IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 3, Ser. 3 (May. – June. 2025), PP 53-54
www.iosrjournals.org

Security Challenges and Solutions in Multi-Cloud Environments: A Comparative Study

Annoo
UGC
Contact email: ananyaannusmile@gmail.com

Abstract
The growing adoption of multi-cloud strategies by organizations introduces both flexibility and complexity in managing cloud services. While leveraging multiple cloud providers improves redundancy, performance, and cost optimization, it also amplifies security challenges such as data leakage, compliance inconsistency, and inter-cloud communication vulnerabilities. This paper conducts a comparative study of security mechanisms implemented by major cloud service providers (AWS, Microsoft Azure, and Google Cloud) in multi-cloud architectures. Using a mixed-method approach, including literature analysis and case studies, the paper evaluates identity and access management (IAM), data encryption, and security orchestration capabilities across platforms. The study identifies significant gaps in unified governance and proposes a framework for centralized policy enforcement. The findings aim to inform cloud architects and security professionals in designing resilient multi-cloud systems.

Keywords: Cloud Computing, Multi-Cloud, Security, Data Privacy, IAM

Date of Submission: 02-06-2025 Date of Acceptance: 12-06-2025

I. Introduction

Define cloud computing and multi-cloud.
Importance of cloud in modern IT infrastructure.
Highlight security concerns in a multi-cloud context.
Research objectives or questions.

II. Literature Review

Discuss existing research on:
- General cloud security.
- Security in single-cloud vs. multi-cloud.
- Industry case studies.

Highlight gaps your paper addresses.

III. Methodology

Type: Comparative analysis, case study, or experimental.
Data sources: Official documentation, whitepapers, or hands-on testing.
Evaluation criteria: IAM, encryption, policy enforcement, etc.

IV. Results

Tables/graphs comparing AWS, Azure, GCP.
Analysis of strengths/weaknesses in security.

V. Discussion

Implications of findings.
Recommendations for secure multi-cloud adoption.
Discuss limitations of your analysis.

VI. Conclusion

Recap the research.
Reinforce the contribution.
Propose future work (e.g., AI in cloud threat detection).

References

Use IEEE, APA, or the journal's required style.
Cite peer-reviewed sources, standards (NIST), and vendor whitepapers.