


Please cite the Published Version

Ali, T, Al-Khalidi, M  and Al-Zaidi, R (2024) Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. Journal of Computer Information Systems. pp. 1-28. ISSN 0887-4417

DOI: <https://doi.org/10.1080/08874417.2024.2329985>

Publisher: Taylor and Francis

Version: Published Version

Downloaded from: <https://e-space.mmu.ac.uk/634479/>

Usage rights:  [Creative Commons: Attribution 4.0](https://creativecommons.org/licenses/by/4.0/)

Additional Information: This is an open access article published in Journal of Computer Information Systems, by Taylor and Francis.

Enquiries:

If you have questions about this document, contact openresearch@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from <https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines>)

Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review

Tarek Ali, Mohammed Al-Khalidi & Rabab Al-Zaidi

To cite this article: Tarek Ali, Mohammed Al-Khalidi & Rabab Al-Zaidi (29 Mar 2024): Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review, Journal of Computer Information Systems, DOI: [10.1080/08874417.2024.2329985](https://doi.org/10.1080/08874417.2024.2329985)

To link to this article: <https://doi.org/10.1080/08874417.2024.2329985>



© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.



Published online: 29 Mar 2024.



Submit your article to this journal [↗](#)



Article views: 566



View related articles [↗](#)



View Crossmark data [↗](#)

Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review

Tarek Ali^a, Mohammed Al-Khalidi^a, and Rabab Al-Zaidi^b

^aManchester Metropolitan University, Manchester, UK; ^bUniversity of Salford, Manchester, UK

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

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.¹ 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.²

In the study conducted by Khan et al.³ 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.⁴ Moreover, Cloud Computing offers network-accessible services with virtually limitless computing resources, available on-demand without

requiring technical expertise or maintenance. Users are solely billed for the resources they actively utilize.^{5,6}

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.,⁷ 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.^{8–11} As mentioned in the given statement, these are considered to be the crucial areas of study,^{5,6} 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

CONTACT Tarek Ali  tarek.ali@stu.mmu.ac.uk  Department of Computing and Mathematics, Manchester Metropolitan University, All Saints Building, Manchester M15 6BH, UK

© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

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, Tariq¹² 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.¹³

In their work Li et al.¹³ 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.¹⁴ 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.¹³

Hosting in the cloud has become an essential strategic orientation for companies such as Amazon, Microsoft, and Google.¹⁵ 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.¹⁵ 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.¹⁵

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.¹⁶ Padmaja and Seshadri¹⁷ 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 meticulously developed and proactive information security management system is of the utmost importance to limit such attacks effectively. This paper examines the various classification and categorization schemes for cloud computing security issues, such as service models, deployment models, and involved parties, this research analyses the criteria and dimensions employed in developing classifications and taxonomies for cloud computing security. The study also focuses on the possibilities and problems presented to organizations when it comes to safeguarding their data in the cloud. This research is a valuable reference for businesses aiming to enhance their understanding of information security management in the context of cloud computing. It achieves this goal by concentrating on four primary key responsibilities: Risk Management and Auditing, Security Culture in Cloud Computing, Technological Security Controls, and Safeguarding Data in the Cloud.

The rest of the paper is structured as follows. [Section 2](#) presents a comprehensive analysis and comparison of various scholarly articles, incorporating our own. The section systematically reviews these papers

based on essential aspects of information security, such as privacy, data integrity, event management, frameworks, policies for counter-measures, solutions, and cryptography. The landscape of information security threats and attacks within cloud computing is discussed in [Section 3](#), while [Section 4](#) centers around highlighting risk management and auditing in cloud computing, exploring the importance of risk management, and conducting an extensive analysis of the numerous potential risks that businesses and organizations may encounter. Furthermore, it investigates the function that audits play in ensuring that cloud computing environments adhere to the set of security laws and regulations. The security culture in cloud computing is the primary emphasis of [Section 5](#). This section investigates the significance of cultivating a security conscious culture in cloud computing settings and considers the many approaches businesses may take to adopt this mind-set among their employees further. In [Section 6](#), technological security measures in cloud computing are investigated offering an overview of the various technological safeguards businesses can employ to defend their information systems against attacks and threats. In addition, the section investigates the difficulties associated with applying technical controls in an environment that is both dynamic and scalable. Finally, the paper is concluded in [Section 7](#).

Literature review

Cloud computing requires a comprehensive examination of information security threats and attack landscape; furthermore, it holds significant importance in this domain due to its growing prevalence in current business operations. This creates new and complex security threats, such as data breaches, Distributed Denial of Service (DDoS) attacks, and phishing; for example, unauthorized access causes one of the essential security threats, a data breach. Many approaches are available that ensure data integrity and make cloud computing more secure.¹⁸ Data integrity guarantees that digital data remains unaltered and can only be accessed or modified by authorized individuals.^{19,20} In their study, Pai T and Aithal²¹ have analyzed the security problems associated with cloud computing while discovering its possibility to enhance systems security issues cost-effectively.

Even though cloud computing technology has the advantage of making data easier, users need to be very careful and stay aware of the security risks and challenges that come with it. In their extensive analysis, Gill et al.²² conducted a comprehensive investigation into the privacy and security issues within

cloud computing, accompanied by a detailed case study on intelligent security keys. This case study emphasized the importance of effectively addressing security challenges in the field of cloud computing, stimulating further research in cloud security. Additionally, another study by Alrasheed et al.²³ have performed an analysis study concentrating on different deployment methods for intelligent devices in cloud computing services, encompassing the Internet of Things (IoT). They have recognized several data security matters and suggested tools and frameworks for assessing the security capabilities of cloud services.

Sadavarte and Kurundkar²⁴ executed a comprehensive examination of data security-related issues, analyzed considerable data security strategies and techniques, and offered several safe cloud data storage methods, all with the goal of delivering optimal data protection by mitigating threats and risks. Hussain et al.²⁵ Implemented was a distinctive model for categorizing security threats at multiple levels, specifically designed to identify risks associated with various cloud services. The model specifies risk ratings and attack types for each tier and determines the intensity of the danger categories dependent on the positioning of the layers within the cloud infrastructure. Additionally, the security requirements of different cloud services, including data encryption, multi-tenancy, data privacy, authentication, and authorization, are crucial factors in determining the extent to which these risk categories exist. The multi-layer categorization approach offers a flexible security framework for each layer of the cloud, addressing the specific security needs of both cloud providers and consumers.

Kumar et al.²⁶ surveyed data security issues in multi-tenant cloud computing environments, providing resolutions to address the problems. The research underlines that data violations or corruption can damage public confidence and confidentiality, leading to enterprise failure. The widespread adoption of cloud computing by numerous organizations underscores the importance for information security management firms to prioritize data security in this field. Radwan et al.²⁷ reviewed deployment and delivery prototypes for cloud computing and analyzed significant security considerations, threats, and problems facing the cloud field. The study also compares cloud computing with other computing models and highlights the need for security criteria for cloud deployment and delivery approaches. The authors conclude by summarizing possible investigation directions for cloud computing security.

Aldossary and Allen²⁸ determined obstacles to cloud implementation and proposed a new solution to reduce

associated risks. The emphasis was placed on addressing the specific obstacles associated with storing data in the cloud, including Confidentiality, Integrity, and data Availability (CIA). Various solutions were presented to tackle these challenges. Further, the same study highlighted the difficulty of conveying cloud-stored data among considerable users due to inconsistent authentication and approval by cloud service providers.

Data integrity protection is vital to stop unauthorized deletion, alteration, or manipulation of data and stop accessing valuable information or services.²⁰ Furthermore, in cloud computing, data integrity plays a crucial role by enabling centralized management, streamlined network event monitoring, improved traffic analysis and web filtering, and simplified disaster recovery planning. ACID (Atomicity, Consistency, Isolation, and Durability) transactions safeguard data integrity, while access to data is carefully regulated to prevent unauthorized use, theft, and misappropriation. However, access control solutions in cloud computing are more complex than traditional systems because of the need for more trust between cloud servers and users.²¹

Table 1 presents a comprehensive analysis and comparison of various scholarly articles, incorporating our own. The table systematically reviews these papers based on essential aspects of information security, such as privacy, data integrity, event management, frameworks, policies for countermeasures, solutions, and cryptography. A thorough examination of the table reveals that the reviewed papers emphasize particular aspects of information security. For instance, Sharma et al.,²⁸ Patel and Patel³⁰ emphasize incident management and countermeasure policies, emphasizing the fortification of data against unauthorized access and establishing effective incident response procedures. In contrast, Alkadi et al.²⁹ focuses on confidentiality and

cryptography to prevent the unauthorized disclosure of sensitive information. Our study distinguishes itself from other publications in several significant ways. Our research employs a comprehensive methodology that encompasses all of the evaluated factors. We place equal value on privacy, data integrity, incident management, and frameworks, among other factors. This all-encompassing perspective distinguishes our research in cloud computing systems. The comparison table is a valuable academic resource that equips practitioners and researchers in the field of information security risk assessment. It provides nuanced insights into the strengths and limitations of previous research endeavors, effectively identifying knowledge deficits and areas requiring additional study.

Various studies have addressed the constraints associated with only depending on frameworks for cloud security. Chauhan and Shialees⁴³ highlight the need to implement novel security rules and procedures to tackle the distinctive problems posed by cloud security effectively. Barraza de la Paz et al.⁴⁴ examine and contrast several frameworks for managing information security risks in cloud computing, emphasizing the need to adopt a complete strategy. Krishnan et al.⁴⁵ presents a model for designing and implementing cloud security architecture that is efficient and successful. Sun⁴⁶ analyses the protection of user data in cloud computing and suggests a methodical strategy for cloud service providers. These findings highlight the need of implementing a holistic approach to cloud security that goes beyond frameworks alone.

Our research aims to conduct a complete investigation of several facets of data security and privacy in the context of cloud computing. The aforementioned elements involve several facets such as flexibility, considerations pertaining to hardware and software, technological advancements, ensuring data integrity, a comprehensive

Table 1. Review comparison table.

Paper	Confidentiality	Data integrity	Incident management	Frameworks	Countermeasure	Policies	Solutions	Cryptography
Sharma et al. ²⁸	✗	✗	✓	✗	✓	✗	✗	✓
Alkadi et al. ²⁹	✓	✗	✗	✗	✗	✗	✗	✓
Patel and Patel ³⁰	✗	✓	✗	✗	✓	✗	✗	✓
Xie et al. ³¹	✓	✗	✗	✗	✗	✗	✗	✓
Gai et al. ³²	✗	✓	✓	✗	✓	✗	✗	✓
Pavithra et al. ³³	✗	✓	✗	✗	✗	✗	✗	✓
Memon et al. ³⁴	✗	✗	✗	✓	✗	✗	✗	✓
Murthy and Shri ³⁵	✗	✗	✓	✗	✓	✗	✗	✓
Xu et al. ³⁶	✓	✓	✗	✗	✓	✗	✗	✓
Prianga et al. ³⁷	✓	✗	✗	✗	✗	✗	✗	✓
Gill et al. ²²	✗	✗	✓	✓	✓	✗	✗	✓
Mohammadian et al. ³⁸	✗	✗	✗	✗	✗	✗	✗	✗
Isharufe et al. ³⁹	✗	✓	✗	✗	✓	✗	✗	✗
Shyam and Theja ⁴⁰	✗	✓	✗	✓	✗	✗	✓	✗
Panda et al. ⁴¹	✗	✗	✓	✓	✓	✗	✓	✗
Khoda Parast et al. ⁴²	✗	✗	✗	✗	✗	✗	✓	✗
Our study	✓	✓	✓	✓	✓	✓	✓	✓

Table 2. Contribution to the literature review.

Paper Title	References	Contribution
Security and Privacy Issues in Cloud Computing	Chen and Zhao ¹⁸	The paper examines data privacy and security in cloud computing, describing potential solutions to these problems and outlining directions for future research.
Data security and integrity in cloud computing	Aldossary and Allen ²⁰	The paper analyses issues and solutions related to data security in cloud storage. It also provides solutions for users sharing data with an untrustworthy cloud service provider, among other users, by focusing on data confidentiality, integrity, and availability (CIA) in the cloud.
Data security and integrity in cloud computing: Threats and Solutions	Sadavarte and Kurundkar ²⁴	This study conducts an investigation of data protection approaches and tactics in cloud computing, with a focus on ensuring optimum data security and integrity.
Machine learning classification of texture features of MRI	Hussain et al. ²⁵	The research investigates using MRI to predict treatment outcomes in breast cancer. The study reveals that the prediction accuracy significantly improves when early treatment data and molecular information are considered.
To Discovery The Cloud Services Authentication An Expert Based System Using Multi-Factor Authentication	Kumar et al. ²⁶	The paper explores methods to enhance cloud authentication for improved security, with a specific focus on advocating for the implementation of multi-factor authentication as a robust solution.
Cloud computing security: challenges and future trends	Radwan et al. ²⁷	The study assesses the cloud's primary security concerns, difficulties, and threats. Moreover, the article explores the discourse around security prerequisites for cloud deployment and delivery methods. Furthermore, it provides valuable insights into forthcoming trends and research prospects within cloud computing security.

classification of security risks at multiple levels, an analysis of security strategies, suggested solutions, and the maintenance of data integrity and security. Furthermore, we explore the obstacles and emerging patterns in the realm of cloud computing security. Cumulatively, our study offers vital insights and knowledge to the current corpus of literature, therefore facilitating future investigations and progress in this particular domain. Table 2 provides a concise overview of a range of scholarly publications, effectively delineating their respective contributions to the academic discipline.

Information security threat and attack landscape

The aim of managing information security in cloud computing is to safeguard the infrastructure, data, and applications.⁴⁷ 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.⁴⁷

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.⁴⁸ 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.⁴⁹ As previously demonstrated by Chen⁴⁹ 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).⁵⁰

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.⁵¹

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.⁵² 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.⁵³

Yu et al.⁵⁴ 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.

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

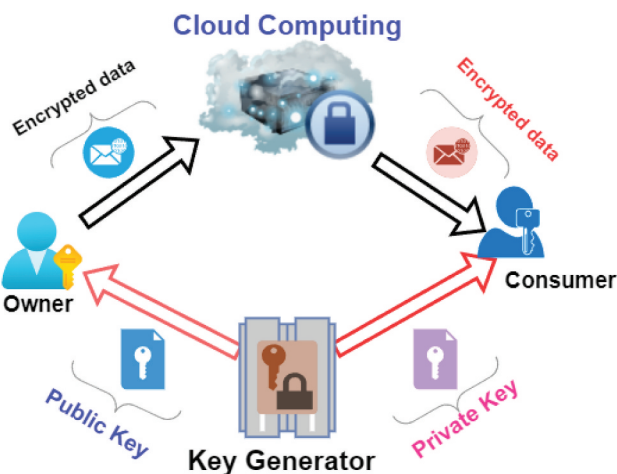


Figure 1. Cryptography techniques in cloud computing.

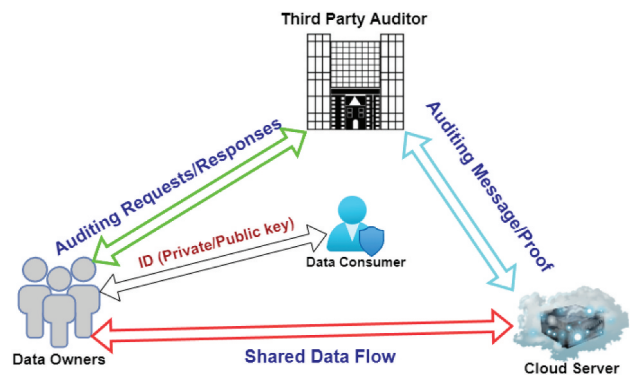


Figure 2. Remote data integrity checking (RDIC).

may violate data confidentiality, one of the three factors of information security management that must be controlled.⁵⁵ 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.⁵⁵ The solution presented in the study by More and Chaudhari,⁵⁶ 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.

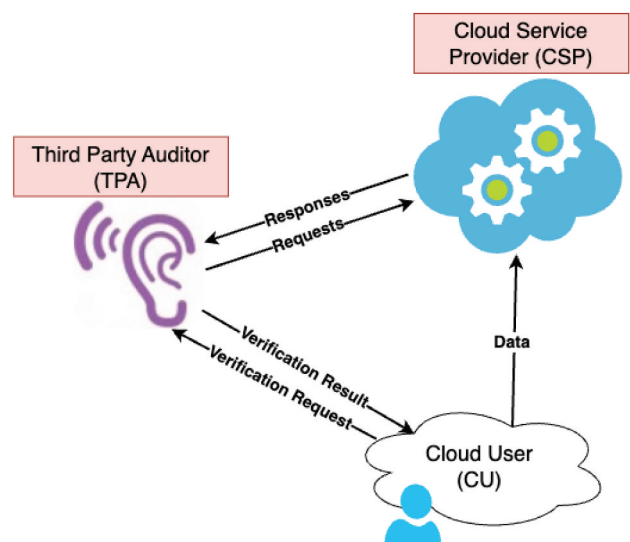


Figure 3. Third party auditor (TPA) signatures.

In contemporary times, many enterprise organizations have transitioned to cloud-based services, enabling them to offer a pay-as-you-go model.⁵⁷ 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.^{46,58} Kurosawa and Ohtaki⁵⁹ 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.^{27,60,61}

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.^{47,58} 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.^{47,58}

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.^{47,58} 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.⁶² 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.^{63–65} 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.²⁵

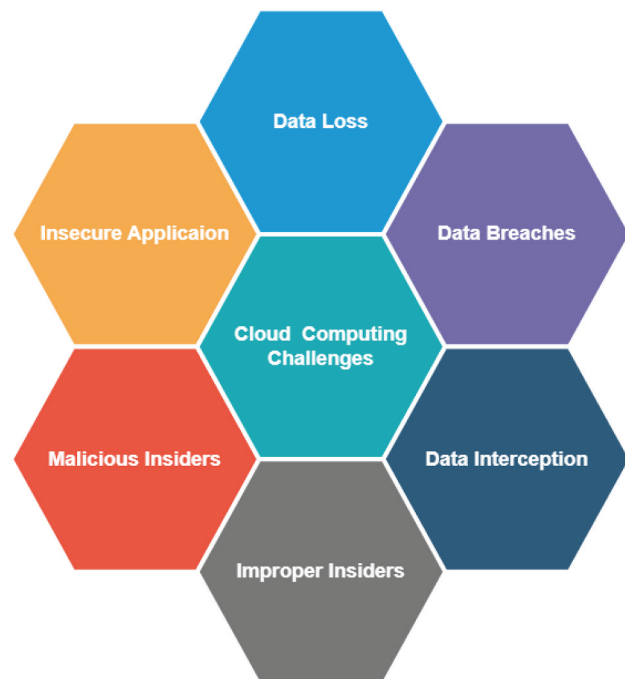


Figure 4. Cloud computing threats and attacks.

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.⁶⁶ Nevertheless, effective risk management frameworks must address the dynamic nature of changes. According to Petraşcu,⁶⁷ Risk management can be defined as identifying and assessing potential uncertainties that may result in adverse outcomes for an organization.⁶⁶

Furthermore, there exists a risk that may harm the feasibility of cloud services.⁶⁸ Hence, risk management refers to the actions undertaken to guide and oversee individuals and organizations.⁶⁹ 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.,⁷⁰ 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.¹⁵ 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.⁷¹ 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.⁷² The evaluation of hybrid methodologies and individual algorithms is also conducted to ascertain the optimal outcomes concerning fulfilling user specifications.⁷³ 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.⁷⁴ 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.¹⁵

The research conducted by Ismail and Islam⁷⁵ 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.⁷⁶ 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.⁷⁶ 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.⁷⁷ 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.⁷⁸

Examining the cloud security categories is essential for dealing with the possibility of prejudice or subjectivity in the evaluation procedure. Narang⁷² 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 Islam⁷⁵ 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.⁷⁹ 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.⁸⁰ 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.⁸¹ 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.⁸¹

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.⁸²

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.⁸³

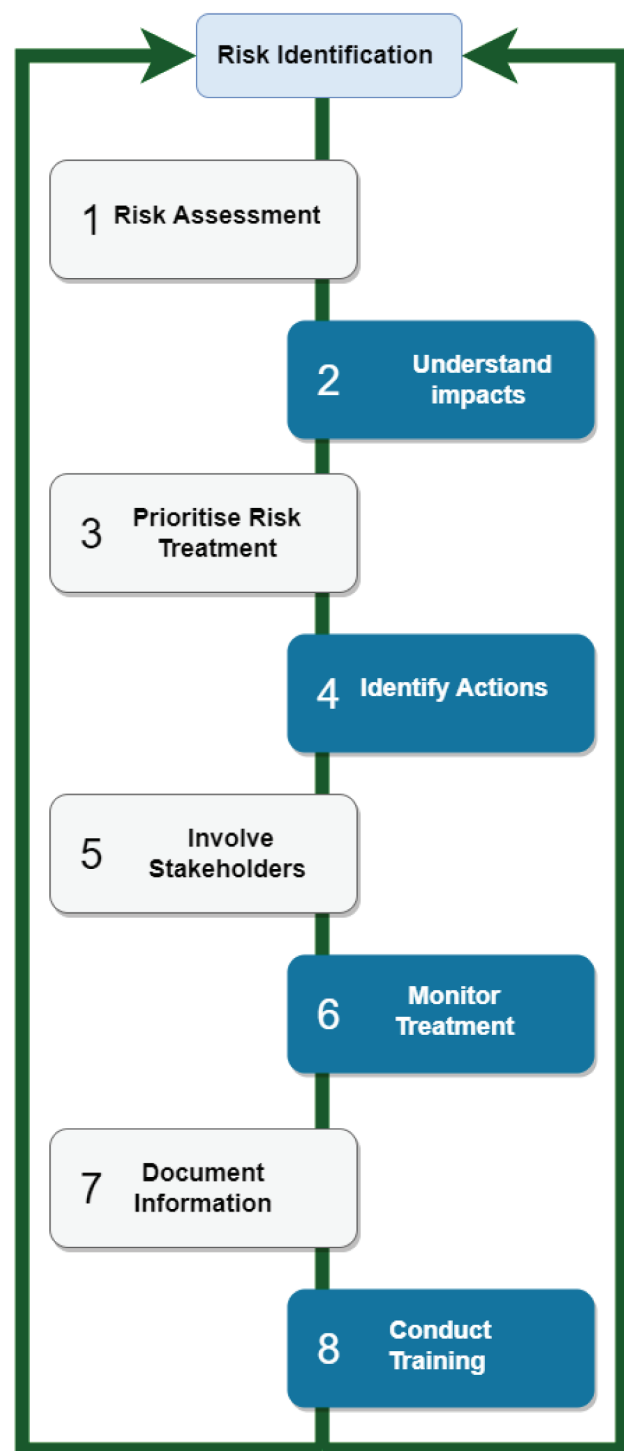


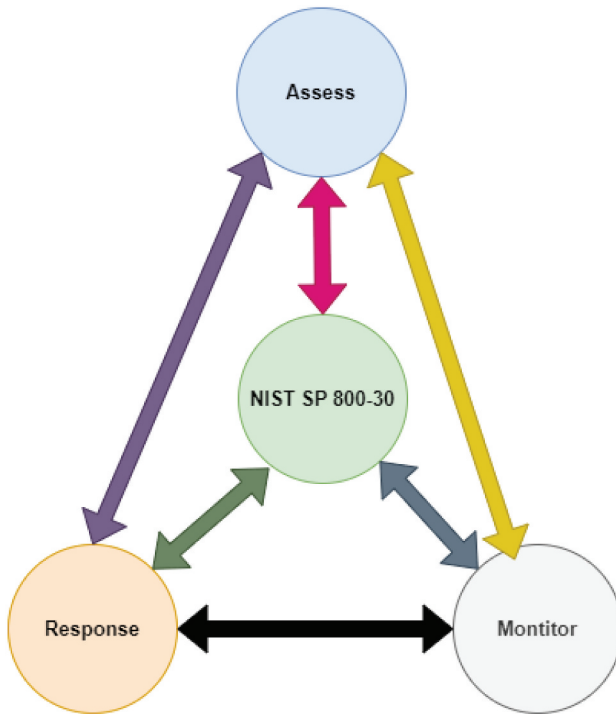
Figure 5. ISO27005 risk management process.

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

Table 3. ISO27005 risk management process.

Step	Description
1	Engage in an activity to identify potential risks.
2	Conduct a business-oriented risk assessment.
3	Gain insight into the potential consequences and impacts of the identified risk.
4	Prioritize the risk treatment approaches
5	Give priority to the actions aimed at minimizing the likelihood of risks.
6	Involve stakeholders in risk management decisions
7	Set up risk treatment monitoring and perform regular monitoring of the risk management procedure
8	Record all relevant information to enhance the risk management procedure.
9	Provide training to the organization's staff regarding the risks involved and the implemented measures to mitigate them.

**Figure 6.** NIST SP 800-30 risk management process.

on identifying possible threats and vulnerabilities that might put the safety of the systems at risk.⁸⁴ The OCTAVE model may be broken down into four distinct phases, each contributing to the overall execution of the process.^{85,86}

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.⁸⁷ 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.⁸⁷

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.⁸⁸ The methodology consists of three distinct stages.

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.⁸⁹ To describe the CORAS method using the Unified Modeling Language (UML), a graphical language is utilized that employs diagrams to illustrate the

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

Phase	Description
1	Conducting a risk framing exercise to establish a risk management strategy.
2	Conduct a risk assessment to identify threats, vulnerabilities, potential harm, and likelihood of occurrence.
3	Develop an action plan to respond to the identified risks and implement the response based on prioritized actions.
4	Perform ongoing risk monitoring activities to track changes in the organization's risk profile and ensure all necessary actions are implemented effectively.

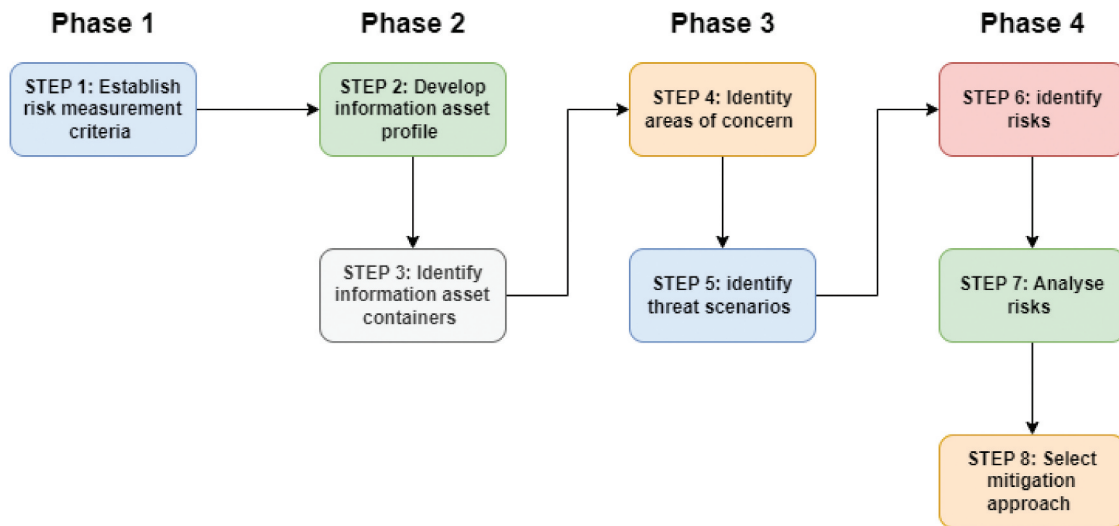


Figure 7. OCTAVE model stages and steps.

Table 5. OCTAVE model stages and steps.

Phase	Description
ONE	Step 1: Establish a risk measurement criterion and utilize a ranking system to evaluate and quantify the level of the impact associated with risks.
TWO	Step 2: Create an information asset profile as part of the process.
THREE	Step 3: Evaluate the information systems infrastructure in order to prioritize critical components, both internal and external, as well as key assets and resources such as software, hardware, networks, and personnel.
THREE	Step 4: Employ brainstorming methods to identify areas of concern associated with risks.
THREE	Step 5: Identify potential risks, evaluate their likelihood of occurrence, and analyze the potential impact they may have in order to proactively prepare for threat scenarios.
FOUR	Step 6: Identify risks.
FOUR	Step 7: Establish a risk analysis.
FOUR	Step 8: Measure the impact of risks and create a mitigation plan.

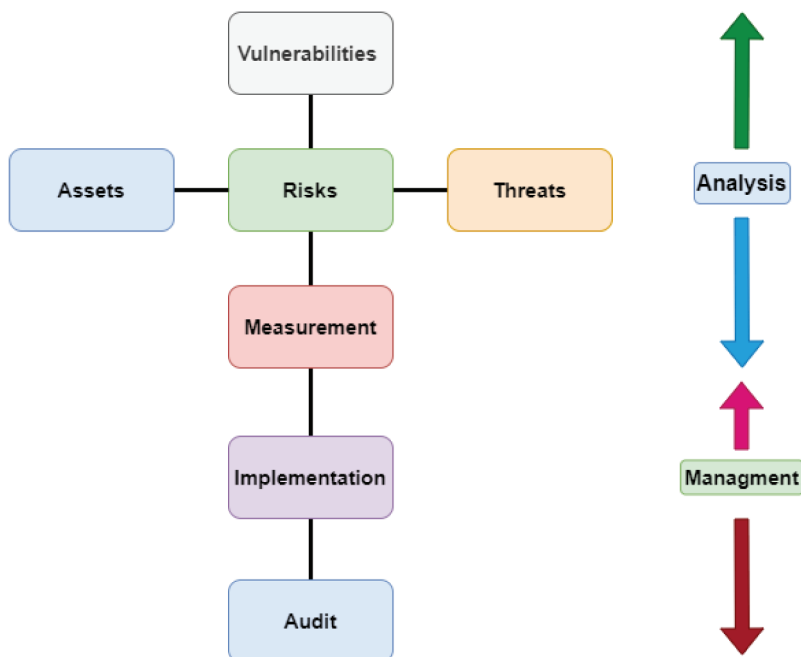
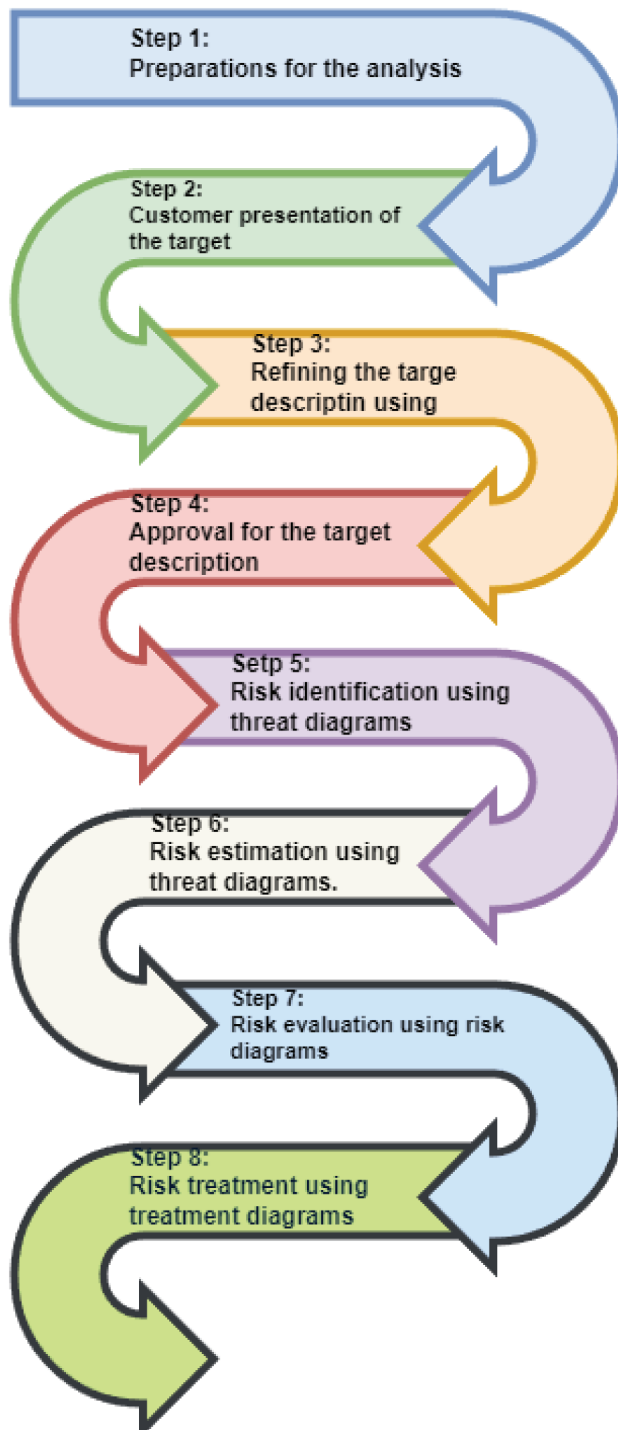


Figure 8. CRAMM model stages and steps.

Table 6. Phases of the CRAMM methodology.

Phase	Description
1	In this initial phase, the organization performs an assessment to identify assets and evaluate their value.
2	During this phase, the team evaluates threats to the system by analyzing their nature and potential impact. The vulnerabilities are also examined to determine their degree of risk.
3	The final phase involves selecting an appropriate mitigation strategy based on the risks identified in phase two. Recommendations are made to help the organization address the identified risks.

**Figure 9.** CORAS model stages and steps.

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.⁹⁰

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.⁹¹

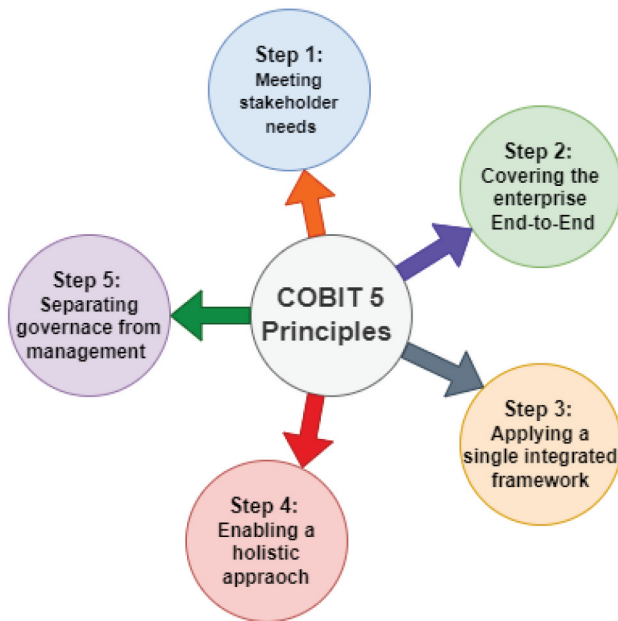
The suitability of different security models, developed and deployed across different domains, relies on the understanding of the organization's business objectives and risk management framework. After assessing the levels of risk that are deemed acceptable, organizations can pick the risk management 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.^{92–96}

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

Table 7. CORAS model stages and steps.

Step	Description
1	The first step involves defining the primary objective and scope of the analysis to be undertaken.
2	During the subsequent phase, it is necessary to engage with customers to gain insight into their analysis needs and requirements, and to establish a shared understanding.
3	The third step aims to ensure that there is mutual agreement on the focus, scope, and organizational assets for the analysis.
4	Step four involves documenting the analysis, including setting the target, focus, and objectives.
5	The next step is to identify risks through brainstorming, walkthroughs, and workshops with relevant individuals.
6	Step six involves determining the level of risk and estimating its impact based on the previous step.
7	The organization then decides which risks to accept and which require further treatment.
8	The final step is to identify and evaluate potential treatments for the identified risks.

**Figure 10.** COBIT 5 model stages and steps.

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.

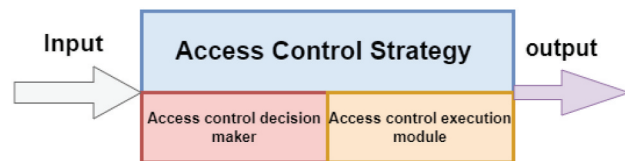
Strategic Information Security Culture Identification for Cloud Computing: Extensive research was conducted to identify the most pertinent strategic information security culture. The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a recognized approach for addressing cybersecurity risks, including those related to cloud computing. The NIST framework emphasizes five fundamental functions: Identity, Protect, Detect, Respond, and Recover.⁹⁷

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.^{98,99} Most of the research in cloud computing security is primarily concerned with safeguarding data privacy,¹⁰⁰ the utilization of ciphertext for data retrieval and possession of evidence,¹⁰⁰ and access control,¹⁰¹ which is essential for preventing unauthorized access to confidential data.

Access control is crucial to safeguard cloud-stored data and has undergone extensive research. Belguith et al.¹⁰² 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),¹⁰³ which provides complete access authorization to the

**Figure 11.** Access control model.**Table 8.** COBIT 5 rules.

Rule	Description
1	Transform stakeholder needs into practical goals.
2	Encompass the entire enterprise and seamlessly integrate IT and business functionalities.
3	Implement a unified and integrated framework that aligns with various other standards.
4	Enable a holistic approach for managing IT and information assets.
5	Decouple governance from operational management.

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),¹⁰⁴ the system is designed to meet the confidentiality requirements of the information by implementing the Role-Based Access Control (RBAC) mechanism,^{105,106} 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.¹⁰⁷ Attribute access control is a technique of access management that is built on attribute encryption.¹⁰⁸

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.⁷⁰ Data protection policies in cloud computing place significant importance on encryption.¹⁰⁹ 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.¹¹⁰ 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.¹¹¹ 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.¹¹² 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](#).

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.¹¹³ 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.¹¹⁴ 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.¹¹⁴ 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.¹¹⁴ 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.

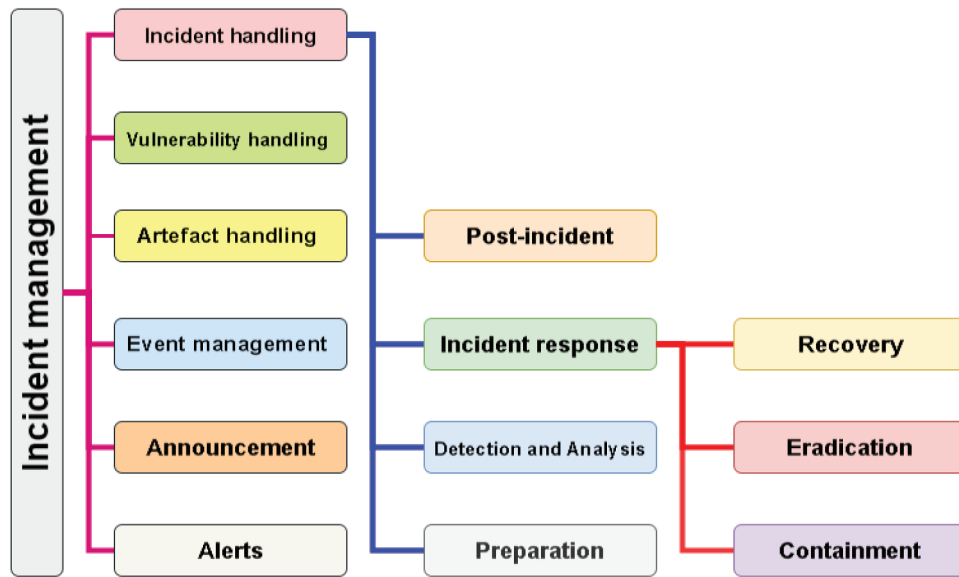


Figure 12. Incident management.

- 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.¹¹⁵ It has been demonstrated through research carried out by Luo et al.,¹¹⁶ Anwar et al.¹¹⁷ that AIRS is effective in reducing the time between detection and response. This leads to the genuine case of complex and multi-stage attacks, significantly improving incident response rates.

Implement policies effectively

There are various phases of cloud interactions where risk analysis can be conducted.¹¹⁸ 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.¹¹⁸ 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,⁴³ 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 Islam⁷⁵ 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 Shiaeles⁴³ 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 Islam⁷⁵ 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.¹¹⁹ 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.,⁷⁹ 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 Shiaeles⁴³ 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.¹¹⁸

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.¹⁵ Therefore, a reliable Risk management strategy and models are required to safeguard vital data assets.¹²⁰ 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.¹²⁰ The second step is mitigating those dangers once they have been discovered. El Fray¹²¹ 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,



Figure 13. Implement and manage policies.

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.¹⁵

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.¹²²

Dynamic mapping

The dynamic mapping model is a method for selecting response strategies according to incident context.¹¹⁵ 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.¹²²

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.¹²² 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.¹²³

Post-incident

The phase that follows the resolution of an incident is known as the post-incident phase.¹²² 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.¹²⁴

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.¹²⁵ According to Ab Rahman and Choo,¹²² 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.¹²⁴ *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 Choo¹²² in their work, as shown in Figure 14. This information is typically documented in a report.¹²⁶ Additionally, this stage involves presenting formal reports to higher-level management and suggesting enhancements to incident handling, considering both technical and managerial aspects. Taylor¹²⁶ implies that conducting research on generic information content and templates would be beneficial in generating a comprehensive and informative report, particularly

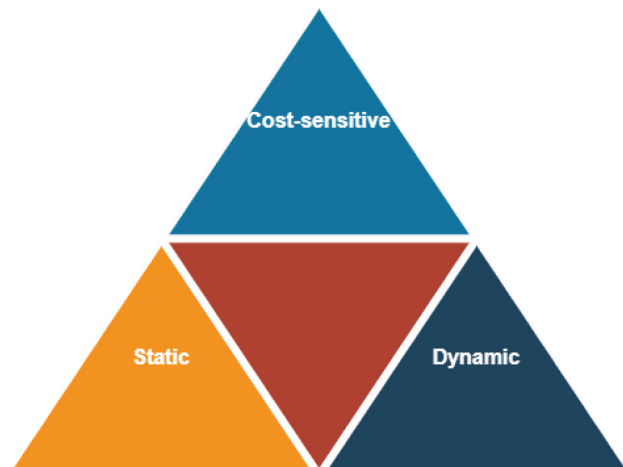


Figure 14. Three response models.

when the report is intended for utilization by law enforcement agencies or in a courtroom setting.¹²²

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.

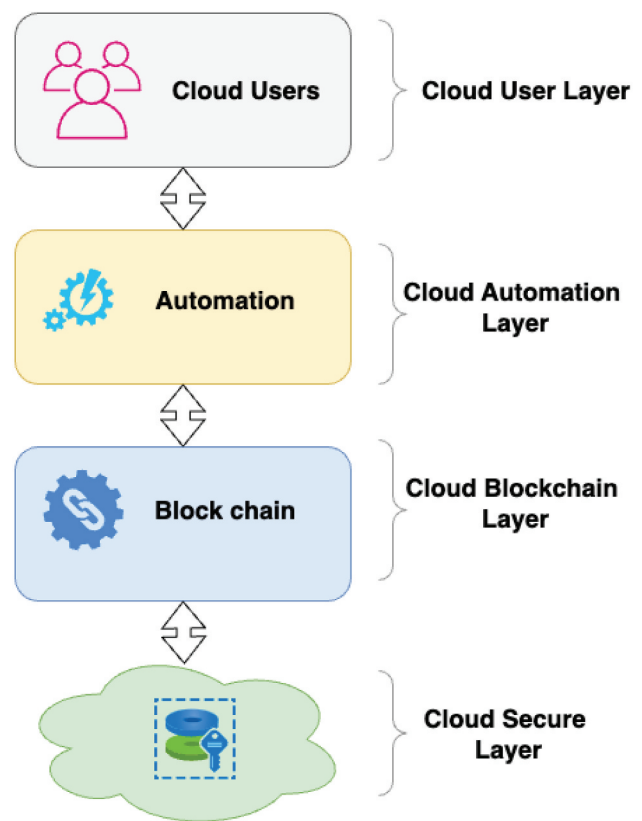


Figure 15. Secure encryption-based cloud framework.

Table 10 demonstrates an evaluation of the encryption's strengths, shortcomings, and prospective consequences. For instance, Butt et al.¹²⁷ highlights the importance of encryption in cloud computing as it helps protect data from unauthorized access. Pavithran et al.¹²⁸ 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.²⁹ 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 Joseph¹²⁹'s proposal for blockchain as a solution for cloud security and storage.

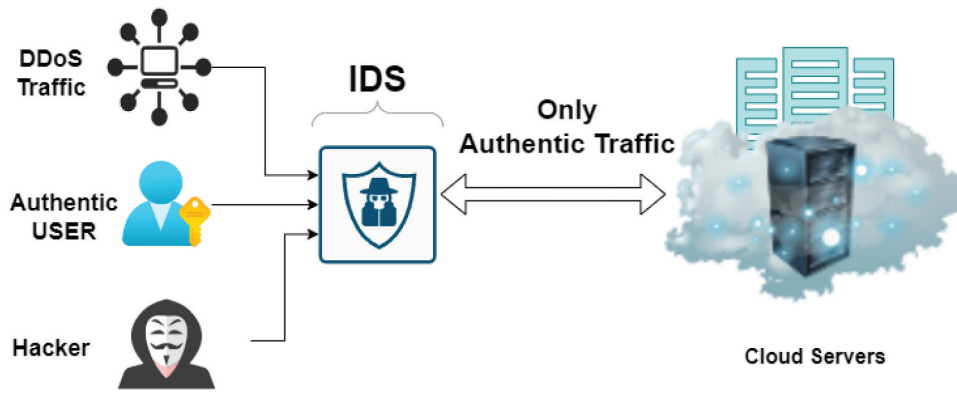


Figure 16. Intrusion detection architecture.

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.¹³⁰ 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,¹³¹ 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.¹³² 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.^{133,134} 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.,¹³⁵ 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.¹³⁶

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

Table 9. Number of reiteration cycles for different key sizes in AES²⁶.

Key Size in bits	Number of Reiteration Cycles
128	10
192	12
256	14

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.²⁶

Intrusion detection

According to Nadeem et al.¹³⁷ 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.¹³⁸ Implementing IDPS in cloud computing environments can significantly improve overall security and prevent various security incidents, as pointed out by.¹³⁸ Therefore, IDPS is considered a critical security strategy for cloud computing.

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.,¹³⁹ 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.¹⁴⁰ 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.¹⁴¹ developed an architecture implemented on a practical utility called snort. An automatic host-based methodology was suggested by Gassais et al.¹⁴² that uses machine learning techniques to identify intrusions coming from smart devices. Mazini et al.¹⁴³ 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.¹⁴⁴ went through several articles and discussed how DOS attacks could occur on cloud platforms, webpages, levels of the OSI model, and other places.

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.¹⁴⁵ 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.¹⁴⁵ Costante et al.¹⁴⁶ introduced

Table 10. Technical security controls critical assessment.

Methods	Strengths	Weaknesses	Potential Impacts
Encryption	Offers a strong level of safeguarding for data while it is stored and during its transfer.	Key management can be challenging, especially for large organizations with complex encryption requirements.	Encryption can enhance the reputation of cloud providers by demonstrating their commitment to security and data privacy.
	Encryption is selective, allowing organizations to protect only their most sensitive data.	Encryption can impact performance, especially for data-intensive applications.	Encryption can increase customer trust by providing an additional layer of protection for sensitive data.
	Encryption is a widely used and accepted security control in the cloud.		The cost of implementing encryption may impact the finances of smaller organizations, but it can be an important investment for larger organizations that handle significant amounts of sensitive data.
Access Control	Restricts access to sensitive resources.	Can be complex to implement and maintain.	Effective access control can significantly improve data security and prevent unauthorized access to sensitive resources.
	Can be implemented using various mechanisms such as RBAC, ABAC, and MAC. RBAC can simplify access management.	Requires careful management of user identities, roles, and privileges.	Weak access control can result in data breaches, loss of sensitive information, and compromise of critical systems.
		If access controls are misconfigured, sensitive data may become vulnerable.	Complex access control mechanisms can be challenging to implement and maintain, leading to errors and misconfigurations that can compromise security.
Multi-Factor Authentication	Requires multiple authentication factors for access, providing an additional layer of security.	Can increase complexity for users and IT administrators, potentially leading to confusion and errors.	Can cause inconvenience for users, especially when MFA is required frequently or when using certain devices or locations.
	Reduces the risk of unauthorized access due to compromised passwords or single-factor authentication methods.	May not be foolproof, as attackers may be able to bypass MFA using social engineering techniques or other means.	Can be subject to false positives or false negatives, leading to legitimate users being denied access or unauthorized users being granted access.
	Can be implemented using various mechanisms such as OTP, smart cards, and biometric authentication, allowing for flexibility and customization.	Can increase processing overhead, potentially leading to slower system performance or increased costs.	Can require additional resources and time for implementation and maintenance.
Intrusion Detection	Can improve compliance with security regulations and standards.		Can create compatibility issues with certain systems or devices, requiring additional modifications or upgrades to the infrastructure.
	Monitors network traffic and detects/prevents unauthorized access and other security incidents.	Can generate false positives or false negatives, leading to ineffective security measures.	Increased security: IDPS can significantly increase the security posture of cloud computing environments by detecting and preventing unauthorized access and other security incidents. This can help prevent data breaches and other types of cyber attacks.
	Either host-based or network-based, and it may use signature-based or behavior-based techniques.	May not be able to detect sophisticated or zero-day attacks.	Decreased productivity: False positives or false negatives generated by IDPS can lead to ineffective security measures, causing legitimate traffic to be blocked. This can negatively impact productivity and cause frustration for users.
Data Loss Prevention	Can significantly increase the security posture of cloud computing environments.	Can increase processing overhead.	Missed threats: IDPS may not be able to detect sophisticated or zero-day attacks, leaving the network vulnerable to advanced threats such as malware and APTs.
			Increased costs: The implementation and maintenance of IDPS can be costly, especially for large-scale cloud computing environments. Additionally, the processing overhead required by IDPS can require additional hardware or resources, further increasing costs.
	Monitors data flow and prevents data leakage, unauthorized access, and data loss	Can be complex to configure and maintain	Can significantly increase the security posture of cloud computing environments
	Can be network-based or host-based	Can increase processing overhead	May generate false positives or false negatives, leading to ineffective security measures DLP policies may cause delays or disruptions in normal business operations

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.¹⁴⁷ suggested yet another method for preventing data loss, but it cannot safeguard pictures. Ong et al.¹⁴⁸ 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,¹⁴⁹ and Gartner has approved this technology. To protect vital information, it functions by utilizing proxy servers developed by various cybersecurity companies such as CipherCloud.¹⁵⁰ 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,¹⁵¹ that encrypts textual data in preexisting cloud services. However, it cannot handle data items such as binary files or picture files. Mimesis Aegis¹⁵² offers confidential data separation via a conceptual layer for mobile apps but does not offer data file security. CryptDB¹⁵³ 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.¹⁵⁴ 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. Virtru¹⁵⁵ 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,¹⁵⁶ 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.

Disclosure statement

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

References

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. Szalay M, Mátray P, Toka L. State management for cloud-native applications. *Electronics*. 2021;10(4):423. doi:10.3390/electronics10040423.
8. 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.
9. 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.
10. 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.
11. Abomhara M, Yang H. Collaborative and secure sharing of healthcare records using attribute-based authenticated access. *Int J Adv Secur*. 2016;9(3).
12. Tariq MI. Agent based information security framework for hybrid cloud computing. *KSII Trans Int Inf Syst*. 2019;13:406–34.
13. 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.
14. Tian J. Quantitative assessment method of multi-node network security situation based on threat propagation. *Comput Res Dev*. 2017;54:731–41.
15. 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.
16. 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.
17. 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.
18. 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.
19. Abdul-Jabbar SS, Aldujaili A, Mohammed SG, Saeed HS. Integrity and security in cloud computing environment: a review. *J Southwest Jiaotong Univ*. 2020;55(1). doi:10.35741/issn.0258-2724.55.1.11.
20. Aldossary S, Allen W. Data security, privacy, availability and integrity in cloud computing: issues and current solutions. *Int J Adv Comput Sci Appl*. 2016;7(4). doi:10.14569/IJACSA.2016.070464.
21. Pai TV, Aithal PS. Cloud computing security issues-challenges and opportunities. *Int J Manage Technol Social Sci*. 2017;1(1):33–42. doi:10.47992/IJMTS.2581.6012.0004.
22. Gill S, Abdur Razzaq M, Ahmad M, Almansour F, Ul Haq I, Jhanjhi N, Zaib M, Masud M. Security and privacy aspects of cloud computing: a smart campus

- case study. *Intell Autom Soft Comput.* **2021**;31(1):117–28. doi:[10.32604/iasc.2022.016597](https://doi.org/10.32604/iasc.2022.016597).
23. Alrasheed SH, Aied Alhariri M, Adubaykhi SA, El Khediri S. Cloud computing security and challenges: issues, threats, and solutions. In: *2022 5th Conference on Cloud and Internet of Things (CIoT)*; **2022** Mar. p. 166–72.
 24. Sadavarte RK, Kurundkar GD. Data security and integrity in cloud computing: threats and solutions. *IJSRCSEIT.* **2020**;356–63. doi:[10.32628/CSEIT206667](https://doi.org/10.32628/CSEIT206667).
 25. Hussain L, Huang P, Nguyen TB, Lone KJ, Ali A, Khan MS, Li H, Suh DY, Duong TQ. Machine learning classification of texture features of MRI breast tumor and peri-tumor of combined pre- and early treatment predicts pathologic complete response. *Biomed Eng Online.* **2021**;20(1). doi:[10.1186/s12938-021-00899-z](https://doi.org/10.1186/s12938-021-00899-z).
 26. Kumar GS, Kandavel N, Madhavan K. To discovery the cloud services authentication an expert based system using multi-factor authentication. In: *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*; **2020** Mar. p. 1014–16.
 27. Radwan T, Azer MA, Abdelbaki N. Cloud computing security: challenges and future trends. *Int J Comput Appl Technol.* **2017**;55(2):158–72. doi:[10.1504/IJCAT.2017.082865](https://doi.org/10.1504/IJCAT.2017.082865).
 28. Sharma P, Jindal R, Borah MD. Blockchain technology for cloud storage: a systematic literature review. *ACM Comput Surv.* **2020**;53(4):89:1–32. doi:[10.1145/3403954](https://doi.org/10.1145/3403954).
 29. Alkadi O, Moustafa N, Turnbull B. A review of intrusion detection and blockchain applications in the cloud: approaches, challenges and solutions. *IEEE Access.* **2020**;8:104893–917. doi:[10.1109/ACCESS.2020.2999715](https://doi.org/10.1109/ACCESS.2020.2999715).
 30. Patel P, Patel H. Review of blockchain technology to address various security issues in cloud computing. In: Kotecha K, Piuri V, Shah H Patel R, editors. *Data science and intelligent applications*. Singapore: Springer; **2021**. p. 345–54. *Lecture Notes on Data Engineering and Communications Technologies*.
 31. Xie S, Zheng Z, Chen W, Wu J, Dai HN, Imran M. Blockchain for cloud exchange: a survey. *Comput Electr Eng.* **2020**;81:106526. doi:[10.1016/j.compeleceng.2019.106526](https://doi.org/10.1016/j.compeleceng.2019.106526).
 32. Gai K, Guo J, Zhu L, Yu S. Blockchain meets cloud computing: a survey. *IEEE Commun Surv Tut.* **2020**;22(3):2009–30. doi:[10.1109/COMST.2020.2989392](https://doi.org/10.1109/COMST.2020.2989392).
 33. Pavithra S, Ramya S, Prathibha S. A survey on cloud security issues and blockchain. In: *2019 3rd International Conference on Computing and Communications Technologies (ICCCT)*; **2019** Feb. p. 136–40.
 34. Memon R, Li J, Ahmed J, Nazeer I, Mangrio MI, Ali K. Cloud-based vs. Blockchain-based IoT: a comparative survey and way forward. *Front Inform Technol Electron Eng.* **2020**;21(4):563–86. doi:[10.1631/FITEE.1800343](https://doi.org/10.1631/FITEE.1800343).
 35. Murthy CB, Shri ML. A survey on integrating cloud computing with Blockchain. In: *2020 International Conference on Emerging Trends in Information Technology and Engineering (Ic-ETITE)*; **2020** Feb. p. 1–6.
 36. Xu H, Cao J, Zhang J, Gong L, Gu Z. A survey: cloud data security based on blockchain technology. In: *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)*; **2019** Jun. p. 618–24.
 37. Prianga S, Sagana R, Sharon E. Evolutionary survey on data security in cloud computing using blockchain. In: *2018 IEEE International Conference on System, Computation, Automation and Networking (ICSCA)*; **2018** Jul. p. 1–6.
 38. Mohammadian V, Navimipour NJ, Hosseinzadeh M, Darwesh A. Comprehensive and systematic study on the fault tolerance architectures in cloud computing. *J Circuits Syst Comput.* **2020**;29(15):2050240. doi:[10.1142/S0218126620502400](https://doi.org/10.1142/S0218126620502400).
 39. Isharufe W, Jaafar F, Butakov S. Study of security issues in platform-as-a-service (paas) cloud model. In: *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*. IEEE; **2020**. p. 1–6.
 40. Shyam GK, Theja RSS. A survey on resolving security issues in SaaS through software defined networks. *Int J Grid Util Comput.* **2021**;12(1):1–14. doi:[10.1504/IJGUC.2021.112475](https://doi.org/10.1504/IJGUC.2021.112475).
 41. Panda DR, Behera SK, Jena D. A survey on cloud computing security issues, attacks and countermeasures. In: *Advances in Machine Learning and Computational Intelligence: Proceedings of ICMLCI 2019*. Springer; **2021**. p. 513–24.
 42. Khoda Parast F, Sindhav C, Nikam S, Izadi Yekta H, Kent KB, Hakak S. Cloud computing security: a survey of service-based models. *Comput Secur.* **2022**;114:102580. doi:[10.1016/j.cose.2021.102580](https://doi.org/10.1016/j.cose.2021.102580).
 43. Chauhan M, Shiaeles S. An analysis of cloud security frameworks, problems and proposed solutions. *Network.* **2023**;3(3):422–50. doi:[10.3390/network3030018](https://doi.org/10.3390/network3030018).
 44. Barraza de la Paz JV, Rodríguez-Picón LA, Morales-Rocha V, Torres-Argüelles SV. A systematic review of risk management methodologies for complex organizations in industry 4.0 and 5.0. *Systems.* **2023**;11(5):218. doi:[10.3390/systems11050218](https://doi.org/10.3390/systems11050218).
 45. Krishnan P, Jain K, Aldweesh A, Prabu P, Buyya R. OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure. *J Cloud Comp.* **2023**;12(1):26. doi:[10.1186/s13677-023-00406-w](https://doi.org/10.1186/s13677-023-00406-w).
 46. Sun P. Security and privacy protection in cloud computing: discussions and challenges. *J Netw Comput Appl.* **2020**;160:102642. doi:[10.1016/j.jnca.2020.102642](https://doi.org/10.1016/j.jnca.2020.102642).
 47. Hasan MZ, Hussain MZ, Mubarak Z, Siddiqui AA, Qureshi AM, Ismail I. Data security and integrity in cloud computing. In: *2023 International Conference for Advancement in Technology (ICONAT)*; **2023** Jan. *2023 International Conference for Advancement in Technology (ICONAT)*. p. 1–5.
 48. Ali O, Shrestha A, Ghasemaghahi M, Beydoun G. Assessment of complexity in cloud computing adoption: a case study of local governments in Australia. *Inf Syst Front.* **2021**;24(2):595–617. doi:[10.1007/s10796-021-10108-w](https://doi.org/10.1007/s10796-021-10108-w).

49. Chen L. Using algebraic signatures to check data possession in cloud storage. *Future Gener Comput Syst.* **2013**;29(7):1709–15. doi:[10.1016/j.future.2012.01.004](https://doi.org/10.1016/j.future.2012.01.004).
50. Zhang Y, Zhang H, Hao R, Yu J. Authorized identity-based public cloud storage auditing scheme with hierarchical structure for large-scale user groups. *China Commun.* **2018**;15(11):111–21. doi:[10.1109/CC.2018.8543053](https://doi.org/10.1109/CC.2018.8543053).
51. Indhumathil T, Aarthy N, Devi VD, Samyuktha VN. Third-party auditing for cloud service providers in multicloud environment. In: 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM); **2017** Mar. p. 347–52.
52. Ma H, Zhang R, Yang G, Song Z, He K, Xiao Y. Efficient fine-grained data sharing mechanism for electronic medical record systems with mobile devices. *IEEE Trans Depend Secure Comput.* **2020**;17(5):1026–38. doi:[10.1109/TDSC.2018.2844814](https://doi.org/10.1109/TDSC.2018.2844814).
53. Verma V, Kumar P, Verma RK, Priya S. A novel approach for security in cloud data storage using AES-DES-RSA hybrid cryptography. Raigarh, India: *Emerging Trends in Industry 4.0 (ETI 4.0)*; **2021**. p. 1–6. doi:[10.1109/ETI4.051663.2021.9619274](https://doi.org/10.1109/ETI4.051663.2021.9619274).
54. Yu Y, Au MH, Ateniese G, Huang X, Susilo W, Dai Y, Min G. Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. *IEEE Trans Info Forensic Secur.* **2017**;12(4):767–78. doi:[10.1109/TIFS.2016.2615853](https://doi.org/10.1109/TIFS.2016.2615853).
55. Mohanty S, Pattnaik PK, Kumar R. Confidentiality preserving auditing for cloud computing environment. In: 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE); **2018** Aug. San Salvador: IEEE. p. 1–4.
56. More S, Chaudhari S. Third party public auditing scheme for cloud storage. *Procedia Comput Sci.* **2016**;79:69–76. doi:[10.1016/j.procs.2016.03.010](https://doi.org/10.1016/j.procs.2016.03.010).
57. Charanya R, Aramudhan M, Mohan K, Nithya S. Levels of security issues in cloud computing. *Int J Eng Technol.* **2013**;5(2).
58. Beek C, Dinkar D, Gund Y, Lancioni G, Minihihane N, Moreno F, Peterson E, Roccia T, Schmugar C, Simon R. McAfee labs threats report. Santa Clara (CA): McAfee; **2017**.
59. Kurosawa K, Ohtaki Y. How to update documents verifiably in searchable symmetric encryption. In: Hutchison D, Kanade T, Kittler J, Kleinberg J, Mattern F, Mitchell J, Naor M, Nierstrasz O, Pandu Rangan C, Steffen B, et al., editors. *Cryptology and network security*. Vol. 8257. Cham: Springer International Publishing; **2013**. p. 309–28.
60. Khalil IM, Khreishah A, Azeem M. Cloud computing security: a survey. *Computers.* **2014**;3(1):1–35. doi:[10.3390/computers3010001](https://doi.org/10.3390/computers3010001).
61. Stergiou C, Psannis KE, Gupta BB, Ishibashi Y. Security, privacy & efficiency of sustainable cloud computing for big data & IoT. *Sustain Comput.* **2018**;19:174–84. doi:[10.1016/j.suscom.2018.06.003](https://doi.org/10.1016/j.suscom.2018.06.003).
62. Al-Hashimi MT, Alkhuwayldeh AR, Al-Nidawi WJ, Al-Wassiti SK. Evaluating information security governance frameworks in cloud computing environments using the analytic hierarchy process (AHP). *NeuroQuantology.* **2022**;20:7682.
63. Sattar H, Bajwa IS, Amin RU, Sarwar N, Jamil N, Malik MA, Mahmood A, Shafi U. An IoT-based intelligent wound monitoring system. *IEEE Access.* **2019**;7:144500–15. doi:[10.1109/ACCESS.2019.2940622](https://doi.org/10.1109/ACCESS.2019.2940622).
64. Hameed K, Bajwa IS, Sarwar N, Anwar W, Mushtaq Z, Rashid T. Integration of 5G and block-chain technologies in smart telemedicine using IoT. *J Healthc Eng.* **2021**;2021:1–18. doi:[10.1155/2021/8814364](https://doi.org/10.1155/2021/8814364).
65. Rafique W, Khan M, Sarwar N, Dou W. A security framework to protect edge supported software defined internet of things infrastructure. In: *Collaborative Computing: Networking, Applications and Worksharing: 15th EAI International Conference, CollaborateCom 2019, London, UK, August 19–22, 2019, Proceedings 15*. Springer; **2019**. p. 71–88.
66. Weil T. Standards for cloud risk assessments—what’s missing? *IT Prof.* **2020**;22(6):16–23. doi:[10.1109/MITP.2019.2949361](https://doi.org/10.1109/MITP.2019.2949361).
67. Petraşcu D, Tamaş, A. Internal audit versus internal control and coaching. *Procedia Econ Financ.* **2013**;6(3):694–702. doi:[10.1016/s2212-5671\(13\)00191-3](https://doi.org/10.1016/s2212-5671(13)00191-3).
68. Drăgoi AM. Research regarding the risks in the audit mission of computerised systems. *Audit Financiar.* **2015**;13(124):72.
69. International Organization for Standardization. ISO 31000: risk management: principles and guidelines. 1st ed. Geneva: ISO; **2009**. p. 11–15.
70. Singh S, Jeong YS, Park JH. A survey on cloud computing security: issues, threats, and solutions. *J Netw Comput Appl.* **2016**;75:200–22. doi:[10.1016/j.jnca.2016.09.002](https://doi.org/10.1016/j.jnca.2016.09.002).
71. Krishnamoorthy N, Umarani S. Implementation and management of cloud security for industry 4.0 - data using hybrid elliptical curve cryptography. *J High Technol Manage Res.* **2023**;34(2):100474. doi:[10.1016/j.hitech.2023.100474](https://doi.org/10.1016/j.hitech.2023.100474).
72. Narang A. Analysis of frameworks in cloud environment. *IJIRCST.* **2020**;8(3). doi:[10.21276/ijircst.2020.8.3.38](https://doi.org/10.21276/ijircst.2020.8.3.38).
73. Fu X, Sun Y, Wang H, Li H. Task scheduling of cloud computing based on hybrid particle swarm algorithm and genetic algorithm. *Cluster Comput.* **2023**;26(5):2479–88. doi:[10.1007/s10586-020-03221-z](https://doi.org/10.1007/s10586-020-03221-z).
74. Ali M, Jung LT, Sodhro AH, Laghari AA, Belhaouari SB, Gillani Z. A Confidentiality-based data classification-as-a-service (C2aaS) for cloud security. *Alexandria Eng J.* **2023**;64:749–60. doi:[10.1016/j.aej.2022.10.056](https://doi.org/10.1016/j.aej.2022.10.056).
75. Ismail UM, Islam S. A unified framework for cloud security transparency and audit. *J Inf Secur Appl.* **2020**;54:102594. doi:[10.1016/j.jisa.2020.102594](https://doi.org/10.1016/j.jisa.2020.102594).
76. Sampson D, Chowdhury MM. The growing security concerns of cloud computing. In: 2021 IEEE International Conference on Electro Information Technology (EIT). IEEE; **2021**. p. 050–055.
77. Nieuwenhuis LJ, Ehrenhard ML, Prause L. The shift to cloud computing: the impact of disruptive technology on the enterprise software business ecosystem. *Technol Forecast Soc.* **2018**;129:308–13. doi:[10.1016/j.techfore.2017.09.037](https://doi.org/10.1016/j.techfore.2017.09.037).
78. El Mhouthi A, Erradi M, Nasseh A. Using cloud computing services in e-learning process: benefits and

- challenges. *Educ Inf Technol (Dordr)*. 2018;23 (2):893–909. doi:10.1007/s10639-017-9642-x.
79. Jamshidi P, Ahmad A, Pahl C. Cloud migration research: a systematic review. *IEEE Trans Cloud Comput*. 2013;1(2):142–57. doi:10.1109/TCC.2013.10.
 80. Pendleton M, Garcia-Lebron R, Cho JH, Xu S. A survey on systems security metrics. *ACM Comput Surv*. 2016;49(4):62:1–35. doi:10.1145/3005714.
 81. Kure HI, Islam S, Mouratidis H. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Comput Appl*. 2022;34(18):15241–71. doi:10.1007/s00521-022-06959-2.
 82. Wangen G, Hallstensen C, Snekenes E. A framework for estimating information security risk assessment method completeness: core unified risk framework, CURF. *Int J Inf Secur*. 2018;17(6):681–99. doi:10.1007/s10207-017-0382-0.
 83. Joint Task Force Transformation Initiative. Guide for conducting risk assessments. Gaithersburg (MD): National Institute of Standards and Technology; 2012. Report No: NIST SP 800-30r1.
 84. Vorster A, Labuschagne LES. A framework for comparing different information security risk analysis methodologies. In: Proceedings of the 2005 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries; 2005. p. 95–103.
 85. Alfarisi S, Surantha N. Risk assessment in fleet management system using OCTAVE allegro. *Bulletin Of Elect Eng Info*. 2022;11(1):530–40. doi:10.11591/eei.v11i1.3241.
 86. Caralli RA, Stevens JF, Young LR, Wilson WR. Introducing octave allegro: improving the information security risk assessment process. Carnegie-Mellon University Pittsburgh PA Software Engineering Institution; 2007. Report No.
 87. Zahran B, Hussaini A, Ali-Gombe A, T-ARAS I. IIoT/ICS automated risk assessment system for prediction and prevention. In: Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy; 2021 Apr. New York (NY). Association for Computing Machinery. p. 305–07. CODASPY '21.
 88. Kerti A, Nyári N. Software development teamwork from an information security perspective. *Biztonságtudományi Szemle*. 2021;3:37–53.
 89. Lund MS, Solhaug B, Stølen K. Model-driven risk analysis: the CORAS approach. Berlin; London; New York: Springer Science & Business Media; 2010. doi:10.1007/978-3-642-12323-8.
 90. Sheikh J, Malviya B. Managing Cyber Risk and Security In Cloud Computing. *Int J Advan Comput Technol*. 2020;9:01–06.
 91. Supriyadi Y, Hardani CW. Information system risk scenario using COBIT 5 for risk and NIST SP 800-30 Rev. 1 a case study. In: 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE). IEEE; 2018. p. 287–91.
 92. Akinrolabu O, Nurse JRC, Martin A, New S. Cyber risk assessment in cloud provider environments: Current models and future needs. *Comput Secur*. 2019;87:101600. doi:10.1016/j.cose.2019.101600.
 93. Faris S, El Hasnaoui S, Medromi H, Iguer H, Sayouti A. Toward an effective information security risk management of universities' information systems using multi agent systems, ITIL, ISO 27002, ISO 27005. *Int J Advan Comput Sci Appl*. 2014;5(6). doi:10.14569/IJACSA.2014.050617.
 94. Mannane N, Bencharhi Y, Boulafourd B, Regragui B. Survey: risk assessment models for cloud computing: evaluation criteria. In: 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech); 2017. p. 1–5.
 95. Lim C, Suparman A. Risk analysis and comparative study of the different cloud computing providers in Indonesia. In: 2012 International Conference on Cloud Computing and Social Networking (ICCCSN). IEEE; 2012. p. 1–5.
 96. Pandey SK. A comparative study of risk assessment methodologies for information systems. *Bulletin Of Elect Eng Info*. 2012;1(2):111–22. doi:10.12928/eei.v1i2.231.
 97. Carter T, Kroll JA, Bret Michael J. Lessons learned from applying the NIST privacy framework. *IT Prof*. 2021;23 (4):9–13. doi:10.1109/MITP.2021.3086916.
 98. Zhou L, Wang C. Technology study on cloud computing security. *Software Guide*. 2014;3:132–33.
 99. Coppens P, Veeckman C, Claeys L. Privacy in location-based social networks: privacy scripts & user practices. *J Locat Based Serv*. 2015;9(1):1–15. doi:10.1080/17489725.2015.1017015.
 100. Liu ZY, Tseng YF, Tso R, Mambo M, Chen YC. Public-key authenticated encryption with keyword search: Cryptanalysis, enhanced security, and quantum-resistant instantiation. In: Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security; 2022 May. New York (NY): Association for Computing Machinery. p. 423–36. ASIA CCS '22.
 101. Gupta R, Singh AK. Differential and access policy based privacy-preserving model in cloud environment. *J Web Eng*. 2022;609–32. doi:10.13052/jwe1540-9589.2132.
 102. Belguith S, Kaaniche N, Hammoudeh M. Analysis of attribute-based cryptographic techniques and their application to protect cloud services. *Trans Emerging Telecommun Technol*. 2022;33(3):e3667. doi:10.1002/ett.3667.
 103. di Vimercati SDC. Access control policies, models, and mechanisms. *Encycl Cryptogr Secur Priv*. 2021.
 104. Ren H. Status and developments of access control model. *Comput Digit Eng*. 2013;41:452–56.
 105. Zhen Y. Improvement of role-based access controlModel. *Software Guide*. 2014;13:32–34.
 106. Abdul AM, Mohammad AAK, Venkat Reddy P, Nuthakki P, Kancharla R, Joshi R, Kannaiya Raja N. Enhancing security of mobile cloud computing by trust-and role-based access control. *Sci Program*. 2022;2022:1–10. doi:10.1155/2022/9995023.
 107. Servos D, Osborn SL. Current research and open problems in attribute-based access control. *ACM Comput Surv (CSUR)*. 2017;49(4):1–45. doi:10.1145/3007204.
 108. Hermans J, Pashalidis A, Vercauteren F, Preneel B. A new RFID privacy model. In: Computer security–ESORICS 2011: 16th European symposium on research

- in computer security; 2011 Sept 12-14. Proceedings 16. Leuven (Belgium): Springer; 2011. p. 568–87.
109. Zheng X, Mukkamala RR, Vatrappu R, Ordieres-Mere J. Blockchain-based personal health data sharing system using cloud storage. In: 2018 IEEE 20th International Conference on E-Health Networking, Applications and Services (Healthcom). IEEE; 2018. p. 1–6.
 110. Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. *J Netw Comput Appl*. 2011;34(1):1–11. doi:10.1016/j.jnca.2010.07.006.
 111. Rittinghouse JW, Ransome JF. Cloud computing: implementation, management, and security. 1st ed. Boca Raton: CRC press; 2016.
 112. Hashem IAT, Yaqoob I, Anuar NB, Mokhtar S, Gani A, Ullah Khan S. The rise of “big data” on cloud computing: review and open research issues. *Inf Syst*. 2015;47:98–115. doi:10.1016/j.is.2014.07.006.
 113. Baskerville R, Spagnoletti P, Kim J. Incident-centered information security: managing a strategic balance between prevention and response. *Inf Manage*. 2014;51(1):138–51. doi:10.1016/j.im.2013.11.004.
 114. Cichonski P, Millar T, Grance T, Scarfone K. Computer security incident handling guide: recommendations of the national institute of standards and technology. NIST Special Publ. 2012;800:1–147.
 115. Anuar NB, Papadaki M, Furnell S, Clarke N. A response selection model for intrusion response systems: response strategy model (RSM). *Secur Commun Netw*. 2014;7(11):1831–48. doi:10.1002/sec.896.
 116. Luo Y, Szidarovszky F, Al-Nashif Y, Hariri S. A fictitious play-based response strategy for multistage intrusion defense systems. *Secur Commun Netw*. 2014;7(3):473–91. doi:10.1002/sec.730.
 117. Anwar S, Zain JM, Zolkipli MFB, Inayat Z, Khan S, Anthony B, Chang V. From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. *Algorithms*. 2017;10(2):39. doi:10.3390/a10020039.
 118. Achara S, Rathi R. Security related risks and their monitoring in cloud computing. *Int J Comput Appl*. 2014;86(13):42–47. doi:10.5120/15049-3417.
 119. Andrikopoulos V, Binz T, Leymann F, Strauch S. How to adapt applications for the cloud environment. *Computing*. 2013;95(6):493–535. doi:10.1007/s00607-012-0248-2.
 120. Damenu TK, Balakrishna C. Cloud Security Risk Management: A Critical Review. In: 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies; 2015 Sep. p. 370–75.
 121. El Fray I. A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment (FoMRA) in information systems. In: Cortesi A, Chaki N, Saeed K, Wierzcho n’ S, editors. Computer information systems and industrial management. Berlin (Heidelberg): Springer; 2012. p. 428–42.
 122. Ab Rahman NH, Choo KKR. A survey of information security incident handling in the cloud. *Comput Secur*. 2015;49:45–69. doi:10.1016/j.cose.2014.11.006.
 123. Fessi BA, Benabdallah S, Boudriga N, Hamdi M. A multi-attribute decision model for intrusion response system. *Inf Sci*. 2014;270:237–54. doi:10.1016/j.ins.2014.02.139.
 124. Ahmad A, Hadgkiss J, Ruighaver AB. Incident response teams—challenges in supporting the organisational security function. *Comput Secur*. 2012;31(5):643–52. doi:10.1016/j.cose.2012.04.001.
 125. Shedden P, Ahmad A, Ruighaver A. Organisational learning and incident response: promoting effective learning through the incident response process. In: Proceedings of the 8th Australian Information Security Management Conference; 2010 Nov 30. Edith Cowan University.
 126. Taylor LP. Developing an incident response plan ‘. FISMA compliance handbook. 2013;95–115.
 127. Butt UA, Mehmood M, Shah SBH, Amin R, Shaukat MW, Raza SM, Suh DY, Piran MJ. A review of machine learning algorithms for cloud computing security. *Electronics*. 2020;9(9):1379. doi:10.3390/electronics9091379.
 128. Pavithran D, Shaalan K, Al-Karaki JN, Gawanmeh A. Towards building a blockchain framework for IoT. *Cluster Comput*. 2020;23(3):2089–103. doi:10.1007/s10586-020-03059-5.
 129. Mughal A, Joseph A. Blockchain for Cloud Storage Security: A Review. In: 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS); 2020 May. p. 1163–69.
 130. Mondal A, Paul S, Goswami RT, Nath S. Cloud computing security issues & challenges: A Review. In: 2020 International Conference on Computer Communication and Informatics (ICCCI); 2020 Jan. p. 1–5.
 131. Venifa Mini G, Angel Viji KS. Emerging Access Control Techniques in Cloud Computing: A Survey. In: 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI); 2018 May. p. 1354–59.
 132. Blaze M, Feigenbaum J, Lacy J. Decentralized trust management. In: Proceedings 1996 IEEE Symposium on Security and Privacy; 1996 May. p. 164–73.
 133. Fang L, Yin LH, Guo YC, Fang BX. A survey of key technologies in attribute-based access control scheme. *Chinese J Comput*. 2017;40:1680–98.
 134. El Sibai R, Gemayel N, Bou Abdo J, Demerjian J. A survey on access control mechanisms for cloud computing. *Trans Emerging Telecommun Technol*. 2020;31(2):e3720. doi:10.1002/ett.3720.
 135. Bose R, Chakraborty S, Roy S. Explaining the workings principle of cloud-based multi-factor authentication architecture on banking sectors. In: 2019 Amity International Conference on Artificial Intelligence (AICAI); 2019 Feb. p. 764–68.
 136. Chung L, Mingji M, Bingxu L, Shuxin C. Design and implementation of trust-based access control model for cloud computing. In: 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) vol. 5; 2021 Mar. p. 1934–38.
 137. Nadeem M, Arshad A, Riaz S, Band SS, Mosavi A. Intercept the cloud network from brute force and DDoS attacks via intrusion detection and prevention system. *IEEE Access*. 2021;9:152300–09. doi:10.1109/ACCESS.2021.3126535.

138. Gupta A, Kalra M. Intrusion detection and prevention system using cuckoo search algorithm with ANN in cloud computing. In: 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC); 2020 Nov. p. 66–72.
139. Basu S, Bardhan A, Gupta K, Saha P, Pal M, Bose M, Basu K, Chaudhury S, Sarkar P. Cloud computing security challenges & solutions-A survey. In: 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC); 2018 Jan. p. 347–56.
140. Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India, Snehi J, Bhandari A, Department of Computer Science and Engineering, Panjab University, Patiala, India, Baggan V, Engineering Department, Infosys Limited, Chandigarh, India, Snehi M, Engineering Department, Infosys Limited, Chandigarh, India Ritu, Engineering Department, Infosys Limited, Chandigarh, India. Diverse methods for signature based intrusion detection schemes adopted. IJRTE. 2020;9(2):44–49.
141. Aryachandra AA, Arif YF, Anggis SN. Intrusion detection system (IDS) server placement analysis in cloud computing. In: 2016 4th International Conference on Information and Communication Technology (ICoICT); 2016 May. p. 1–5.
142. Gassais R, Ezzati-Jivan N, Fernandez JM, Aloise D, Dagenais MR. Multi-level host-based intrusion detection system for internet of things. J Cloud Comput (Heidelb). 2020;9(1):62. doi:10.1186/s13677-020-00206-6.
143. Mazini M, Shirazi B, Mahdavi I. Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. J King Saud Univ Comput Inf Sci. 2019;31(4):541–53. doi:10.1016/j.jksuci.2018.03.011.
144. De La Torre Parra G, Rad P, Choo KKR, Beebe N. Detecting internet of things attacks using distributed deep learning. J Netw Comput Appl. 2020;163:102662. doi:10.1016/j.jnca.2020.102662.
145. Bucur V, Stan O, Miclea LC. Data loss prevention and data protection in cloud environments based on authentication tokens. In: 2019 22nd International Conference on Control Systems and Computer Science (CSCS); 2019 May. p. 720–25.
146. Costante E, Fauri D, Etalle S, den Hartog J, Zannone N. A hybrid framework for data loss prevention and detection. In: 2016 IEEE Security and Privacy Workshops (SPW); 2016 May. p. 324–33.
147. Gómez-Hidalgo JM, Martín-Abreu JM, Nieves J, Santos I, Brezo F, Bringas PG. Data leak prevention through named entity recognition. In: 2010 IEEE Second International Conference on Social Computing; 2010 Aug. p. 1129–34.
148. Ong YJ, Qiao M, Routray R, Raphael R. Context-aware data loss prevention for cloud storage services. In: 2017 IEEE 10th International Conference on Cloud Computing (CLOUD); 2017 Jun. p. 399–406.
149. Ahmad S, Mehruz S, Mebarek-Oudina F, Beg J. RSM analysis based cloud access security broker: a systematic literature review. Cluster Comput. 2022;25(5):3733–63. doi:10.1007/s10586-022-03598-z.
150. Tian H, Peng F, Quan H, Chang CC. Identity-based public auditing for cloud storage of internet-of-vehicles data. ACM Trans Internet Technol. 2023;22(4):88:1–24. doi:10.1145/3433543.
151. He W, Akhawe D, Jain S, Shi E, Song D. ShadowCrypt: encrypted web applications for everyone. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security; 2014 Nov. New York (NY): Association for Computing Machinery. p. 1028–39. CCS '14.
152. Lau B, Chung S, Song C, Jang Y, Lee W, Boldyreva A. Mimesis aegis: a mimicry privacy shield—A system's approach to data privacy on public cloud. In: 23rd USENIX security symposium (USENIX security 14). San Diego (CA): USENIX Association; 2014. p. 33–48.
153. Popa RA, Redfield CMS, Zeldovich N, Balakrishnan H, Crypt DB. Protecting confidentiality with encrypted query processing. In: Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles; 2011 Oct. New York (NY): Association for Computing Machinery. p. 85–100. SOSP '11.
154. Grubbs P, McPherson R, Naveed M, Ristenpart T, Shmatikov V. Breaking web applications built on top of encrypted data. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security; 2016 Oct. New York (NY): Association for Computing Machinery. p. 1353–64. CCS '16.
155. Rathore MS, Poongodi M, Saurabh P, Lilhore UK, Bourouis S, Alhakami W, Osamor J, Hamdi M. A novel trust-based security and privacy model for internet of vehicles using encryption and steganography. Comput Electr Eng. 2022;102:108205. doi:10.1016/j.compeleceng.2022.108205.
156. Redondo C, Arora R, Greyfish. An out-of-the-box, reusable, portable cloud storage service. In: Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (Learning); 2019 Jul; New York (NY): Association for Computing Machinery. p. 1–6. PEARC '19.