

Survey of Adoption Multi-Cloud Management and Monitoring in Various Sectors

Jyoti P. Bartakke¹, Ankush Kudale²

^{1,2}Sinhgad Institute of Management Savitribai Phule Pune University, Pune, India

¹jyotibartakke@hotmail.com, ²ankush.kudale@gmail.com

Peer Review Information	Abstract
Type: Article Received: 25 March 2026 Revised: 17 April 2026 Accepted: 26 May 2026 Published: 16 June 2026	Organizations are moving to multi-cloud systems to improve scalability, flexibility, and less dependency on a single provider as a result of the increasing popularity of cloud computing. However, the multiple platforms in multi-cloud environments faces difficulties for continuous security compliance, interoperability, unified management, and continuous monitoring. With an emphasis on security orchestration strategies, observability methodologies, and multi-cloud management frameworks. The survey explores multi-cloud adoption across multiple sectors, discussing its practical applications, implementation challenges, and strategic recommendations for organizations and practitioners. In industries including IT, Manufacturing, Retail, Healthcare, Finance, previous year's literature is examined and categorized according to architectural models, and sector-wise uptake. The main advantages and disadvantages of the available alternatives are highlighted in a comparative analysis. Additionally, the report highlights unresolved issues such as fragmented threat intelligence integration, limited automation, and interoperability constraints. This paper presents challenges, assesses sector-wise impacts, and offers practical recommendations for governance. This research provides practical guidance for organizations that aim to strengthen operational maturity in multi-cloud environments. Keywords: Cloud Adoption; Multi-Cloud Monitoring Challenges; Multi-Cloud Security Challenges; Multi-Cloud Computing; Complex Management; Complex Monitoring; Cloud Management; Cloud Security; Monitoring; Cost Optimization; Cloud Governance; Large Infrastructure; Interoperability.

How to Cite This Article

Bartakke, J. P., & Kudale, A. (2026). *Survey of adoption multi-cloud management and monitoring in various sectors*. Open Access International Journal of Science and Engineering, 9(6), 7–15

Introduction

Cloud computing is very popular nowadays. Many organizations adopt cloud computing to their organization for work. Cloud computing has changed organization by providing infrastructure and services that can be scaled as needed and accessed on demand. “Cloud computing use pay as u use “strategy. [1]cloud adoption has become more established, many organizations have moved from single cloud to using multi-cloud approaches they Uses Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).previous studies suggest that every nine in ten organizations now do their workloads across more than one cloud provider[2].

A multi-cloud approach can support service continuity, reduce dependencies on a single provider, meet regulatory requirements across any cloud, and allow teams to select specialized services when needed. Additionally, these advantages effects in increased operational complexity. Continued concerns include cost management, continuously security monitoring, dependable observability, and interoperability across diverse platforms [3].

Although multi-cloud systems are widely used, only over 25% of organizations employ specialist tools to manage them, indicating gaps in governance and daily operational maturity [4], various sector in Pune region, provides a useful setting for examining these challenges. Organizations in region this run a range of multi-cloud workloads across international markets and regulated sectors [5]. This paper addresses the following research questions:

1. What is the type of your organization?
2. What are your primary motivations for using multi-cloud computing?
3. How would you describe your current cloud computing usage patterns?
4. What challenges are you're currently facing in managing and securing your multi-cloud environment?
5. How do you currently manage your multicloud environment?
6. What level of visibility is required of your multi-cloud workloads and resources?
7. What methods and resources are you using to continuously manage compliance?
8. What are the main difficulties you face in maintaining and protecting multi-cloud environments?
9. How would you like to automate management tasks across multiple cloud platforms?
10. What are your requirements for cost optimization and resource utilization in your multi-cloud environment?
11. What are your requirements for real-time monitoring of your multi-cloud environment?
12. How would you like to be alerted about critical events and potential security threats in your multi-cloud environment?
13. What are your requirements for managing resource provisioning and utilization across your multi-cloud environment?
14. What are your requirements for securing your multi-cloud environment against unauthorized access and data breaches?
15. What key features are you looking for in a multi-cloud network monitoring tool?
16. Any other suggestions

Questionnaire Themes

Following figure no. 1 shows questionnaire themes here all question was mapped to a specific research objective. And after responses we have designed themes. Themes were divide challenges, benefits, and usage patterns in multi-cloud computing. These themes will be used for qualitative analysis.

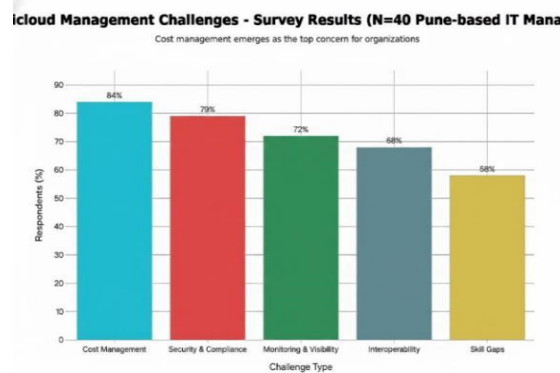


Fig. 1. Questionnaire Themes

This research in various sectors in Pune. Organizations who use multi cloud computing in their organizations send questionnaire through Google form and collect data.

1) What is type of your organization?
34 responses

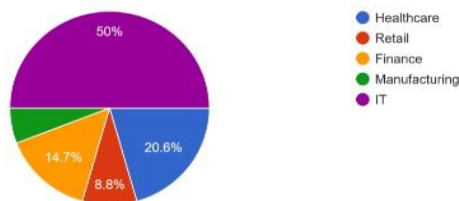


Fig. 2. Organization Types

Above figure no. 2 indicate the organization types that collected responses from Pune region various sectors organizations who uses multi-cloud. Involve 50% came from the IT sector, which suggests strong participation from an industry with high levels of cloud maturity. **Healthcare sector 20.6%** while the finance sector 14.7% with retail sector 8.8%. This survey shows supports analysis across industries that differ in their level of digital transformation and in how far they have progressed in adopting multicloud systems.

2) What are your primary motivations for adopting multi-cloud computing? (Select all that apply)
35 responses

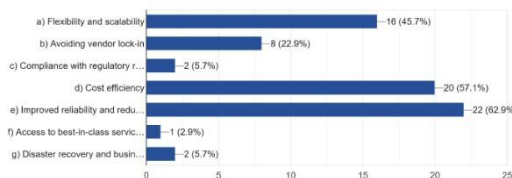


Fig. 3. Motivation of multi-cloud adoption

The figure no.3 shows the Survey data that organizations in Pune adopting multi-cloud environments for improve reliability and reduce risk (62.9%). and a cost-efficiency measure of 57.1%. Flexibility and scalability were assigned a score of 45.7% also appear as an important motivation, along with avoiding vendor lock-in 22.9% share plays a smaller, though still noticeable, role. Compliance, disaster recovery, and access to best-in-class services are cited less often as the main reasons for adoption.

3) How would you describe your current cloud computing usage patterns?
35 responses

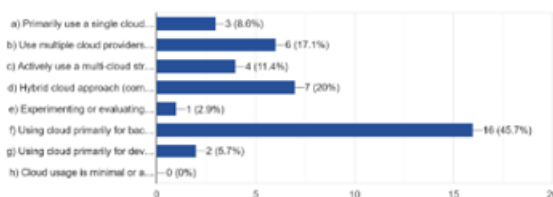


Fig. 4. Cloud usage types

Above figure no. 4 describes a survey of organizations in Pune found that the IT sector accounts for 50% of reported multi-cloud adoption, making it the most represented sector in the sample. Current cloud use is mainly for backup and disaster recovery, reported by 45.7% of respondents. Survey results indicate that rely on a single public cloud, while 20% use a hybrid cloud approach and 17.1% work with multiple providers without a defined strategy. The main reasons organizations adopt a multi-cloud approach are to improve reliability and to reduce risk (62.9%). The reported values were and cost efficiency at 57.1%. The first item accounted for, followed by flexibility and scalability at 45.7%.

4) What challenges are you currently facing in managing and securing your multi-cloud environment? (Select all that apply)
35 responses

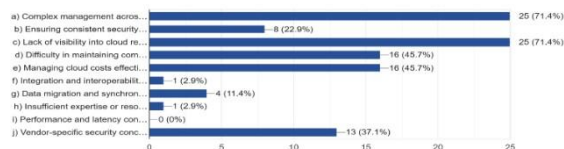


Fig. 5. Multi-cloud challenges

Above figure no. 5 indicates that, based on the analysis of the questionnaire responses, organizations across multiple sectors that have implemented multi-cloud computing are encountering several critical challenges, notably the complexity of management, increased operational costs, and limited visibility into cloud resources.



Fig. 6. Current Multi-Cloud Environment Management.

The figure no. 6 describes that many organizations, according to survey responses, manage their multi-cloud environments manually (based on requirements) or through collaboration with managed service providers. Cloud monitoring and analytics tools are also utilized by some organizations.



Fig. 7. Level of Multi-cloud Visibility

The figure no. 7 indicates level of multi-cloud visibility in organizations most often report a need for real-time monitoring of workload performance and system health (62.9%), along with a reported need for customizable dashboards (45.7%) while reported complete, aggregated visibility across all cloud environments.31.4% Cost-related insights accounted for 22.9% of the reported observations, suggesting that spending patterns were a recurring focus in the analysis target is preferred, operational performance remains the main priority. Security and compliance visibility (17.1%). The proportion is relatively low, and there is a clear need to integrate with existing tools. A value of 2.9% is low, which suggests that attention is centered on core, unified operational oversight.[6]

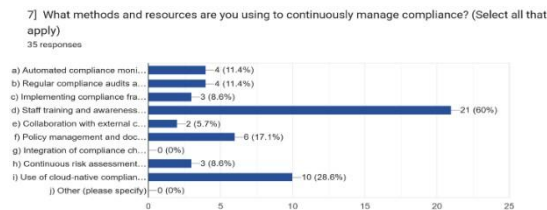


Fig. 8. Continuous Compliance Management Methods and Resources

The figure no. 8 indicates a survey response suggest that many organizations in different sectors manage compliance on an ongoing basis by providing staff training and running awareness programs. Some organizations rely on cloud-native compliance features offered by cloud providers

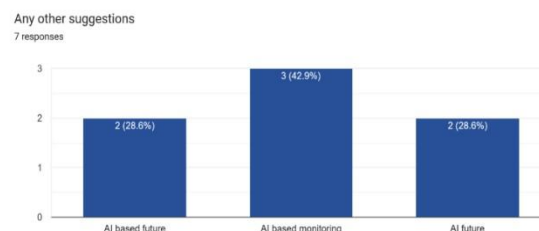


Fig. 9. AI based system

Above figure no.9 shows that several managers who took part in the survey suggested adding AI-based features to their monitoring tools.

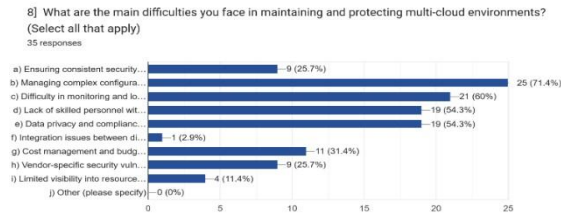


Fig. 10. Multi-cloud maintaining difficulties

This figure no.10 describes that many who adopting multi-cloud in organizations commonly face four main challenges when they seek to maintain and protect multi-cloud environments. The first is the difficulty of managing complex configurations and security policies across different cloud providers. The second is the challenge of monitoring system activity and collecting logs in a consistent way across multiple environments. The third is a shortage of staff with practical multi-cloud skills, which can slow incident response and day-to-day governance. The fourth involves data privacy and regulatory compliance, since rules may differ by location and data type, and responsibilities can be divided across providers and the organization.

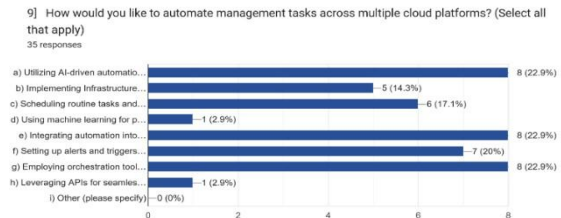


Fig. 11. Multi-Cloud Management Task Automation

The figure no. 11 describes that a survey responses suggest that many organizations are seeking AIdriven automation tools, automation integrated into CI/CD pipelines, and orchestration tools for resource management.

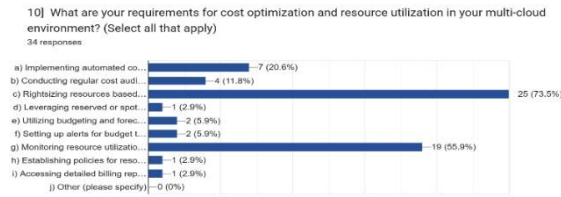


Fig. 12. Cost Optimization and Resource Utilization Requirements

Above figure no. 12 indicates that in this research survey any respondents across sectors reported that controlling costs in multi-cloud settings depends on matching resource size to actual demand. They stressed the value of tracking usage patterns and using real-time monitoring to identify resources that are overprovisioned or underused

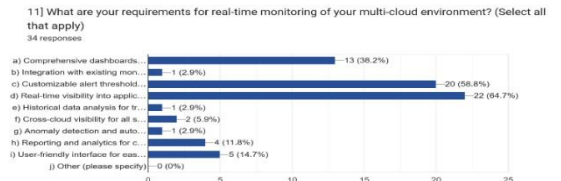


Fig. 13. Real -time monitoring approaches

This figure no.13 indicates requirements for real- time monitoring in multi-cloud environments, many organizations place clear priority on real-time monitoring capabilities. The central requirement is to obtain real-time visibility into the application’s performance and overall health. 64.7%, which suggests a need for immediate operational insights. Many respondents stressed the need to set alert thresholds that users can adjust for critical events, reported by 58.8% of participants. Which allows them to receive notifications that are timely and relevant.

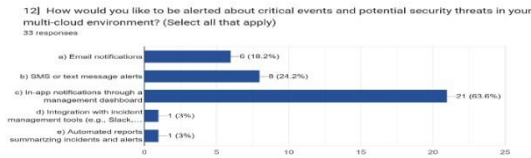


Fig. 14. Alert Events

This figure no. 14 shows that many organizations need integrated, real-time updates for critical alerts, with 63.6% of respondents reporting this requirement of respondents reported a preference for receiving in-app notifications through management dashboards. A smaller share of organizations chooses SMS, at about 24.2% email at 18.2%, respondents reported limited interest in external incident management tools or automated summary reports.

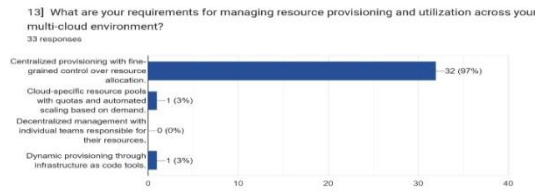


Fig. 15. Analysis of requirements resource provisioning

Analysis of the questionnaire responses indicates that most organizations need centralized provisioning and fine-grained control of resource allocation to manage resource provisioning and resource use across multi-cloud environments. The figure no.15 illustrate the same.

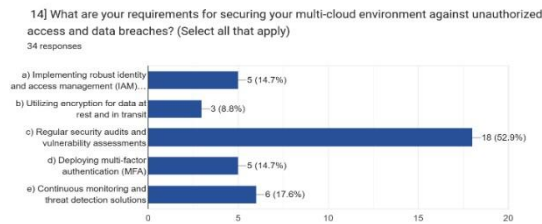


Fig. 16. Requirement for Security

The figure no.16 shows that currently most organizations requirements regular security audits and vulnerability assessments for securing multicloud environments against unauthorized access and data breaches

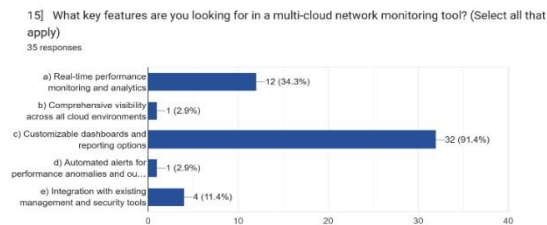


Fig. 17. Network monitoring tool approach

The figure no. 17 shows the survey results suggest that many organizations need multi-cloud network monitoring tools with customizable dashboards and a wide range of reporting features. For some organizations, real-time monitoring of performance and analytics is necessary

Multicloud Adoption and Deployment Models

Multi-cloud is using services from two or more cloud providers to run applications and store data. and hybrid cloud approaches that mix private and public infrastructure [12][13], a multi-cloud environment uses services from more than one public cloud provider and may also include edge or private resources.[4]. Three main deployment patterns are commonly observed:

A segmented multi-cloud approach assigns different applications to different cloud providers, based on factors such as cost or specific technical capabilities. Redundant multi-cloud refers to a setup in which the same workloads run in more than one cloud platform so that

services can stay available if one provider fails and recovery after an outage is faster [5]. Centralized multi-cloud term refers to describe a strategy where an orchestration layer distributes and relocates workloads among multi-cloud providers in response to current requirements.

This survey results from organizations in Pune suggest that the main reason for adopting a multicloud approach is to avoid vendor lock-in (95%). This Research survey shows challenges include cost optimization (88%), improving flexibility (82%), need more strict compliance (76%), and using specialize services from many providers (72%).[5]

Cost Management Challenges in Multi-Cloud Environments

This research survey indicates that cost management was the challenge, shown by 84% of respondents. Because multiple cloud providers depend on different pricing structures, billing methods, and discount policies, it is complex to obtain a single, view of costs across providers. Organization data indicates that almost half of cloud-related waste stems from limited visibility into costs.

In a multi-cloud environment, the main cost drivers are computing usage at 35%, multi-region storage at 28%, data egress charges at 18%, tooling licenses at 12%, and operational overhead at 7%.

In data-intensive fields such as healthcare and financial services, data egress charges can account for about 15–22% of total cloud spending.[7] Survey data indicate that 88% of organizations use a multi-cloud approach to reduce costs, only 31% report having formal FinOps practices. This gap is associated with excess provisioning, unclear ownership of spending, and weak budget forecasting. Organizations established FinOps initiatives claimed 20–30% cost savings. [8].

Security And Compliance Challenges

Multi-cloud adoption, each cloud has its own rules, compliance and security governance in a multi-cloud setup can be complex, because provider follows its own methods for identity management, data encryption, and compliance. so, maintaining uniform security controls and enforcing policies across platforms becomes complexities. In cloud security faulty configurations is main problem, and the risk increases with the number of identity systems [7].

This research survey respondents reported managing many of identity settings across multiple platforms, which makes enforcing least-privilege access difficult. Encryption is also fragmented, since each provider requires its own key management system. In many sectors, staff often report that preparing and maintaining compliance documentation takes about

15–25% of day-to-day operational work. Using multiple cloud provider can increase the attack surface because it introduces multiple APIs, more links between cloud environments, and credentials that may be shared across systems. In the financial services sample, 83% of respondents reported cross-cloud security incidents, which they most often linked to access policies that granted broader permissions than needed.[10]. There are issues in cloud computing security out of it authentication and access control is one of the key issues. [12]

Monitoring, Observability, And Visibility Challenges

Many organizations adopting multi-cloud computing in their workload have faced many challenges in because centralized visibility. Each cloud has their own rules so, monitoring tools built into cloud service providers often do not integrate across platforms, so teams must maintain separate monitoring systems. It is creating complexities. It also creates visibility gaps, particularly with regard to inter-cloud traffic and latency, and prolongs the time required to handle crises. Standardizing performance metrics across providers remains difficult because measurement methods vary and are not applied consistently. Organizations reported that it took about 3 to 6 months to set reliable performance baselines, which delayed planned improvement efforts. It is not possible to buy all that commercial observability platforms can provide a unified view of systems but often come with high costs, whereas open-source options usually demand dedicated engineering expertise to implement and maintain. Multi-cloud environments, where coordinated monitoring techniques are required to guarantee visibility and threat detection across multiple cloud platforms, real-time monitoring for network security does not address integrated monitoring and security management.[14]

Interoperability And Platform Integration Challenges

Multi-cloud providers many cloud Application Programming Interfaces, Software Development Kit, and service behaviour make it harder to move applications between providers and to build reliable automation. Many organizations depend on custom abstraction layers, which tends to increase both development workload and day-to-day operational complexity. Even with multi-cloud approaches in place, 64% of respondents said they still experienced vendor lock-in, mainly because they relied on proprietary services, faced pricing features that were hard to replace, and had in-house expertise concentrated in one provider.

Hybrid integration increases operational complexity, and many organizations report that 20–30% of cloud operations effort is spent connecting on-premises systems to multi-cloud environments. [6]

Sector -Wise Effect

IT sectors organizations is higher usability then other sectors, network demand, with peak events sometimes driving short-term increases of 10 to 100 times above normal levels. In Pune various sectors who adopted multi cloud computing in their organizations reported a value of 99. The system maintained 99% uptime, reduced costs by 28%, and lowered latency by 15–25% Increasing cybersecurity risks and complicated regulations challenge modern IT and cloud infrastructures. Healthcare organizations place priority on compliance and reliability. The main challenges include managing complex configurations, monitoring across multiple environments, and addressing the shortage of skilled staff.

Finance sectors, 14.7 % respondent use multi-cloud computing in their organization. Research show, multi-cloud strategies lowered recovery time objectives by as much as 40%, supporting system resilience while also meeting regulatory requirements.

Retail settings, the main challenges include managing complex configurations, monitoring across multiple environments, and addressing the shortage of skilled staff.

Manufacturing cost reduction work focuses on aligning staffing and equipment with demand and tracking resource use in real time. The survey sampled multi-cloud adopters based in Pune, with respondents drawn mainly from the IT sector (50%) and healthcare (20.6%), and Finance (14.7%), and Retail (8.8%)[7][8][8][9].Across sectors such as Manufacturing, the data suggest that organizations are mainly motivated by the need to improve reliability while reducing costs. Current use is often focused on backup and disaster recovery and on hybrid models, yet day-to-day management is still mostly handled manually or outsourced to managed service providers. Based on this research show that there is strong demand for real-time, centralized visibility and monitoring. This demand impacts the requirments for clear insights into application performance and for alert settings that can be adjusted to fit specific operational requirements. The main challenges is complex management configurations, complex monitoring across multiple environments, and addressing the lack of trained staff. Cost optimization efforts focus on rightsizing resources and real-time utilization monitoring. Previous research showed the use of 5G-enabled intelligent systems in facilitating real-time and distributed computing environments. Previous research showed the use of 5G-enabled intelligent systems in facilitating real-time and distributed computing environments. These features are important to multi-cloud designs, where continuous connectivity and minimal latency are essential for effective workload distribution, real-time monitoring, and inter-cloud coordination.[8]

Recommendations

Based on my survey I observed that still many challenges in adoption of multi-cloud. Multi-cloud management and monitoring workloads in multiple providers focus on clear governance policies, suitable tools for monitoring and control, and an organization that has the skills and processes to apply these consistently. For standardize governance framework requires policy as- code. Unified observability platforms that support visibility across multiple cloud environments. Allocate resources to develop DevOps [11] and cloud computing skills through structured training, supervised practice, and relevant certifications. zero-trust security effectively addresses cloud computing's security challenges by assuming no implicit trust and requiring continuous verification, outperforming traditional models. [13]

Conclusion

Multi-cloud computing is very popular often treated as a strategic requirement, but its value depends on clear governance and strong operational management across providers. Research survey shows that still gap in maturity between adopting the system and running it well in day-to-day practice. This research survey shows that the various sectors TI, Finance, Manufacturing, Retail, Healthcare still faces many challenges by adopting multi-cloud in their organizations. This paper outlines practical steps organizations can take to strengthen multicloud governance, limit risk, and improve return on investment. Adopt FinOps methods and invest in a unified observability platform to obtain the best value from multi-cloud use.

References

1. Bele, Prof. (2024). *Cloud Computing: Trends, Challenges, and Future Directions*. International Journal for Research in Applied Science and Engineering Technology, 12, 202–206. <https://doi.org/10.22214/ijraset.2024.64993>
2. Gosipathala, S. B. (2025). *Multi-Cloud Enterprise Architecture: A Comprehensive Framework for Hybrid Cloud Orchestration*. International Journal of Scientific Research in Engineering and Technology. <https://doi.org/10.32628/IJSRSET2512606>
3. Seth, D., Nerella, H., Najana, M., & Tabbassum, A. (2024). *Navigating the Multi-Cloud Maze: Benefits, Challenges, and Future Trends*. International Journal of Global Innovations and Solutions (IJGIS). <https://doi.org/10.21428/e90189c8.8c704fe4>
4. Schmidt, P. (2022). *Literature Review on Multi Cloud Management*. Seminar Paper, Fachhochschule Wedel, Germany.
5. Cloud Security Alliance. (2024). *The State of Multi-Cloud Identity Management Survey Report*. Retrieved from <https://cloudsecurityalliance.org/artifacts/the-state-of-multi-cloud-identity-survey>

6. Saxena, D., Gupta, R., & Singh, A. K. (2021). *A Survey and Comparative Study on Multi-Cloud Architectures: Emerging Issues and Challenges for Cloud Federation*. arXiv:2108.12831. <https://arxiv.org/abs/2108.12831>
7. Hope, O. S. (2023). *Multi-Cloud Strategy for Enterprise Applications: Cost, Performance, and Resilience Considerations*. *International Journal of Cloud Computing and Database Management*, 4(1), 63–73.
8. Bartakke, J. (2025). *The Future of Poultry Farming: Intelligent Aquaculture With 5G*. Vidhyayana, 10(si4). Available at: <http://www.vidhyayanaejournal.org/index.php/journal/issue/view/v10si4>
9. Kudale, A. (2025). *Blockchain Safeguards: Securing the Future of Kitchen Operations*. Vidhyayana, 10(si4). <https://doi.org/10.58213/bwezb546>
10. Kushala, M. V., & Shylaja, B. S. (2020). *Recent Trends on Security Issues in Multi-Cloud Computing: A Survey*. *Proceedings of ICOSEC 2020*.
11. Rios, E., Mallouli, W., Rak, M., Casole, V., & Ortiz, A. M. *SLA-Monitoring of Multi-Cloud Application Components Using the MUSA Framework*.
12. Kudale, A., & Hemalatha, S. (2021). *Cloud Computing: An Analysis of Authentication Methods Over Internet*. In M. S. Kaiser, J. Xie, & V. S. Rathore (Eds.), *Information and Communication Technology for Competitive Strategies (ICTCS 2020)*, *Lecture Notes in Networks and Systems* (Vol. 190). Springer, Singapore. https://doi.org/10.1007/978-981-16088-2-7_68
13. Bartakke, J., & Kashyap, D. R. (2024). *The Usage of Clouds in Zero-Trust Security Strategy: An Evolving Paradigm*. *Journal of Information and Organizational Sciences*, 48(1).
14. Kebande, V. R., Karie, N. M., & Ikuesan, R. A. (2021). *Real-Time Monitoring as a Supplementary Security Component of Vigilantism in Modern Network Environments*. *International Journal of Information Technology*, 13, 5–17. <https://doi.org/10.1007/s41870-020-00585-8>