Therefore, the research indicates the possibility of additional investigation to integrate and adapt the mentioned methods, as well as assess various risk management approaches considering different factors.

References

- Tripathi A, Mishra A. Cloud computing security considerations. In: 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC); 2011 Sep. p. 1–5.

  Google Scholar

- Wang J, Mu S. Security issues and countermeasures in cloud computing. In: Proceedings of 2011 IEEE International Conference on Grey Systems and Intelligent Services; 2011 Sep. p. 843–46.

Google Scholar

- Khan MI, Ullah F, Imran M, Khan JAM, Khan A, AlGhamdi AS, Alshamrani SS. Identifying challenges for clients in adopting sustainable public cloud computing. Sustainability. 2022;14(16):9809. doi:10.3390/su14169809.

  Web of Science ®Google Scholar

- Tissir N, El Kafhali S, Aboutabit N. Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. J Reliab Intell Environ. 2021;7(2):69–84. doi:10.1007/s40860-020-00115-0.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

- Tripathi A, Mishra A. Cloud computing security considerations. In: 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC); 2011 Sep. p. 1–5.

  Google Scholar

- Wang J, Mu S. Security issues and countermeasures in cloud computing. In: Proceedings of 2011 IEEE International Conference on Grey Systems and Intelligent Services; 2011 Sep. p. 843–46.

  Google Scholar

- Khan MI, Ullah F, Imran M, Khan JAM, Khan A, AlGhamdi AS, Alshamrani SS. Identifying challenges for clients in adopting sustainable public cloud computing. Sustainability. 2022;14(16):9809. doi:10.3390/su14169809.

  Web of Science ®Google Scholar

- Tissir N, El Kafhali S, Aboutabit N. Cybersecurity management in cloud computing: semantic literature review and conceptual framework

proposal. J Reliab Intell Environ. 2021;7(2):69–84. doi:10.1007/s40860-020-00115-0.

Google Scholar

- El Kafhali S, Salah K. Modeling and analysis of performance and energy consumption in cloud data centers. Arab J Sci Eng. 2018;43(12):7789–802. doi:10.1007/s13369-018-3196-0.

  Web of Science ®Google Scholar

- Lucanin D, Pietri I, Holmbacka S, Brandic I, Lilius J, Sakellariou R. Performance-based pricing in multi-core geo-distributed cloud computing. IEEE Trans Cloud Comput. 2020;8(4):1079–1092. doi:10.1109/TCC.2016.2628368.

  Web of Science ®Google Scholar

- Szalay M, Mátray P, Toka L. State management for cloud-native applications. Electronics. 2021;10(4):423. doi:10.3390/electronics10040423.

  Web of Science ®Google Scholar

- Hanini M, Kafhali SE, Salah K. Dynamic VM allocation and traffic control to manage QoS and energy consumption in cloud computing environment. Int J Comput Appl Technol. 2019;60(4):307–16. doi:10.1504/IJCAT.2019.101168.

  Web of Science ®Google Scholar

- Shakir M, Hammood M, Muttar AK. Literature review of security issues in saas for public cloud computing: a meta-analysis. Int J Eng Technol. 2018;7(3):1161–71. doi:10.14419/ijet.v7i3.13075.

  Google Scholar

- Shanmugapriya E, Kavitha R. Medical big data analysis: preserving security and privacy with hybrid cloud technology. Soft Comput. 2019;23(8):2585–96. doi:10.1007/s00500-019-03857-z.

Web of Science ®Google Scholar

- Abomhara M, Yang H. Collaborative and secure sharing of healthcare records using attribute-based authenticated access. Int J Adv Secur. 2016;9(3).

  Google Scholar

- Tariq MI. Agent based information security framework for hybrid cloud computing. KSII Trans Int Inf Syst. 2019;13:406–34.

  Web of Science ®Google Scholar

- Li Z, Tang Z, Lv J, Li H, Han W, Zhang Z. An information security risk assessment method for cloud systems based on risk contagion. In: 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC); 2020 Jun. p. 83–87.
  - View

  Google Scholar

- Tian J. Quantitative assessment method of multi-node network security situation based on threat propagation. Comput Res Dev. 2017;54:731–41.

  Google Scholar

- Irsheid A, Murad A, AlNajdawi M, Qusef A. Information security risk management models for cloud hosted systems: a comparative study. Procedia Comput Sci. 2022;204:205–17. doi:10.1016/j.procs.2022.08.025.

  Google Scholar

- Iqbal S, Mat Kiah ML, Dhaghighi B, Hussain M, Khan S, Khan MK, Raymond Choo KK. On cloud security attacks: a taxonomy and intrusion detection and prevention as a service. J Netw Comput Appl. 2016;74:98–120. doi:10.1016/j.jnca.2016.08.016.

Web of Science ®Google Scholar

- Padmaja K, Seshadri R. Analytics on real time security attacks in healthcare, retail and banking applications in the cloud. Evol Intel. 2021;14(2):595–605. doi:10.1007/s12065-019-00337-z.

  Web of Science ®Google Scholar

- Chen D, Zhao H. Data security and privacy protection issues in cloud computing. In: 2012 International Conference on Computer Science and Electronics Engineering. Vol. 1; 2012 Mar. p. 647–51.

  Google Scholar