International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 10 | Oct 2026 www.irjet.net p-ISSN: 2395-0072

Security Challenges in Multi-Cloud Environments: An Analysis of Threats, Vulnerabilities, and Mitigation Strategies

Tanisha Kamdar, Asst. Prof. Swati Kadu, Swarupa Vadam, Omkar Padwal

Master of Computer Applications, D Y Patil Schools of Humanities & Sciences, Navi Mumbai

---

Abstract - *The growing use of more than one cloud provider has led to the formation of multi-cloud environments, which have become an important part of modern IT infrastructure. Organizations choose different cloud providers to gain greater flexibility, scalability, and availability while reducing their dependence on a single provider. At the same time, securing a multi-cloud environment presents several challenges due to differences in security settings, identity and access management, monitoring, APIs, data protection, and compliance requirements. This paper explores the main security threats and vulnerabilities that may arise from the use of multi-cloud environments, such as identity-based attacks, cloud misconfigurations, insecure APIs, data exposure, and lack of visibility across the environment. In addition, common security practices for mitigating these threats are discussed, including multi-factor authentication, least-privilege access, Zero Trust security, encryption, continuous monitoring, and automated configuration management. Based on this analysis, the paper proposes implementing a unified security approach to improve the security and visibility of different cloud platforms.*

Key Words: Multi-Cloud Computing, Cloud Security, Security Threats, Security Vulnerabilities, Identity and Access Management, Zero Trust, Data Security, Security Management

1. INTRODUCTION

Cloud computing has gained importance in today's IT infrastructures and organizations use multiple cloud providers to satisfy their computing and storage requirements. This kind of setup is called multi-cloud computing and it offers advantages like flexibility, scalability, availability, and reduction in reliance on a single cloud provider. However, managing multiple cloud computing platforms which have different architectures and security settings may make it harder for organizations to maintain a consistent security environment.

The multi-cloud environment may have security issues like unauthorized access, misconfiguration, insecure API usage, identity-based attacks, and data exposure. Protection of data and identity management would also be hard because data and user access would exist in multiple clouds. It would thus be useful to understand multi-cloud architecture, security threats and vulnerabilities, and challenges faced in protecting data and managing identities.

2. OBJECTIVES AND RESEARCH QUESTIONS

The study has three objectives: (1) To investigate the architecture and features of multi-cloud systems, which include their design, advantages, and usage of different cloud service providers; (2) To determine possible security risks in multi-cloud systems, which may include configuration issues, unauthorized access, data breaches, and insecure application programming interfaces (APIs); (3) To examine the challenges of data protection and identity management in multiple cloud platforms, which include access control, authentication, encryption, and privacy.

Research questions: RQ1: What are the important architectural aspects of multi-cloud architectures, and what are their advantages? RQ2: What are the important security risks and vulnerabilities in multi-cloud architectures? RQ3: What are the issues involved with data protection and identity management in multi-cloud architectures?

3. LITERATURE REVIEW

Recent studies have highlighted several security challenges in multi-cloud environments, particularly related to data security, authentication, authorization, privacy, and interoperability. A systematic literature review identified data security, cryptography, authentication, and authorization as major concerns in multi-cloud environments.

Data leakage and privacy are significant concerns because organizations store and transfer data across multiple cloud platforms with different security policies and controls. Existing research suggests that encryption, access control, and secure data management can help reduce these risks.

Identity and access management is another important challenge. NIST's Zero Trust Architecture guidance recommends identity-based authentication and authorization for cloud-native applications operating across multi-cloud environments. This approach reduces

reliance on traditional network boundaries and supports more controlled access to cloud resources.

Existing studies also discuss threats such as misconfiguration, unauthorized access, data breaches, denial-of-service attacks, and vulnerabilities in cloud interfaces. Various mitigation techniques, including encryption, multi-factor authentication, Zero Trust, continuous monitoring, and security automation, have been proposed to address these threats.

4. METHODOLOGY

This research is based on a qualitative study of existing literature related to security in multi-cloud environments. Information was collected from research papers, journals, technical articles, and trusted sources such as IEEE Xplore, ScienceDirect, Springer, Google Scholar, and NIST.

For the literature search, keywords such as "multi-cloud security," "cloud security threats," "multi-cloud vulnerabilities," "security mitigation strategies," and "Zero Trust in multi-cloud" were used. The selected studies were then reviewed and grouped into three main areas: security threats, vulnerabilities, and security measures.

After reviewing the studies, the information was compared to understand the common security problems faced by organizations using multiple cloud providers. The existing security solutions and their limitations were also studied. This helped in identifying the main research gaps and understanding which security practices can be useful for protecting multi-cloud environments.

5. FINDINGS AND ANALYSIS

The study shows that security can become more difficult to manage when an organization uses more than one cloud provider. Different providers have different security settings, policies, tools, and ways of managing access. Because of this, organizations may face problems such as data breaches, data leakage, wrong configurations, unauthorized access, API vulnerabilities, and denial-of-service attacks.

One of the main concerns found in the reviewed studies is identity and access management (IAM). Users and applications may need to access resources from different cloud platforms. If access rules are not properly managed across these platforms, unauthorized users may get access to resources they should not be able to use.

Data protection is another important concern. Data may be stored in different cloud platforms or transferred from one provider to another. This makes it important for organizations to have proper security controls in place wherever the data is stored or transferred.

The studies reviewed in this research commonly suggest the use of encryption, multi-factor authentication (MFA), Zero Trust Architecture, access controls, and continuous monitoring. These methods can improve security, but using them in the same way across different cloud providers can be challenging.

Overall, the findings show that there is no single security solution that can completely protect a multi-cloud environment. Organizations need to use several security measures together and continuously monitor their cloud resources.

Table 1: Threat Mitigation Analysis

Threat	Related Vulnerability	Mitigation Strategy
Data Leakage	Weak data protection and insecure data transfer	Encryption, DLP, secure data transfer
Unauthorized Access	Weak IAM and stolen credentials	MFA, RBAC, Zero Trust
Misconfiguration	Inconsistent cloud security settings	CSPM, security audits, standardized policies
API Attacks	Insecure APIs and interfaces	API authentication, authorization, API monitoring
DDoS Attacks	Resource and availability weaknesses	DDoS protection, traffic monitoring, rate limiting
Insider Threats	Excessive privileges or misuse of access	Least privilege, IAM, activity monitoring
Lack of Visibility	Different monitoring systems across providers	Centralized logging, SIEM, continuous monitoring
Data Loss	Inadequate backup and recovery mechanisms	Regular backups, disaster recovery, data redundancy

6. DISCUSSION

Securing a multi-cloud environment is more complicated than managing security in a single-cloud environment. When an organization uses different cloud providers, it has to deal with different platforms, security settings, policies, and access methods. This can make it harder to identify and manage issues such as misconfiguration, unauthorized access, data exposure, and lack of visibility.

The findings from this study are similar to what has been discussed in previous research. Identity management, authentication, authorization, and data protection are repeatedly identified as important security areas. Measures such as MFA, encryption, Zero Trust, and continuous monitoring can help reduce these risks.

However, implementing a security tool alone does not guarantee proper protection. The security settings need to be configured correctly and maintained across all cloud platforms. If one cloud environment has weaker controls than the others, it can still create a security risk for the overall infrastructure.

Another important point is that organizations cannot rely on one security method to handle every type of threat. Different controls need to work together. Proper identity management, access control, data protection, monitoring, and regular security checks are all important parts of a multi-cloud security strategy.

Better coordination between cloud platforms can also help organizations get a clearer view of their overall security situation. Centralized monitoring and common security policies can make it easier to identify problems and respond to them quickly.

7. SECURITY IMPLEMENTATION CHALLENGES

Application of security solutions in multi-cloud infrastructure is a task with a set of difficulties that arise due to the diversity of cloud providers, security solutions, and security policies. First, the challenge is related to the complexity of integration, which may cause the difficulties with centralized management of security solutions. Insecure security policies may result in configuration errors and breaches in security. Moreover, the cost of security solutions and lack of specialists are the factors that affect the implementation process negatively. Lack of visibility and monitoring of multi-platform environment leads to delays in threat detection and incident management. The challenges mentioned above demonstrate the necessity of a unified security solution, which will allow implementing consistent security policies, centralizing the monitoring, and conducting automatic security assessment.

8. RESEARCH GAP

Although existing studies cover individual security threats and mitigation techniques, there is still a need for an integrated analysis of threats, vulnerabilities, and mitigation strategies specifically in multi-cloud environments. Different cloud providers may use different security mechanisms, making consistent security enforcement and centralized monitoring difficult. Therefore, this research focuses on analyzing major multi-cloud security challenges and evaluating suitable mitigation strategies for improving security across heterogeneous cloud platforms.

9. PROPOSED SOLUTION

To address security risks in multi-cloud computing environment, companies can opt for a holistic security strategy that offers continuous security in different cloud environments. A robust identity and access control through multi-factor authentication, role-based access control and least privilege principle can be a good starting point. For data protection, companies can rely on data encryption, secure key management, and data backup while configuration risk mitigation can be achieved by performing regular configuration assessments, secure API authentication and security testing. In addition, companies can consider centralized logging of security events from different cloud providers and automate security policies and compliance requirements. Such strategies can offer a structured solution to minimize security risks in multi-cloud computing environments. Nevertheless, further practical application and evaluation of such solutions are necessary.

10. CONCLUSION

Multi-cloud environments give organizations the freedom to use services from different cloud providers and can provide benefits such as flexibility and scalability. However, using multiple platforms also creates additional security challenges. This study found that data leakage, misconfiguration, unauthorized access, identity management, and limited visibility are some of the important concerns in multi-cloud environments.

The findings show that protecting a multi-cloud environment requires several security measures to work together. Encryption, MFA, proper access control, Zero Trust Architecture, and continuous monitoring can help organizations reduce security risks. However, applying these controls properly across different cloud providers can still be difficult because each provider may have different security features and policies.

For this reason, organizations should not treat each cloud platform as a completely separate environment. Instead, they should follow a common security approach and maintain proper visibility across all platforms. Regular monitoring and security assessments can also help identify problems before they become serious incidents.

Overall, multi-cloud security is not only about using security tools. It also depends on how well an organization manages users, permissions, data, policies, and monitoring across all its cloud environments. A well-coordinated approach can help organizations protect their data and

resources while making their multi-cloud infrastructure more secure and reliable.

REFERENCES

1) D. C. Diningrat, Suhardi, and B. Rahardjo, "Security Issues in Multi-Cloud: A Systematic Literature Review," IEEE Access, vol. 13, pp. 70006–70017, 2025, doi: 10.1109/ACCESS.2025.3561352.

2) S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2020, doi: 10.6028/NIST.SP.800-207.

3) W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," NIST Special Publication 800-144, National Institute of Standards and Technology, Gaithersburg, MD, USA, Dec. 2011, doi: 10.6028/NIST.SP.800-144.

4) P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, National Institute of Standards and Technology, Gaithersburg, MD, USA, Sep. 2011, doi: 10.6028/NIST.SP.800-145.

5) Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing v5, Cloud Security Alliance, 2024.

6) L. Megouache, A. Zitouni, and M. Djoudi, "Ensuring user authentication and data integrity in multi-cloud environment," Human-centric Computing and Information Sciences, vol. 10, art. no. 15, 2020, doi: 10.1186/s13673-020-00224-y.

7) M. Kumar, C. Maple, and S. Chand, "An efficient and secure identity-based integrity auditing scheme for sensitive data with anti-replacement attack on multi-cloud storage," Journal of King Saud University Computer and Information Sciences, vol. 35, no. 9, art. no. 101745, 2023, doi: 10.1016/j.jksuci.2023.101745.

8) A. Musa, A. Yeboah-Ofori, A. Jafar, T. Abisogun, I. Hilton, and W. Oseni, "Data security and governance in multi-cloud computing environment," in Proc. 11th International Conference on Future Internet of Things and Cloud (FiCloud), 2024, pp. 215–222, doi: 10.1109/FiCloud62933.2024.00040.

9) J. C. John, S. Sural, and A. Gupta, "Attribute-based access control management for multicloud collaboration," Concurrency and Computation: Practice and Experience, vol. 29, art. no. e4199, 2017, doi: 10.1002/cpe.4199.

10) "Security and privacy in multi-cloud and hybrid cloud environments: Challenges, strategies, and future directions," Computers & Security, vol. 157, art. no. 104599, 2025, doi: 10.1016/j.cose.2025.104599.