International Journal of Advanced Digital Systems and Multidisciplinary Studies (IJADSMS), Vol. 1, Issue 2, pp. 14–17, (2026)
Published: February 2026

Cloud Computing Security Frameworks: Addressing Emerging Cyber Threats

Ms. Lakshmi Kumari [1], Mr. Ajit Kumar[2], Ms. Kumari Puja [3] , Mr. Abhishek Kumar[4], Ms. Anupama[5],Mr. Sachin Kashyap[6]

[1,3,4,5,6] *Assistant Professor ,School of Computer Applications, Noida Institute of Engineering and Technology (NIET) Greater Noida*

[2]*Assistant Professor, Amity Institute of Information Technology (AIIT), Amity University Jharkhand, Ranchi*

lakshmi1051999@gmail.com[1] , *akumar7@rnc.amity.edu[2], gkp2910@gmail.com[3],abhishek.kumar@niet.co.in[4] , anupama0140@gmail.com[5] , sachinkashyap80770@gmail.com[6]*

Abstract

This paper critically examines the efficacy of current cloud security frameworks in mitigating advanced persistent threats, data breaches, and insider threats within dynamic cloud environments. It evaluates how well these frameworks, such as ISO/IEC 27001, FedRAMP, and SOC 2, align with the Cloud Security Alliance's benchmarks for addressing prevalent cloud vulnerabilities. Furthermore, the research delves into the adaptability of these frameworks to novel attack vectors and their capacity to ensure regulatory compliance in a multitenant cloud infrastructure. It further investigates the societal impact of these cyberattacks, proposing general preventive measures and advocating for policy changes to enhance public awareness and safeguard cloud services. This study also undertakes a comparative analysis of established security frameworks like COBIT 5, NIST, and ISO, alongside cloud-specific methodologies such as CSA STAR and AWS Well-Architected Framework, to identify their respective strengths and limitations in addressing the unique security challenges presented by cloud computing.

keywords: Cloud computing, Security of cloud services, Risk assessment, Data protection, Cyber threats, Mitigation strategies.

Introduction

Cloud computing has become an indispensable paradigm for modern enterprises, offering unparalleled scalability, flexibility, and cost-efficiency; however, this widespread adoption also introduces a complex landscape of security challenges that necessitate sophisticated and adaptive frameworks to mitigate emerging cyber threats [1], [2]. This paper critically examines existing cloud security frameworks, highlighting their strengths and limitations in addressing the dynamic nature of contemporary cyber-attacks, and proposes a comprehensive approach incorporating advanced risk management strategies [3], [4]. The proliferation of cloud technologies, while transformative for data management and operational efficiency, simultaneously introduces novel vulnerabilities stemming from multi-tenancy, shared infrastructure, and reliance on third-party service providers [5]. These unique security concerns, including data privacy and threat prevention, mandate a robust and integrated security posture that extends beyond traditional on-premises security paradigms [2], [5]. Consequently, organizations must transition from conventional security models to holistic frameworks that systematically identify, analyze, assess, and address risks across interconnected cloud domains, thereby enhancing security measures [6]. This comprehensive review aims to thoroughly examine security assessment frameworks specifically designed for cloud computing, analyzing current methodologies and suggesting improvements to further cloud security practices [4]. Even with advancements in cryptographic techniques for cloud data protection, the linear runtime of most cryptographic systems poses a challenge for ensuring data security, particularly with large datasets [3]. Therefore, evaluating secure proofs from cryptographic evaluators and assigning confidence levels is crucial for selecting appropriate distributed frameworks that align with the evolving cloud security landscape [7]. This paper investigates optimized approaches to cloud information security management by reviewing the current threat landscape and evaluating key risk management frameworks to provide practical solutions for enhancing enterprise cloud security [8]. This involves a comprehensive understanding of various cloud service models and deployment strategies, ensuring that proposed solutions are both adaptable and scalable across diverse cloud environments [4].

Literature Review

This section reviews prominent research and conceptual models pertinent to cloud computing security, highlighting critical challenges such as data security in multi-tenant

environments and the need for robust risk assessment methodologies [9], [10]. Key areas of concern include communication interception, denial-of-service attacks, and the injection of cloud malware, all of which pose significant threats to data integrity and availability within cloud infrastructures [11]. The widespread adoption of cloud computing by various organizations underscores the importance for information security management firms to prioritize data security in this domain, as data violations or corruption can significantly damage public confidence and confidentiality, potentially leading to enterprise failure [12]. Therefore, a thorough examination of security assessment frameworks designed specifically for cloud technology is essential to understand the intricacies of protecting cloud-based systems [4]. This involves a methodical process of detecting potential threats, evaluating vulnerabilities, and implementing controls to mitigate risks, encompassing comprehensive assessments of infrastructure, applications, and data within cloud environments [4]. These evaluations often involve a multi-layer categorization approach to address the specific security needs of both cloud providers and consumers, considering factors like data encryption, multi-tenancy, data privacy, authentication, and authorization [13]. Such frameworks are critical for identifying vulnerabilities and ensuring compliance with regulatory requirements, thereby safeguarding sensitive information and maintaining operational resilience in the face of evolving cyber threats [14]. The security challenges in cloud environments extend beyond traditional IT, encompassing issues such as limited resource elasticity, multi-tenancy complexities, and unpredictable environmental factors [15]. For instance, distributed denial-of-service attacks, account hijacking, malware infiltration, and data breaches remain persistent threats that necessitate advanced mitigation strategies like security awareness training, vulnerability management, and robust identity and access management systems [16]. Furthermore, the dynamic nature of cloud environments, characterized by rapid provisioning and de-provisioning of resources, necessitates continuous security assessments and an agile risk management framework to effectively address evolving threats [17].

Methodology

This section outlines the systematic approach undertaken to identify, analyze, and synthesize the relevant literature on cloud computing security frameworks, focusing on their efficacy in addressing contemporary cyber threats. Our methodology rigorously followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses guidelines to ensure a comprehensive and unbiased selection of pertinent studies [18]. This systematic literature review focused on identifying taxonomies and frameworks for categorizing cloud computing security issues and vulnerabilities, ensuring a robust foundation for understanding the complexities involved [19]. The structured approach facilitated a comprehensive evaluation of existing mitigation strategies and threat landscapes within cloud computing environments [16]. Specifically, this involved extensive database searches using predefined keywords to identify scholarly articles published between 2012 and 2023, primarily from IEEE Xplore and Google Scholar [18]. This systematic approach ensured a wide breadth of coverage, allowing for the inclusion of diverse perspectives on cloud security challenges and their corresponding solutions [16], [19]. This systematic literature review also incorporates a comparative analysis of various Information Security Risk Management frameworks specifically designed for cloud environments, emphasizing their structured approach to categorizing multifaceted cloud security risks and mitigation strategies [20]. This systematic review utilized methodologies from Webster and Watson, Levy and Ellis, and Kitchenham to conduct a thorough analysis, with a particular emphasis on Kitchenham's widely adopted guidelines for computer and information system domains [21]. The initial search across these databases using keywords such as "Cloud Computing Security" and "Cyber Threats" yielded 8580 papers, which were then systematically filtered to ensure relevance and quality [18]. This rigorous filtering process involved several stages, including title and abstract screening, followed by a full-text review of selected articles, ultimately narrowing down the corpus to a manageable set of highly relevant studies for in-depth analysis [15], [22]. This meticulous selection process aimed to identify novel architectures for AI-based threat detection systems and comprehensive reviews of intelligent intrusion detection techniques in cloud environments [23], [24].

Results

The subsequent analysis of these refined results focused on synthesizing common themes, identifying prevalent threats, and evaluating the effectiveness of proposed security frameworks and mitigation strategies [16], [25]. The thematic analysis, based on a meticulous literature review, allowed for the extraction of meaningful patterns and insights from the selected research studies, thereby identifying emerging trends in cloud computing security, threats, and mitigation strategies [16]. This comprehensive approach facilitated the identification of critical gaps in existing security frameworks and highlighted areas requiring further research and development to address the dynamic nature of cloud cyber threats [16]. Specifically, common threats identified include data breaches, which involve unauthorized access to sensitive information, and various malware attacks designed to disrupt operations or corrupt data integrity [16]. Beyond these, distributed denial-of-service attacks continue to pose significant challenges by overwhelming cloud resources, while insider threats and account hijacking represent persistent vulnerabilities within cloud environments [16]. Emerging trends, such as integrating artificial intelligence and machine learning, serverless computing, and containerization, further complicate the security landscape, necessitating advanced AI-enhanced threat detection mechanisms to adapt to these evolving paradigms [16], [24], [26]. The continuous development of sophisticated cyber-physical systems and the proliferation of IoT devices also introduce new attack vectors, demanding a re-evaluation of current security protocols and the implementation of adaptive, real-time response mechanisms [27]. Moreover, the shift towards data-centric and user-access control models in

cloud security, as highlighted by recent findings, underscores a fundamental evolution from infrastructure-focused protection to more granular and context-aware security paradigms [3].

Discussion

This section delves into a comprehensive analysis of the identified security frameworks, evaluating their strengths, weaknesses, and applicability in mitigating the sophisticated cyber threats prevalent in modern cloud environments [16]. This evaluation focuses on understanding how these frameworks address issues such as data breaches, unauthorized access, and insider threats, while also considering their adaptability to emerging technologies like AI and machine learning [16], [28], [29]. The discussion further examines the evolution of cloud computing, tracing its historical development and highlighting the new security challenges and opportunities that have arisen in tandem with its growth [3]. It also scrutinizes the shared responsibility model, a cornerstone of cloud security, and analyzes the inherent complexities and potential pitfalls it presents for organizations in maintaining a robust security posture [16]. Furthermore, this section explores how various proposed solutions, including advanced encryption techniques, sophisticated Identity and Access Management systems, and AI-driven threat detection mechanisms, are being developed and refined to counteract the increasing complexity of cloud computing security concerns [2], [5].

Conclusion

The ongoing progression of cloud security frameworks necessitates a continuous re-evaluation of current models to address the rapid advancements in threat landscapes, especially with the integration of AI and machine learning for predictive and real-time threat responses [3], [5]. Organizations are increasingly adopting collaborative security models to share threat intelligence and standardize security protocols across diverse cloud platforms, moving beyond traditional, isolated defense strategies [3]. This collaborative approach, often underpinned by established security frameworks such as those proposed by the Cloud Security Alliance, the National Institute of Standards and Technology, and the International Organization for Standardization, aids in establishing robust security measures and promotes a more unified defense against cyber threats [30]. These frameworks aim to provide a methodical and all-encompassing strategy for safeguarding against cloud threats, even in scenarios with limited resources or expertise [31]. Such frameworks, by offering standardized guidelines and best practices, enable organizations to systematically identify, assess, and mitigate risks, thereby enhancing their overall security posture in complex cloud ecosystems [2].

References

[1] K. Arumugam, “Behind the Cloud: Uncovering Critical Security Threats,” Jan. 2025, doi: 10.2139/ssrn.5160686.

[2] J. J. Ang’udi, “Security challenges in cloud computing: A comprehensive analysis,” World Journal of Advanced Engineering Technology and Sciences , vol. 10, no. 2, p. 155, Dec. 2023, doi: 10.30574/wjaets.2023.10.2.0304.

[3] F. K. Mupila, H. Gupta, and A. Bhardwaj, “Securing the Cloud: An In-depth Exploration of Conceptual Models, Emerging Trends, and Forward-looking Insights,” Research Square (Research Square) , Oct. 2023, doi: 10.21203/rs.3.rs-3448528/v1.

[4] A. Rathore, “A Security Assessment Framework Based on Cloud Technology: A Comprehensive Review,” International Journal for Research in Applied Science and Engineering Technology , vol. 12, no. 6. International Journal for Research in Applied Science and Engineering Technology (IJRASET), p. 1955, Jun. 28, 2024. doi: 10.22214/ijraset.2024.63424.

[5] Mrs. S. K. Totade, “Security Challenges in Cloud Computing,” International Journal for Research in Applied Science and Engineering Technology , vol. 12, no. 10, p. 1360, Oct. 2024, doi: 10.22214/ijraset.2024.64816.

[6] “BASELINE SECURITY REQUIREMENTS FOR CLOUD COMPUTING WITHIN AN ENTERPRISE RISK MANAGEMENT
FRAMEWORK,” Deleted Journal , p. 31, Apr. 2024, doi: 10.62304/ijmisds.v1i1.115.

[7] F. Edghiem and M. Abualqumboz, “Big Data HE Communities,” in Advances in business strategy and competitive advantage book series , IGI Global, 2021, p. 33. doi: 10.4018/978-1-7998-7513-0.ch003.

[8] J. O. OYENIYI and O. A. Oyeniran, “Optimizing Information Security In Cloud Environments: A Risk Management Approach And Guide For Enterprise Cloud Security,” Journal of Cybersecurity Education Research and Practice , vol. 2025, no. 1, May 2025, doi: 10.62915/2472-2707.1213.

[9] M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas, and S. U. Rehman, “Cyberattacks and Security of Cloud Computing: A Complete Guideline,” Symmetry , vol. 15, no. 11, p. 1981, Oct. 2023, doi: 10.3390/sym15111981.

[10] T. Ali, M. Al-Khalidi, and R. Al-Zaidi, “Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review,” Journal of Computer Information Systems , vol. 66, no. 1, p. 123, Mar. 2024, doi: 10.1080/08874417.2024.2329985.

[11] V. Raja, “Exploring Challenges and Solutions in Cloud Computing: A Review of Data Security and Privacy Concerns,” Deleted Journal , vol. 4, no. 1. p. 121, Apr. 30, 2024. doi: 10.60087/jaigs.vol4.issue1.p141.

[12] A. Miglo, “Crowdfunding Under Market Feedback, Asymmetric Information And Overconfident Entrepreneur,” Entrepreneurship Research Journal , vol. 11, no. 4, Feb. 2020, doi: 10.1515/erj-2019-0018.

[13] A. Miglo, “Crowdfunding Under Market Feedback, Asymmetric Information And Overconfident Entrepreneur,” SSRN Electronic Journal , Jan. 2017, doi: 10.2139/ssrn.3135095.

[14] A. Miglo, “Capital structure and earnings manipulation,” Journal of Economics and Business , vol. 62, no. 5, p. 367, May 2010, doi: 10.1016/j.jeconbus.2010.05.001.

[15] S. Shreyas, “Security Model for Cloud Computing: Case Report of Organizational Vulnerability,” Journal of Information Security , vol. 14, no. 4, p. 250, Jan. 2023, doi: 10.4236/jis.2023.144015.

[16] S. Ahmadi, “Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies,” Journal of Information Security , vol. 15, no. 2, p. 148, Jan. 2024, doi: 10.4236/jis.2024.152010.

[17] X. Zhang, N. Wuwong, H. Li, and X. Zhang, “Information Security Risk Management Framework for the Cloud Computing Environments,” p. 1328, Jun. 2010, doi: 10.1109/cit.2010.501.

[18] A. Alquwayzani, R. Aldossri, and M. Frikha, “Prominent Security Vulnerabilities in Cloud Computing,” International Journal of Advanced Computer Science and Applications , vol. 15, no. 2, Jan. 2024, doi: 10.14569/ijacsa.2024.0150281.

[19] A. K. Routh and P. Ranjan, “Uncovering Cloud Security Complexities-A Comprehensive Five-Perspective Taxonomic Review,” Research Square (Research Square) , Jun. 2024, doi: 10.21203/rs.3.rs-4506913/v1.

[20] M. Khomchak, “A Comprehensive Taxonomy of Modern Public Cloud Services for Infrastructure Selection,” International Journal of Computing , p. 468, Oct. 2024, doi: 10.47839/ijc.23.3.3667.

[21] A. A. Hadwer, M. Tavana, D. Gillis, and D. Rezania, “A Systematic Review of Organizational Factors Impacting Cloud-based Technology Adoption Using Technology-Organization-Environment Framework,” Internet of Things
, vol. 15. Elsevier BV, p. 100407, May 24, 2021. doi: 10.1016/j.iot.2021.100407.

[22] S. Islam, S. Fenz, E. Weippl, and C. Kalloniatis, “Migration Goals and Risk Management in Cloud Computing,” International Journal of Secure Software Engineering , vol. 7, no. 3, p. 44, Jul. 2016, doi: 10.4018/ijsse.2016070103.

[23] M. G. Raj and S. K. Pani, “A Meta-analytic Review of Intelligent Intrusion Detection Techniques in Cloud Computing Environment,” International Journal of Advanced Computer Science and Applications , vol. 12, no. 10. Science and Information Organization, Jan. 01, 2021. doi: 10.14569/ijacsa.2021.0121023.

[24] J. Uddoh, D. Ajiga, B. P. Okare, and T. D. Aduloju, “AI-Based Threat Detection Systems for Cloud Infrastructure: Architecture, Challenges, and Opportunities,” vol. 2, no. 2, p. 61, Jan. 2021, doi: 10.54660/.ijfmr.2021.2.2.61-67.

[25] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernández, “An analysis of security issues for cloud computing,” Journal of Internet Services and Applications , vol. 4, no. 1, p. 5, Jan. 2013, doi: 10.1186/1869-0238-4-5.

[26] H. Arif, A. Kumar, M. Fahad, and H. K. Hussain, “Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research,” International Journal of Multidisciplinary Sciences and Arts , vol. 2, no. 2, p. 242, Jan. 2024, doi: 10.47709/ijmdsa.v2i2.3452.

[27] R. Kalantri, “Advancing Cyber Threat Detection with Ai: Cutting-Edge Techniques and Future Trends,” Journal of Information Systems Engineering & Management , vol. 10, p. 338, Feb. 2025, doi: 10.52783/jisem.v10i14s.2301.

[28] K. Chitreddy, A. M. Anthony, C. M. Bandaru, and O. Abiona, “Information Security in the Cloud: Emerging Trends and Challenges,” International Journal of Communications Network and System Sciences , vol. 17, no. 5, p. 69, Jan. 2024, doi: 10.4236/ijcns.2024.175005.

[29] A. Mathew, “Securing the Cloud: Understanding Threats and Countermeasures,” International Journal for Research in Applied Science and Engineering Technology , vol. 12, no. 12, p. 3026, Mar. 2024, doi:
10.22214/ijraset.2024.59552.

[30] H. Azam et al. , “Innovations in Security: A Study of Cloud Computing and IoT,” International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence , vol. 2, no. 1,
Nov. 2023, doi:
10.54938/ijemdcsai.2023.02.1.252.

[31] Y.-W. Lin, “Hacker Culture and the FLOSS Innovation,” in IGI Global eBooks , IGI Global, 2011. doi: 10.4018/9781591409991.ch004.