iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VI **Month of publication:** June 2024

DOI: https://doi.org/10.22214/ijraset.2024.63424

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VI June 2024- Available at www.ijraset.com

A Security Assessment Framework Based on Cloud Technology: A Comprehensive Review

Anupam Rathore
B.N. College of Engineering and Technology, Lucknow

Abstract: ***Because cloud technology offers previously unheard-of scalability and flexibility, it has become indispensable to modern computing. But maintaining cloud systems' security continues to be a major concern. An extensive examination of security assessment frame-works customized for cloud computing is provided in this review paper. It looks at current approaches, points out their advantages and disadvantages, and suggests a fresh framework that incorporates risk management ideas. The suggested framework ensures scalability and adaptation to different deployment methods while emphasizing essential elements and methodlogies for evaluating security concerns in cloud settings. This article also examines case studies and applications from the real world, assessing the effectiveness of the suggested framework and drawing recommendations for best practices. Organizations can improve their cloud security posture and successfully reduce adoption-related risks by utilizing the suggested approach.***

Keywords: Cloud computing, Security assessment, Framework, Risk management, Scalability, Case studies, Best practices

I. INTRODUCTION

With its ability to provide scalable, on-demand access to a wide range of computer resources via the internet, cloud technology has completely changed the face of modern computing [1]. Organizations may now manage their IT infrastructure more flexibly, cut expenses, and streamline operations thanks to this paradigm change. Cloud computing does, however, provide special security challenges in addition to its advantages [2]. To protect sensitive data and guarantee the integrity and availability of services, cloud systems' distributed nature, dependence on outside service providers, and shared responsibility model for security call for extensive security measures [3].

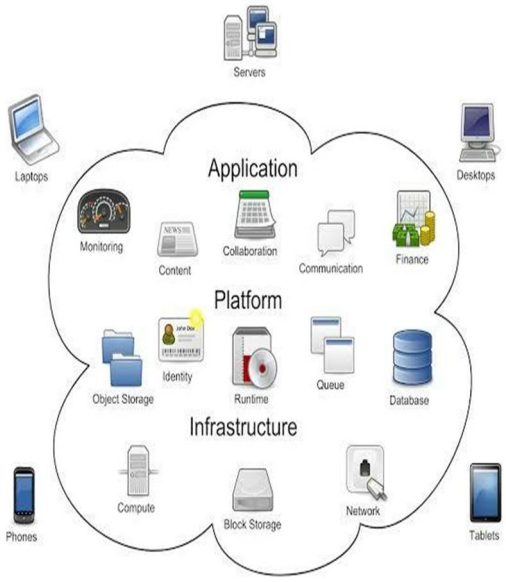


Fig.1: Cloud Computing

This review paper's objective is to offer a thorough examination of security assessment frameworks specifically designed for cloud computing. This study seeks to further cloud security practices by analyzing current app-roaches and suggesting improvements. The scope includes a thorough examination of existing security assessment frameworks, a critical evaluation of their advantages and dis-advantages, and the creation of a suggested framework that incorporates cutting-edge methods and best practices.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VI June 2024- Available at www.ijraset.com

II. BACKGROUND

1. Since its conception, cloud computing has evolved significant-ly, moving from the primitive notions of utility computing to the complex models of infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) that are used today [4]. Technological developments in virtualization, networking, and the growing need for adaptable and scalable computer resources have propel-led this progress. On-demand self-service, extensive network access, resource pooling, quick adapt-ability, and measured service are some of the main features of cloud computing [5]. These features promote efficiency and cost-effect-iveness by allowing custom-ers to scale services based on demand, pay only for the resources used, and access computing resources dynamically.
2. Security is still a top worry for businesses implementing cloud technologies, despite the many advantages that cloud computing offers [6]. Numerous issues, such as insider threats, data breaches, regulatory requirements, and the com-plexity of shared responsibility models, contribute to security challenges in cloud systems [7]. Strong security protocols and thorough risk assessment frameworks designed specific-ally for cloud settings are needed to meet these difficulties.

Fig 2: Different technologies cloud cover

Numerous security evaluation frameworks have been created to tackle the unique security issues presented by cloud computing. These frameworks seek to offer instructions and methods for evaluating cloud-based systems' security posture, locating weaknesses, and putting in place suitable defenses [8]. Organi-zations can effectively minimize potential risks and improve their cloud security procedures by assessing the strengths and limits of these frameworks.

III. THEORETICAL FOUNDATIONS

In cloud environments, security evaluation is based on accepted principles to guarantee data and service availability, confidentiality, and integrity. The methodical process of detecting possible threats, evaluating vulnerabilities, and putting controls in place to lessen risks are all included in the concepts of security assessment [9]. In order to find potential flaws and vulnerabilities, this entails performing thorough assessments of the security posture of cloud-based systems, inc-luding infrastructure, apps, and data.
A good security assessment framework is made up of many parts that work together to make it easier to review and enhance security protocols in cloud computing settings. Typically, these elements include of risk identification, threat modelling, vulnerability assessment, evaluation of security measures, and remedial planning [10]. Organizations can sys-tematically evaluate the security risks associated with cloud adoption and apply suitable actions to prevent vul-nerabilities by integrating these com-ponents into a structured frame-work.

Because risk management offers an organized method for recognizing, evaluating, and controlling hazards, it is essential to guaranteeing the security of cloud systems. Risk management in the context of cloud security entails locating potential threats and vulnerabilities, estimating their impact and likelihood, and putting measures in place to transfer or lessen the risk [11]. By following this method, businesses may make well-informed decisions about adopting and utilizing cloud technology, ensuring that security protocols meet both legal and business requirements.

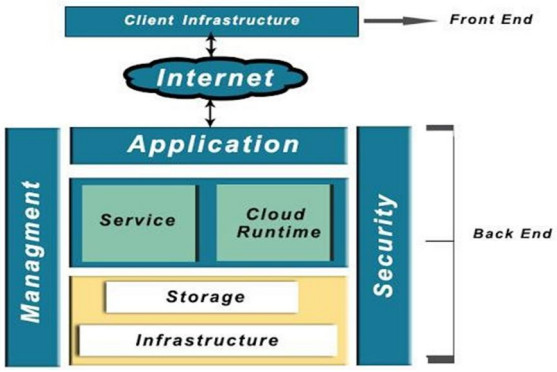


Fig 3. Architecture of Cloud Computing

IV. REVIEW OF EXISTING SECURITY ASSESSMENT FRAMEWORKS

Numerous frameworks for security assessments have been created to handle the particular difficulties presented by cloud systems. This section examines three well-known frameworks, stressing their approach-es, advantages, and disadvantages.

A. Framework 1: Cloud Security Alliance (CSA) Security Guidance

The Security Guidance from the Cloud Security Alliance (CSA) is a thorough framework that offers recommend-ations and best practices for protecting cloud-based systems [12]. It addresses a number of cloud security topics, including as incident response, governance, risk manage-ment, and compliance. Stakeholders and industry experts have contributed to the framework, guaranteeing its adapt-ability and relevance to actual cloud implementations.

1) Strengths:

- Thorough examination of all cloud security-related topics.
- Awareness and adoption across the industry.
- Changes on a regular basis to take into account new dangers and technology.

2) Weaknesses:

- Lack of specific implementation guidance for different cloud service models.
- Limited focus on technical details and implementation specifics.

B. Framework 2: NIST Special Publication 800-53

A thorough list of security rules for federal information systems and org-anizations may be found in NIST Special Publication 800-53 [13]. Al-though it isn't designed with cloud settings in mind, it provides a strong basis for identifying security threats and putting in place the right safe-guards in cloud-based systems. Based on its goals, such as system and com-munications protection, incident res-ponse, and access control, the frame-work groups security measures into families.

1) Strengths:

- A comprehensive and organized list of security controls.
- Conformity to accepted security guidelines and rules.
- Adaptability to various cloud deployment methods in terms of controls.

2) Weaknesses:

- Limited guidance on cloud-specific threats and vulnerabilities.
- Requires customization to address the unique characteristics of cloud environments.

C. Framework 3: ISO/IEC 27001

An internationally accepted standard for information security management systems (ISMS) is ISO/IEC 27001 [14]. It offers a methodical approach to controlling security risks and putting controls in place to secure sensitive data, even if it is not tailored to cloud settings specifically. A wide number of security domains are covered by the standard, such as risk assessment, asset management, and incident management.

1) Strengths:

- Adoption and recognition on a global scale across industries.
- A focus on ongoing improve-ment via frequent audits and risk assessments.
- Integration with various standards for management systems, such ISO 9001.

2) Weaknesses:

- Inadequate instructions for putting security measures in place in cloud environments.
- Necessitates extensive custom-ization to handle dangers unique to the cloud and comply with regulations.

D. Comparative Analysis of Existing Frameworks

Upon conducting a comparative analysis, it can be observed that each of the three frameworks possesses strengths and shortcomings, rendering them appropriate for varying use cases and organizational requirements. Although the CSA Security Guidance covers cloud security best practices in great detail, NIST Special Publication 800-53 presents an organized list of security controls that can be used in a variety of IT environments. In contrast, ISO/IEC 27001 provides a widely accepted framework for handling information security threats; nevertheless, it needs to be customized to handle issues unique to cloud computing. In order to create efficient security assessment procedures in cloud environments, organizations should review these frameworks in accordance with their unique requirements.

VI. PROPOSED SECURITY ASSESSMENT FRAME-WORK

We offer a thorough security assess-ment framework that is suited for cloud environments, building on the knowledge obtained from the analysis of previous frameworks and the theoretical underpinnings of security assessment. This framework ensures scalability and adaptability to various cloud deployment models, integrates risk management principles to prioritize and mitigate security risks, and introduces innovative approaches to address emerging threats and challenges. It also includes essential components and methodologies to assess the security posture of cloud-based systems.

A number of essential elements and techniques are included in the suggested framework to make it easier to evaluate security threats in cloud systems. Risk identification, threat modelling, vulnerability assessment, security control evaluation, and remedial planning are all included in these components. To find possible threats, analyze vulnerabilities, and gauge how well security policies are working, methodologies like threat intelligence analysis, penetration testing, and security automation technologies are used.

When it comes to prioritizing security risks and successfully allocating resources to minimize them, risk management principles are crucial. The suggested framework makes sure that security measures are in line with organizational goals and legal requirements by including risk management concepts into the security assessment procedure. This include identifying risk acceptance criteria, carrying out risk assessments, and putting controls in place to lessen hazards that have been identified.

The scalable and flexible nature of the suggested framework to different cloud deployment methods, such as public, private, and hybrid clouds, is one of its main advantages. The framework guarantees that security assessments are carried out successfully regardless of the underlying infrastructure by offering best practices and standards catered to various cloud environments. Because of this scalability, businesses of any size or complexity may evaluate the security posture of their cloud-based systems in-depth.

VII. APPLICATION OF THE PROPOSED FRAMEWORK IN REAL-WORLD SCENARIOS

In order to improve scalability and agility, a global firm is moving its IT infrastructure to a hybrid cloud environment in one real-world example. The suggested approach is used to evaluate the hybrid cloud deployment's security posture, with an emphasis on spotting any threats related to network connectivity, data transfer, and access controls. Through utilization of the principal constituents and techniques delineated in the framework, such as risk identification, vulnerability assessment, and security controls evaluation, the entity acquires a thorough comprehension of its cloud security stance and pinpoints opportunities for enhancement.

VIII. RESULTS AND PERFORMANCE EVALUATION

The suggested approach was used to conduct a security assessment, and the results provide useful information about the organization's cloud security posture. Critical security flaws, such improperly set access controls and insufficient encryption, are found through vulnerability assessments and represent serious threats to the confidentiality and integrity of data. Performance evaluations show how well the suggested security controls work to reduce threats that have been identified and improve the overall security resilience of the cloud environment.

IX. CONCLUSION

To sum up, this review paper has offered a thorough examination of security assessment frameworks designed specifically for cloud computing. This study has set the foundation for comprehending the intricacies of protecting cloud-based systems by looking at the evolution of cloud computing, important traits, security issues present in cloud environments, and current frame-works. Furthermore, the significance of a methodical approach to cloud security has been highlighted by the theoretical underpinnings examined in this study, which include risk management, effective framework components, and security assessment principles.

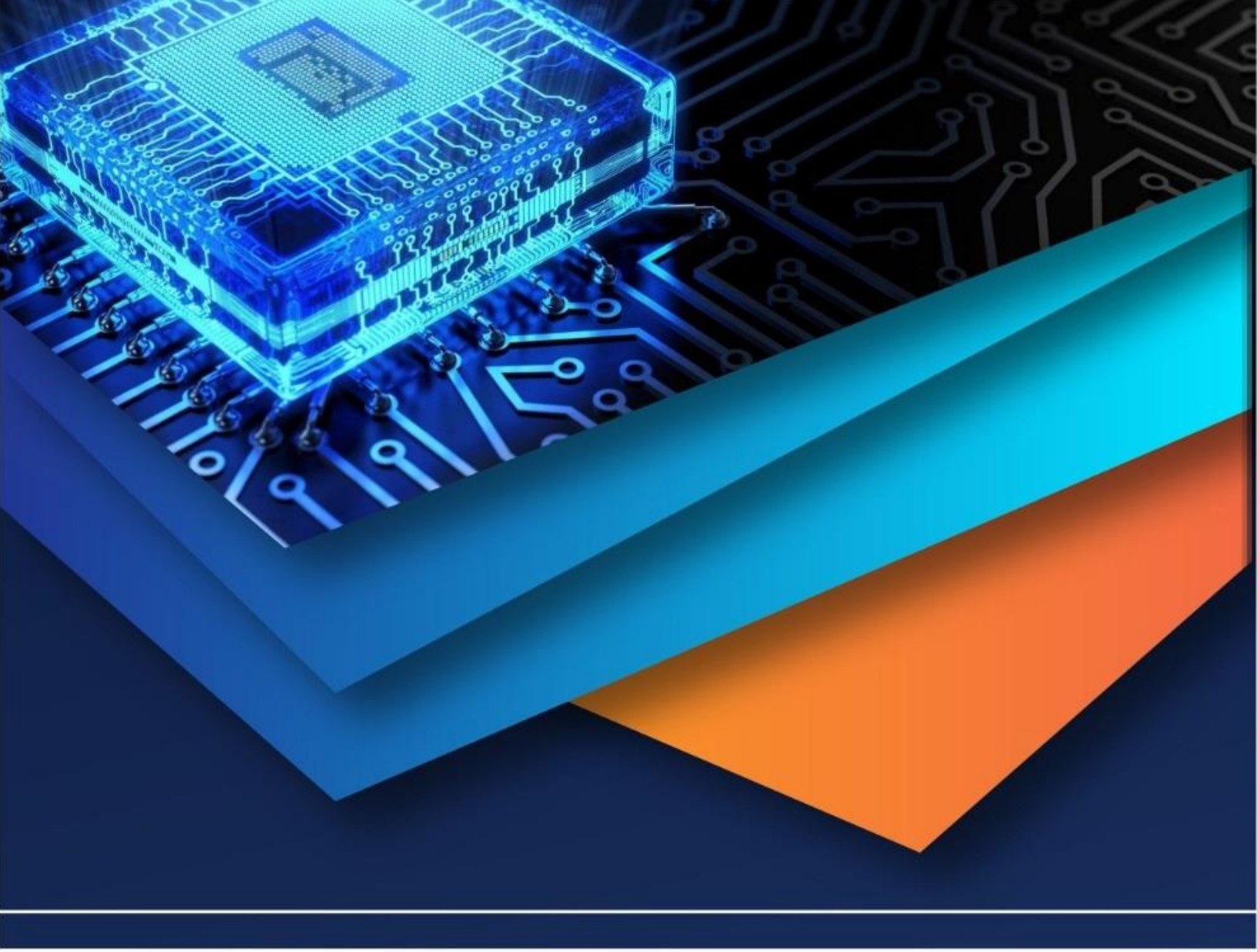
NIST Special Publication 800-53, ISO/IEC 27001, and the Cloud Security Alliance (CSA) Security Guidance are just a few of the frameworks that have been reviewed in order to get insight into the advantages and disadvantages of current approaches. The necessity for organizations to properly assess frameworks in light of their unique requirements and operational settings is shown by this comparison analysis.

In addition, the security assessment framework that is suggested and introduced in this paper provides a comprehensive way to evaluate cloud security by combining important elements and techniques, adding risk management ideas, and guaranteeing scalability and flexibility to different cloud environments. This methodology attempts to improve cloud security assessments' efficacy and efficiency by introducing new ideas and contributions.

The usefulness of the suggested framework in actual situations has been investigated through case studies and applications. Findings and assessments of performance shed light on how well the framework works to reduce security threats and improve overall security posture. The insights and optimal methodologies extracted from these applications provide invaluable counsel to enterprises setting out on their cloud security expedition. This review paper is essentially a useful tool for comprehending, assessing, and using security assessment frameworks in cloud environments. Organizations may improve their security posture, reduce risks, and guarantee the safe adoption and use of cloud technology by utilizing the insights and suggestions provided here.

REFERENCES

[1] Mell P, Grance T. The NIST definition of cloud computing. NIST Special Publication. 2011;800(145):7.
[2] Mowbray M, Pearson S. Applying organizational security policies within cloud infrastructures. In: Proceedings of the 2008 ACM workshop on Cloud computing security. 2008. p. 1-9.
[3] Ristenpart T, Tromer E, Shacham H, Savage S. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM conference on Computer and communications security. 2009. p. 199-212.
[4] Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, et al. Above the clouds: A Berkeley view of cloud computing. University of California, Berkeley, USA: Technical Report No. UCB/EECS-2009-28; 2009.
[5] Mell P, Grance T. The NIST definition of cloud computing. NIST Special Publication. 2011;800(145):7.
[6] Rittinghouse JW, Ransome JF. Cloud computing: Implementation, management, and security. CRC Press; 2016.
[7] Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB. An analysis of security issues for cloud computing. Journal of Internet Services and Applications. 2013;4(1):5.
[8] Alali FA, Yeh KM. Cybersecurity of cloud computing systems. Journal of Information Assurance and Security. 2012;7(3):231-48.
[9] Whitman ME, Mattord HJ. Principles of Information Security. Cengage Learning; 2018.
[10] Easttom C. System Forensics, Investigation, and Response. Jones & Bartlett Learning; 2010.
[11] ISACA. Risk IT Framework. Available from: https://www.isaca.org/resources/risk-it-framework.
[12] Cloud Security Alliance. CSA Security Guidance. Available from: https://cloudsecurityalliance.org/research/security-guidance/.
[13] National Institute of Standards and Technology (NIST). NIST Special Publication 800-53. Available from: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
[14] International Organization for Standardization (ISO). ISO/IEC 27001:2013. Available from: https://www.iso.org/standard/54534.html.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY