

## Cloud Migration: Overcoming Challenges and Ensuring Successful Transition

Sai Krishna Adabala

USA

### ABSTRACT

Cloud migration has become a cornerstone of digital transformation for organizations looking to scale efficiently, reduce costs, and improve operational agility. By moving to the cloud, businesses can tap into flexible, on-demand resources to increase and stay competitive. However, the journey to the cloud is not without its challenges. Data security, regulatory compliance, cost control, and minimizing downtime are all significant concerns during migration. These challenges are especially critical in industries like healthcare, finance, retail, and manufacturing, where a poorly executed migration can lead to operational disruptions, security breaches, and even costly regulatory penalties. This paper examines these hurdles and offers a practical framework for navigating migration. It proposes a phased approach to migration that helps reduce risks and emphasizes the importance of robust data security measures—like encryption and multi-factor authentication—to protect sensitive information. The paper also discusses managing migration costs effectively, using cloud providers' tools to track and optimize spending. Finally, it underscores the need for strong collaboration between IT teams, cloud vendors, and business leaders to ensure a smooth and successful transition. Drawing on real-world case studies, this paper offers actionable insights to help organizations overcome migration challenges, maximize the benefits of the cloud, and set themselves up for long-term success.

### \*Corresponding author

Sai Krishna Adabala, USA

**Received:** January 05, 2024; **Accepted:** January 08, 2024; **Published:** January 20, 2024

**Keywords:** Migration, Cloud Computing, Legacy Systems, Hybrid Architecture, Downtime

### Introduction

Cloud migration is a cornerstone of modern business strategies as organizations shift their operations from on-premise systems to cloud-based platforms. Cloud computing has revolutionized how companies manage their IT infrastructure, offering numerous advantages such as scalability, flexibility, cost efficiency, and enhanced collaboration. By leveraging the power of the cloud, businesses can optimize their resource utilization, streamline processes, and scale their operations rapidly to meet the evolving demands of the digital age. Cloud adoption has seen a sharp rise across industries, with sectors such as healthcare, finance, retail, and government leading the charge due to the immense potential for improved service delivery, innovation, and competitive advantage [1].

However, despite its promising benefits, cloud migration is far from straightforward. The transition from legacy on-premise infrastructure to cloud environments is complex and involves a series of significant challenges that require careful planning and execution. Organizations must address several critical factors to migrate their data, applications, and workloads successfully. These challenges include maintaining data security during the transfer, ensuring compliance with industry-specific regulations, managing the costs associated with migration, and minimizing downtime to avoid disruptions in business operations [2].

One of the most pressing concerns in cloud migration is data security. Organizations must protect sensitive data as it moves

from on-premise systems to cloud environments, often perceived as more vulnerable to cyberattacks and breaches. With increasing regulations around data privacy, especially in sectors like healthcare and finance, ensuring that data is secure both during and after migration is critical [2]. Regulatory compliance also plays a significant role, as strict data storage and protection standards bind industries such as healthcare, banking, and insurance. For example, healthcare organizations must comply with the Health Insurance Portability and Accountability Act (HIPAA). At the same time, financial institutions must adhere to the General Data Protection Regulation (GDPR) and other local compliance laws. Failure to meet these standards could result in legal repercussions, financial penalties, and reputational damage [3].

Another significant challenge is cost management, which often surprises organizations during migration. Cloud migration can be expensive, especially if not properly planned and executed. Costs can quickly escalate due to data transfer fees, storage costs, and resource allocation. The migration process often takes longer than expected, leading to further unanticipated expenses. Effective cost management is essential to ensure that the migration stays within budget and that the long-term benefits of cloud computing outweigh the initial investment. Therefore, organizations must utilize cloud providers' cost-management tools, which help monitor and control expenses throughout the migration process [4].

Moreover, downtime during migration can have severe implications on business continuity. When migrating critical applications or systems, even a small amount of downtime can disrupt operations, leading to a loss of productivity, customer dissatisfaction, and, in extreme cases, financial losses. Minimizing downtime requires

meticulous planning and coordination between cloud providers, internal IT teams, and external stakeholders to ensure a seamless transition.

In addition to these primary concerns, integrating legacy systems into cloud environments presents a further complication, especially for industries with complex IT infrastructures and highly customized applications. While some organizations may opt to re-engineer or rebuild their systems for the cloud entirely, many prefer to find ways to integrate legacy systems with new cloud-based technologies. Solutions like containerization and application programming interfaces (APIs) have been widely adopted to adapt existing systems and ensure compatibility with cloud services [5].

This paper thoroughly explores these challenges by analyzing real-world case studies across various healthcare, finance, and retail sectors. Through the lens of these case studies, we aim to highlight common obstacles faced during cloud migration and discuss the strategies and best practices that organizations have successfully employed to overcome them. By synthesizing these lessons learned, we propose a comprehensive framework for successful cloud migration, focusing on critical aspects such as risk mitigation, security protocols, cost management, and downtime reduction. Additionally, the paper will provide actionable insights into the importance of collaboration between business leaders, IT professionals, and cloud service providers to ensure alignment and success throughout the migration journey.

By the end of this paper, readers will have a clearer understanding of the complexities involved in cloud migration and the practical solutions that can be implemented to overcome these challenges. Our findings are aimed at helping organizations navigate the cloud migration process with greater confidence and efficiency, ensuring that they are well-equipped to leverage the full potential of cloud technologies while minimizing risks and disruptions. However, to harness the full potential of cloud computing, organizations must address several critical challenges during the migration process.

### Key Challenges in Cloud Migration

Cloud migration offers significant benefits, such as enhanced scalability, flexibility, and cost efficiency. However, the transition from on-premise infrastructure to cloud environments is challenging. These challenges can vary by industry, but common obstacles include data security, regulatory compliance, cost management, downtime, and legacy system integration. Below, we discuss organizations' primary challenges and propose strategies for overcoming them [6].

### Data Security and Privacy Concerns

Data security is a critical concern during cloud migration. Moving sensitive data to remote cloud servers introduces new vulnerabilities, such as cyberattack exposure, unauthorized access, and data breaches. These risks are heightened in healthcare, finance, and government industries, where stringent regulations govern data protection and privacy [6].

To mitigate these risks, organizations should implement a multi-layered security approach. This includes:

- **End-to-End Encryption:** Ensuring data is encrypted during transfer and stored in the cloud.
- **Access Controls:** Enforcing secure access policies, including multi-factor authentication (MFA), to limit unauthorized access.
- **Continuous Monitoring:** Monitoring cloud environments for potential threats in real-time to detect and respond to security incidents promptly.

Additionally, organizations should select cloud providers that comply with industry-recognized security certifications (e.g., ISO 27001, SOC 2) and adhere to regulatory standards such as HIPAA or GDPR. Proactive risk management and collaboration with cloud vendors on security measures can significantly reduce the likelihood of data breaches and regulatory violations.

### Regulatory Compliance

Adhering to regulatory requirements is another major challenge in cloud migration. Regulations such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI-DSS) impose strict guidelines on how data should be stored, accessed, and processed.

Migrating data across borders becomes more complex as countries have varying laws and regulations regarding data residency, privacy, and processing. Non-compliance can lead to legal penalties, reputational damage, and customer distrust [7].

### To ensure compliance, organizations should:

- **Engage Legal and Compliance Teams:** Collaborate with internal legal teams to understand industry-specific regulations and incorporate these requirements into the migration strategy.
- **Work with Certified Cloud Providers:** Ensure cloud vendors provide infrastructure that meets necessary compliance standards, including data residency options and certifications.
- **Regular Audits:** Conduct regular audits and security assessments to confirm that data handling processes remain compliant throughout the migration and beyond.

A thorough understanding of applicable regulations and close coordination with cloud providers is crucial to ensuring migration efforts comply with legal and industry standards.

### Cost Management and Budget Control

Cloud migration is often perceived as a cost-saving initiative but can result in unexpected expenses if not appropriately managed. Costs related to data transfer, storage, and additional cloud resources can quickly escalate, mainly when organizations underestimate or fail to account for hidden expenses like data egress fees, scaling resources during migration, or over-provisioning cloud services [8].

### To control migration costs, organizations should:

- **Adopt a Phased Migration Approach:** Start by migrating less critical applications to the cloud, allowing for testing and fine-tuning of the migration process. This also helps to identify and address unforeseen costs early [8].
- **Utilize Cost Management Tools:** Leverage cloud cost management tools such as AWS Cost Explorer, Azure Cost Management, or Google Cloud's Cost Management tools to monitor usage and adjust resource allocation in real-time [8].
- **Optimize Resource Provisioning:** Use cloud providers' cost calculators to estimate migration expenses and avoid over-provisioning accurately. Reserve instances for long-term workloads where applicable to save on costs [9].

By carefully planning and monitoring costs, organizations can avoid budget overruns and ensure that cloud migration leads to long-term cost savings.

### Operational Downtime and Business Continuity

Operational downtime during cloud migration is a significant concern, especially for businesses that rely on continuous availability. Even brief service disruptions can negatively impact

productivity, customer experience, and revenue generation [5].

To minimize downtime, organizations should:

- **Adopt a Hybrid Cloud Strategy:** First, migrate non-critical systems, test migration procedures, and ensure mission-critical applications remain operational. Hybrid models, where some applications remain on-premises while others move to the cloud, can help ensure business continuity.
- **Create Detailed Migration Plans:** Develop comprehensive plans with clearly defined timelines, milestones, and contingency strategies. This includes identifying risks and establishing backup systems to restore services quickly [5].
- **Implement Backup and Recovery Solutions:** Ensure that reliable disaster recovery systems are in place to restore critical data and services in case of migration failures or disruptions.

Thorough planning and careful execution can significantly reduce the risk of downtime, ensuring that business operations continue without significant disruption during the migration process.

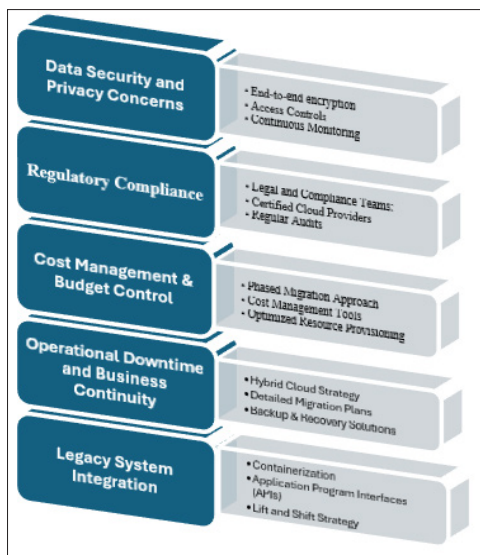
### Legacy System Integration

Integrating legacy systems with cloud environments presents a unique set of challenges. Many legacy applications were built for on-premise environments incompatible with modern cloud architectures. Migrating these systems to the cloud often requires significant re-engineering or replacement [10].

Organizations can address this challenge through:

- **Containerization:** Containerizing legacy applications allows them to run in cloud environments without needing to be fully re-engineered. Containers package the application and its dependencies, ensuring portability across different cloud platforms.
- **Application Programming Interfaces (APIs):** APIs enable seamless communication between legacy systems and cloud services, facilitating data exchange without requiring complete infrastructure overhauls.
- **Lift-and-Shift Strategy:** For some organizations, a "lift-and-shift" approach—where legacy systems are directly moved to the cloud with minimal modification—can be a practical option, especially if re-engineering is not feasible in the short term.

By using these strategies, organizations can integrate legacy systems into the cloud environment and ensure they continue functioning without significant disruptions during the migration.



### Methodology

This study employs a mixed-methods approach, combining qualitative and quantitative research techniques to comprehensively understand the cloud migration process. The methodology is designed to identify common challenges, strategies for overcoming them, and best practices that lead to successful cloud adoption. The approach includes a thorough literature review, interviews with industry professionals, and case study analysis across various sectors. These methods are outlined below:

### Literature Review

The literature review forms the foundation of this research, providing insights into existing academic research, industry reports, and case studies on cloud migration. A thorough review of publications, including peer-reviewed journal articles, white papers, and government reports, was conducted to identify critical challenges and best practices in cloud migration. This helped inform the development of the research framework and guided the formulation of interview questions and case study selection. Key topics explored in the literature included:

- Cloud migration trends and adoption rates across industries.
- Common challenges organizations face when transitioning to the cloud (e.g., data security, regulatory compliance, cost management).
- Effective strategies for overcoming migration obstacles.
- Industry-specific solutions and innovations related to cloud adoption.

### Interviews with Industry Professionals

In-depth interviews were conducted with IT professionals, business leaders, and decision-makers from organizations that had recently undergone cloud migration. These interviews aimed to gather firsthand accounts of the challenges faced during the migration process and explore the strategies used to overcome them. Participants in the interviews were selected from a range of industries, including:

- **Healthcare:** Organizations migrating Electronic Health Records (EHR) and patient data to comply with HIPAA regulations.
- **Finance:** Financial institutions are transitioning payment systems, customer data, and back-office applications to the cloud while adhering to stringent regulations such as GDPR.
- **Retail:** E-commerce platforms moving to the cloud to enhance scalability and support online operations during peak shopping seasons.
- **Manufacturing:** Manufacturing companies integrate IoT-based systems and enterprise resource planning (ERP) software into the cloud to improve production efficiency and data analytics capabilities.

The qualitative data collected through these interviews provided valuable insights into the real-world challenges organizations face and the practical solutions that work for them. These insights were used to refine the research framework and validate key findings.

### Case Study Analysis

The case study analysis is a core component of this research, providing a detailed look at real-world cloud migration experiences across multiple sectors. Several case studies were selected based on their relevance to the study's objectives and their representation of different stages of the migration process—from planning and execution to post-migration optimization. The industries covered in the case studies include healthcare, finance, retail, and manufacturing, as these sectors face unique challenges when migrating to the cloud.

Some of the organizations included in the case study analysis are:

- **Healthcare:** One of the most extensive nonprofit health plans in the US, Kaiser Permanente, faced the challenge of migrating sensitive patient data while ensuring compliance with HIPAA regulations. The case study explores their phased approach to migrating Electronic Health Records (EHR) and using encryption and multi-factor authentication (MFA) to protect patient data during the migration. Additionally, the case examines the integration of cloud-based telemedicine solutions to expand their digital healthcare offerings [11].
- **Finance:** Despite its vast scale—over 300,000 employees across more than 100 countries—JPMorgan Chase & Co., the world's largest bank, migrated a significant portion of its data and applications to the cloud as part of its digital transformation strategy. This migration was complicated by the need to adhere to financial regulations, such as GDPR and the Dodd-Frank Act. The case study highlights the tools JPMorgan used to monitor cloud costs and optimize resource allocation and their efforts to ensure data privacy and security during the transition [12].
- **Retail:** Walmart's cloud migration efforts were driven by the need to scale its e-commerce platform and improve inventory management across its vast retail network. The case study examines Walmart's hybrid cloud strategy, allowing them first to migrate non-critical applications and gradually move to a fully integrated cloud environment. It also explores the use of containerization to integrate legacy systems with cloud-based solutions [13].
- **Manufacturing:** General Electric (GE), a global leader in industrial manufacturing, migrated to the cloud to adopt IoT technologies and leverage data analytics for predictive maintenance in their equipment and machinery. The case study discusses GE's challenges in integrating legacy equipment with new cloud platforms and how containerization and API-based solutions helped bridge the gap between old and new systems [14].

These case studies identified common migration obstacles like security, regulatory compliance, and integration challenges. We also observed successful strategies and tools organizations across different sectors have used to overcome these barriers. For example, adopting hybrid cloud models in the healthcare and retail sectors helped mitigate downtime and ensure business continuity during migration. At the same time, advanced cost management tools allowed organizations to control expenses better during the transition.

### Data Synthesis

The data gathered from the literature review, interviews, and case studies were synthesized to identify best practices and develop a comprehensive framework for successful cloud migration. Key findings were categorized by challenge type (e.g., security, cost, downtime) and the most effective solutions for each issue. These solutions were actionable recommendations for organizations embarking on cloud migration journeys.

The synthesis also included a cross-industry comparison to highlight sector-specific solutions. For example, financial institutions and healthcare organizations emphasized the importance of regulatory compliance tools and certifications, while retail and manufacturing sectors focused on scalability and legacy system integration solutions.

### Discussion

Cloud migration offers organizations significant advantages, including scalability, cost efficiency, and operational agility. However, the transition to cloud-based systems is fraught with challenges that require meticulous planning, careful execution, and strong collaboration across teams. Below, we discuss the primary obstacles organizations face during migration and offer strategies to overcome them.

### Data Security and Compliance

Data security is one of the most critical concerns during cloud migration, particularly for industries such as healthcare, finance, and government, where strict regulations govern the handling of sensitive data. Migrating data to the cloud introduces risks of unauthorized access, breaches, and non-compliance with industry standards, which can result in financial penalties, legal repercussions, and damage to customer trust.

To address these risks, organizations must adopt a **proactive security strategy** that includes:

- **Partnering with cloud providers** that comply with recognized security certifications such as **ISO 27001** or **SOC 2**.
- **Implementing end-to-end encryption** to safeguard data both in transit and at rest.
- **Enforcing multi-factor authentication (MFA)** for users accessing sensitive systems.
- Conducting **regular security audits** to identify vulnerabilities and address them promptly.

By adopting these measures, organizations can mitigate the risks associated with cloud migration and ensure compliance with regulatory frameworks such as **HIPAA** in healthcare and **GDPR** in finance.

### Cost Management

A common challenge in cloud migration is cost overruns, which can occur when organizations must account for hidden costs like data transfer fees, storage charges, or unanticipated resource consumption. These expenses can quickly exceed the initial migration budget, undermining the long-term cost savings that cloud adoption promises [8].

To avoid budget overruns, organizations should:

- **Develop a comprehensive cost forecast** before migration, including potential hidden fees.
- **Monitor cloud expenses in real time** using cost management tools provided by cloud platforms (e.g., **AWS Cost Explorer** or **Azure Cost Management**).
- **Adopt a phased migration approach**, starting with less critical workloads to test cost assumptions and refine strategies.
- **Leverage cost-effective pricing models** such as reserved instances or committed use discounts, which can provide substantial savings over time.

A clear focus on cost management ensures that migration projects remain within budget and that the transition to the cloud delivers the anticipated financial benefits.

### Downtime and Service Disruption

Operational downtime is one of the most significant risks during cloud migration, particularly for businesses with critical, 24/7 operations. Even short disruptions can lead to loss of productivity, customer dissatisfaction, and reputational damage. Minimizing downtime is essential for ensuring business continuity.

### To mitigate downtime, organizations can:

- **Adopt a phased migration strategy**, migrating non-critical systems first to test the process and address potential issues before migrating mission-critical applications.
- **Implement a hybrid cloud approach**, where some systems remain on-premises during migration. This can provide additional stability and reduce the risk of service disruptions.
- **Prepare detailed migration and backup plans**, including contingency measures for potential failures and a clearly defined recovery process.

By taking these steps, businesses can reduce the risk of service disruption and ensure a smoother, more predictable migration process.

### Legacy System Integration

Integrating legacy systems with cloud environments is a significant challenge for many organizations, particularly those with complex, customized, or outdated IT infrastructures. Legacy applications may not be designed for cloud environments, requiring significant re-engineering, which can be costly and time-consuming.

To address this challenge, organizations can:

- **Use containerization** to package legacy applications and their dependencies into portable containers, enabling them to run on any cloud platform without requiring significant changes to the underlying code.
- **Implement application programming interfaces (APIs)** to enable seamless communication between legacy and cloud systems, facilitating data exchange and integration without requiring complete system rewrites.
- **Adopt a hybrid architecture** where legacy systems continue to operate alongside cloud-based solutions, ensuring compatibility and smooth data flow between the two environments.
- By leveraging containerization and APIs, organizations can more easily integrate legacy systems into the cloud, preserving valuable investments in older technologies while taking advantage of the cloud's scalability and flexibility.

### Findings and Recommendations

Based on the analysis of case studies and industry practices, several key findings and actionable recommendations emerge to guide organizations through a successful cloud migration journey:

#### Data Security and Compliance

Data breaches during migration are a significant risk, particularly in highly regulated sectors such as healthcare and finance.

**Recommendation:** Organizations should partner with cloud providers that comply with industry standards like ISO 27001, HIPAA, and GDPR. In addition, implementing encryption, multi-factor authentication (MFA), and continuous security monitoring throughout the migration process is essential to protect sensitive data.

#### Cost Management

Unforeseen costs often arise during cloud migration due to underestimating resource consumption or mismanaging cloud services.

**Recommendation:** Organizations should utilize cloud cost management tools, such as AWS Cost Explorer or Azure Cost Management, to track usage, set budgets, and prevent overprovisioning. A phased migration approach—beginning with non-essential systems—can help identify potential cost overruns early, enabling timely adjustments.

### Minimizing Downtime

Operational downtime can significantly disrupt business operations and impact customer satisfaction.

**Recommendation:** Adopting hybrid migration models—where critical systems remain on-premises initially—helps minimize disruptions. A detailed contingency and backup plan should be in place to quickly restore services in case of migration-related issues or outages.

### Legacy System Integration

Migrating legacy systems to the cloud presents compatibility challenges, particularly for older, complex applications.

**Recommendation:** Solutions like containerization and API-based integrations can facilitate smoother transitions without requiring complete rewrites. These approaches allow legacy systems to maintain functionality in the cloud while reducing migration time and costs.

### Stakeholder Collaboration

Successful cloud migration requires alignment across key stakeholders, including IT teams, business leaders, and cloud providers.

**Recommendation:** Clear communication and establishing shared goals among all stakeholders are crucial. Regular meetings and updates help manage expectations and ensure that risks are identified and mitigated early in the process.

### Conclusion

Cloud migration allows organizations to modernize their IT infrastructure, enhance scalability, and improve operational efficiency. However, the process involves significant challenges, particularly in data security, regulatory compliance, cost management, downtime, and legacy system integration [15].

To successfully navigate these challenges, organizations must take a **strategic, well-planned approach** to migration. This includes:

- Implement robust security measures and ensure compliance with relevant industry regulations.
- Using **cloud cost management** tools to monitor and control expenses throughout the migration.
- **Phased migrations** to minimize downtime and ensure business continuity.
- Employing **containerization** and **API solutions** to integrate legacy systems with modern cloud platforms.

Ultimately, while cloud migration can be complex, a thoughtful, collaborative approach ensures organizations can harness the full benefits of the cloud while minimizing the risks. Careful planning and strategic execution are essential to making the transition smooth, cost-effective, and successful.

### References

1. A Iqbal, R Colomo-Palacios (2019) "Key Opportunities and Challenges of Data Migration in Cloud: Results from a Multivocal Literature Review," *Procedia Computer Science*, vol. 164: 48-55, 2019.
2. MF Gholami, F Daneshgar, G Low, G Beydoun (2016) "Cloud migration process—A survey, evaluation framework, and open challenges," *Journal of Systems and Software* 120: 31-69.
3. V Stantchev, R Colomo-Palacios, M Niedermayer (2014) "Cloud Computing Based Systems for Healthcare," *The Scientific World Journal* 1-2.
4. P Sun (2020) "Security and privacy protection in cloud computing: Discussions and challenges," *Journal of Network and Computer Applications* 160: 1-27.
5. MF Gholami, F Daneshgar, G Beydoun, F Rabhi (2017)

- "Challenges in migrating legacy software systems to the cloud — an empirical study," *Information Systems* 67: 110-113.
6. L Megouache, A Zitouni, M Djoudi (2020) "Ensuring user authentication and data integrity in multi-cloud environment," *Human-centric Computing and Information Sciences* 10: 1-20.
  7. N Amara, H Zhiqui, A Ali (2017) "Cloud Computing Security Threats and Attacks with Their Mitigation Techniques," in 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Nanjing, China.
  8. M Faraji, YS, MN (2023) "Data Integrity and Cost Optimization in Cloud Migration," *International Journal of Information Technology and Management* 19: 47-52.
  9. A Keller, CV (2023) "Cloud-native Application Deployment and Cost Control Strategies," *MDPI Journal of Cloud Computing and Security* 12: 112-125.
  10. T Khanye, J Ophoff, K Johnston (2018) "Issues in Migrating Legacy Systems to the Cloud," in 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India <https://rke.abertay.ac.uk/en/publications/issues-in-migrating-legacy-systems-to-the-cloud>.
  11. L Griebel, HU Prokosch, F Köpcke, D Toddenroth (2015) "A scoping review of cloud computing in healthcare," *BMC Medical Informatics and Decision Making* 15: 1-16.
  12. T Auchterlonic (2021) "JPMorgan's hybrid-cloud approach ensures reliability but isn't affordable for all," *EMarketer* <https://www.emarketer.com/content/jpmorgan-hybrid-cloud-ensures-reliability-but-not-affordable-for-all>.
  13. KB Simon (2018) "Walmart-Microsoft 5-Year Cloud Deal — Three Key Areas of Execution," *Indrastra Global* 1-3.
  14. W Bartkiewicz, Z Gontar (2018) "CLOUD COMPUTING MIGRATION BARRIERS AND ADVANTAGES IN MANUFACTURING – AN ANALYSIS OF AMBIGUITY AND DEPENDENCES IN THE ASSESSMENT CRITERIA," *Econometrics* 22: 41-54.
  15. Maniah, B Soewito, FL G (2022) "A systematic literature Review: Risk analysis in cloud migration," *Journal of King Saud University - Computer and Information Sciences* 34: 3111-3120.

**Copyright:** ©2024 Sai Krishna Adabala. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.