IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, November 2025
Impact Factor: 7.67

Security Challenges in Multi-Cloud and Hybrid-Cloud Environments

Tabish Khan and Faijal Khan
Computer Science and Applications
Sharda School of Engineering & Technology, Sharda University, Greater Noida

Abstract: *With the rapid adoption of cloud computing, organizations are increasingly leveraging multi-cloud and hybrid cloud environments to achieve operational flexibility, cost optimization, and enhanced service availability. A multi-cloud environment involves utilizing services from multiple cloud providers simultaneously, while a hybrid cloud integrates private and public cloud infrastructures to create a unified platform. Although these approaches offer significant benefits in terms of scalability, disaster recovery, and resource optimization, they also introduce complex security challenges that traditional cloud security models may not adequately address.*

In multi-cloud and hybrid cloud architectures, organizations must manage diverse security policies, ensure consistent identity and access management, and protect sensitive data across heterogeneous platforms. The expanded attack surface, increased interconnectivity, and reliance on third-party providers make these environments particularly vulnerable to threats such as data breaches, misconfigurations, insider attacks, account hijacking, and denial-of-service attacks. Furthermore, regulatory compliance becomes more challenging due to data residency and jurisdictional differences among cloud providers.

This paper explores the key security challenges in multi-cloud and hybrid cloud deployments, emphasizing data security, identity and access management, network security, and monitoring complexities. It also reviews current strategies and emerging solutions, such as unified security frameworks, automated compliance tools, and advanced encryption techniques, that can help organizations mitigate risks while maintaining the operational benefits of these cloud models. By identifying critical vulnerabilities and evaluating best practices, this study provides a comprehensive understanding of how organizations can secure multi-cloud and hybrid cloud infrastructures effectively.

Enterprises increasingly adopt multi-cloud and hybrid-cloud architectures to gain flexibility, avoid vendor lock-in, optimize costs, and improve resilience. However, the distributed nature of workloads across different public clouds and on-premises infrastructure significantly increases the complexity of securing the environment. This paper explores the key security challenges in multi-cloud and hybrid-cloud environments, reviews recent research from 2022 to 2025, and proposes practical solutions and implementation strategies. It also highlights future research directions for enhancing security, governance, and compliance, while maintaining cost-efficiency and operational agility. The study emphasizes a humanized and accessible explanation of technical concepts suitable for academic research and professional understanding..

Keywords: Multi-cloud security, hybrid-cloud security, Zero Trust, CNAPP, IAM, misconfiguration, data governance, cloud compliance

DOI: 10.48175/IJARSCT-30074