Journal of Systemics, Cybernetics and Informatics (2025) 23(6), 42-46
https://doi.org/10.54808/JSCI.23.06.42

Key aspects for a secure migration of Databases to the Cloud: Challenges and Solutions

Yadira-Jazmín PÉREZ-CASTILLO
Centro de Investigación en Computación, Instituto Politécnico Nacional, (CIC-IPN).
México, 07738, CDMX.

Sandra-Dinora ORANTES-JIMÉNEZ
Centro de Investigación en Computación, Instituto Politécnico Nacional, (CIC-IPN).
México, 07738, CDMX.

Eleazar AGUIRRE-ANAYA
Centro de Investigación en Computación, Instituto Politécnico Nacional, (CIC-IPN).
México, 07738, CDMX.

ABSTRACT

In the digital age, migrating databases to the cloud has become an essential strategy for organizations seeking greater flexibility, scalability, and operational efficiency. However, this process poses significant challenges related to information security, including cyberattacks, regulatory compliance, data loss, and access control. This article explores the main challenges of migrating and managing databases in the cloud, analyzing the most common risks and their impact on protecting critical data. In addition, practical solutions such as encryption, multi-factor authentication, and disaster recovery strategies are presented to enable organizations to mitigate risks and ensure the confidentiality, integrity, and availability of information. Finally, the article highlights the benefits of adopting good security practices during migration, promoting a smooth transition to the cloud while safeguarding sensitive data. By proactively addressing these challenges, organizations can achieve a more secure and efficient cloud environment.

Keywords: Cloud Migration, Database Security, Cybersecurity, Data Integrity, Access Control.

1. INTRODUCTION

The adoption of cloud computing has grown significantly in recent years, transforming the way organizations manage and store their databases. The flexibility, scalability, and efficiency offered by cloud-based solutions have allowed companies to optimize their technological infrastructure and reduce operational costs. However, this shift to the cloud presents critical challenges, especially in terms of information security and data migration. Transferring databases to the cloud involves risks associated with data integrity, privacy, and accessibility, which require strict security measures to protect sensitive information [1].

In this context, security in the migration of databases to the cloud becomes a priority. A few strategies and best practices should be considered to ensure that data is moved securely, without compromising the confidentiality or availability of information. There are multiple challenges, such as a lack of control over cloud infrastructure, vulnerabilities in authentication systems, and protection against unauthorized access, which need to be adequately addressed. It is also crucial to understand the benefits that cloud migration can bring, such as high availability, cost optimization, and scalability, if robust security mechanisms are in place [1]

This article aims to provide a comprehensive view on the key aspects of secure database migration to the cloud, analyzing the main challenges faced by organizations, the available technological solutions, and the best practices to carry out a successful and secure migration in terms of security. To this end, the most effective strategies to mitigate risks and ensure data protection through emerging technologies and innovative organizational approaches are explored [3].

The article is structured as follows: Section 2 addresses the fundamentals of database migration to the cloud, providing context of the key concepts and stages of the migration process. Section 3 explores the main challenges in migration, highlighting the most significant challenges organizations face during the transfer of databases to the cloud. Section 4 presents best practices for secure migration, which describes the most effective security strategies and measures to mitigate risks and protect information in the process. Section 5 discusses the Emerging Trends and Technologies that are shaping the future of database migration to the cloud, such as artificial intelligence and machine learning. Finally, the article concludes with a Conclusions Section, summarizing key points and highlighting best practices and recommendations for a successful and secure migration.

2. FUNDAMENTALS OF DATABASE MIGRATION TO THE CLOUD

Migrating databases to the cloud has become an essential strategy for organizations looking to improve operational efficiency, reduce costs, and take advantage of the scalable and flexible infrastructure offered by the cloud. This process involves moving databases from on-premises servers or private infrastructures to public or private cloud platforms. Migration not only involves transferring data, but also reconfiguring systems to operate efficiently in the new environment. Despite its benefits, migrating databases to the cloud presents several challenges that organizations must address carefully, such as system compatibility, data management, and security [4] [5].

The three main models of cloud services are IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). In the IaaS model, companies lease computing infrastructure, such as storage and processing, without having to manage physical hardware. This model offers greater flexibility and control over databases, allowing organizations to manage their own systems and applications.

On the other hand, PaaS simplifies database management by providing a ready-made environment for application

development and deployment. SaaS, finally, allows organizations to use complete vendor-managed applications [4].
Migrating databases to the cloud can be approached using different strategies. The lift-and-shift approach, for example, involves moving databases as they are, without significant modifications to their structure. This method is fast, but it does not take full advantage of the cloud's optimized features [5]. Instead, more advanced strategies such as deplatforming and refactoring require modifying databases and applications to better leverage the benefits of the cloud, improving performance and scalability in the long term [6].
Key migration challenges include data compatibility, latency, and security. Compatibility is one of the most common issues, as on-premises databases may not be fully compatible with cloud environments, requiring adjustments to data schemas and architectures [6]. In addition, the migration of large volumes of data can be limited by bandwidth, affecting the availability of systems during the process. Security is another critical aspect, as data is exposed to risks if proper measures such as encryption and controlled access policies are not implemented [4].
Security in database migration is critical, especially when sensitive data must be transferred between systems. We recommend implementing data encryption both in transit and at rest, as well as multi-factor authentication to secure access. In addition, cloud platforms must comply with international regulations such as the GDPR, ensuring the secure processing of personal data [5] [4].

3. MAIN CHALLENGES IN MIGRATION

Migrating legacy systems to the cloud is a process that involves a number of technical, organizational, and strategic challenges. One of the most complex challenges is database migration, a critical component for enterprise applications. According to [7], legacy systems were designed to work in on-premises environments, so adapting their databases to cloud platforms requires a thorough restructuring process. These systems often employ data storage and management technologies that are not compatible with modern cloud architectures, forcing organizations to consider solutions such as reconfiguration, transformation, or even complete restructuring of databases.
The second challenge is the data migration itself. This process involves not only the transfer of information but also the optimization of data storage and management in the cloud, a process that can lead to scalability-related difficulties. Jawed and Sajid [8] explain that the cloud offers advantages in terms of scalability, but the benefits are not automatic. Organizations must adjust their databases and management systems to take advantage of cloud resources. Workload and data access must be managed to ensure performance is not impacted. This poses an additional challenge: ensuring that cloud databases can scale up or down as needed, without compromising efficiency or security.
Another significant challenge in this process is adapting systems to the differences in deployment between the various cloud platforms. Cloud databases are often managed through managed services, which means organizations do not have complete control over the underlying infrastructure. According to [6], this can create incompatibilities between the SQL dialects used by legacy systems and cloud databases. Although there are tools that allow the automatic conversion of SQL queries between different platforms, these solutions do not always cover all needs, especially when it comes to complex or custom queries. This forces organizations to invest time and resources in optimizing queries and adapting SQL queries to ensure they run correctly in the cloud environment.
Aside from technical challenges, there are also organizational and strategic considerations in cloud migration. As mentioned in [9], the adoption of cloud technologies is not only related to infrastructure but also involves a change in organizational culture. The transition to the cloud requires trained personnel and the adoption of new work methodologies, in addition to a review of security and compliance processes. Planning is critical, as organizations must assess the compatibility of legacy systems with the cloud services they choose to deploy, as well as the data security and privacy implications.
Security issues are also a critical concern during database migration. Cloud data control and protection is essential as organizations face potential external and internal threats. Data encryption, access management, and security in application programming interfaces (APIs) are aspects that require special attention [7]. Adopting strategies such as data segmentation and the use of cloud-based security models can help mitigate some of these risks.
Integrating legacy systems with cloud services also presents a significant challenge. Databases in traditional systems are often deeply integrated with other system components, such as applications and business processes. The challenge is to migrate these components in a way that does not disrupt the operation of the organization. In [8], they suggest that hybrid solutions, which allow the integration of on-premises systems with the cloud, are a viable option, although they can also generate additional complexities, especially when it comes to ensuring consistency and synchronization of data in real time.
In summary, database migration to the cloud faces multiple technical and operational challenges. From restructuring legacy databases to adapting SQL queries and managing scalability, to data security and integration with existing systems, organizations must be prepared to meet a variety of challenges. The key to success lies in meticulous planning, choosing the right tools, and training staff so they can manage the transition to the cloud effectively. The table summarizes the main challenges, their impact, and the suggested solutions.

Table 1 Migration Challenges

Challenge	Description
Security and privacy	Risk of security breaches and unauthorized access; need for encryption and robust policies.
Technical compatibility	Adaptation of legacy systems to cloud platforms; need for testing and adjustments.
Performance and latency	Latency in critical applications: solution through optimization and distributed data centers.
Cost Management	Unforeseen expenses in transfer and maintenance; importance of monitoring.
Organizational resistance	Cultural resistance and lack of training; Need for training and change strategies.
Sustainability	Environmental impact of energy consumption; adoption of sustainable practices.

4. BEST PRACTICES FOR SECURE MIGRATION

Securely migrating to cloud services is a critical process that requires the implementation of best practices to ensure data security and regulatory compliance. Here are some best practices based on the current state:

1. ***Assessment and Preparation:*** ISPC Readiness Model: Before migration, it is essential to assess readiness in terms of information security, privacy, and compliance (ISPC). This involves selecting the most appropriate cloud deployment model, service level agreement, and cloud provider that best suits the organization's needs [10].
2. ***Data Security:*** Encryption and Data Protection: Implement data encryption, such as prediction-based encryption (PBE), and establish security layers such as Secure Socket Layer (SSL) to protect privacy during migration [11] [12]. Sensitive Data Separation: Maintain strict separation between sensitive and non-sensitive data, applying encryption to sensitive data [11].
3. ***Proactive Approach:*** Threat Modeling: Use threat modeling to identify and assess potential threats, vulnerabilities, and risks. This helps to prioritize risks and apply effective controls by design [13]**.** Shared Responsibility: Understand the shared responsibility model, where the cloud service provider and customer have specific roles in cloud security [14].
4. ***Communication and Collaboration:*** Efficient Communication: Ensure clear communication between all parties involved in the migration, from decision-makers to IT and legal teams, to avoid disruptions and data loss [14].
5. ***Compliance & Regulations***
   Regulatory Compliance: Ensuring migration complies with industry regulations and internal security policies [14] [15].

5. EMERGING TRENDS AND TECHNOLOGIES

The migration of databases to cloud environments continues to evolve toward more distributed, automated, and security-centered architectures. As the volume, variety, and sensitivity of enterprise data increase, advanced technologies are emerging that aim to mitigate risks related to confidentiality, integrity, availability, and privacy throughout the entire migration lifecycle. Current trends focus not only on strengthening traditional protection layers but also on incorporating intelligent and adaptive mechanisms capable of anticipating threats, managing access with granular precision, and ensuring regulatory compliance in increasingly complex contexts.
This section presents the most relevant trends, covering innovations in encryption, authentication, access control, artificial intelligence applied to security, and an overview of emerging challenges and their potential future solutions.

1. *Encryption Technologies*

Encryption remains the central pillar of data protection both in transit and at rest during migration. Recent innovations aim to increase cryptographic robustness and reduce exposure to sophisticated attacks.

1. *Probabilistic Public Key Encryption (EPPKE)*: This technique optimizes the security of migrated data through covariance matrix adaptation strategies, ensuring data integrity with algorithms such as Luhn and BLAKE 2b encapsulation [16].
2. *Symmetric and RSA encryption:* Used to authenticate and protect data during migration between cloud storage systems, ensuring confidentiality, authorization, authenticity, and integrity [17].
3. *Advanced Encryption (AES-256), SHA-512, and Information Dispersion*: The integration of AES-256 with hash functions such as SHA-512 continues to be widely accepted as a standard in mission-critical environments, as it strengthens verification mechanisms and reduces the likelihood of data-tampering attacks [18].
4. *Post-Quantum Encryption:* Recent literature highlights the need to adopt cryptographic algorithms resistant to quantum computing, especially in the migration of sensitive data. Quantum-enabled attacks could compromise traditional cryptosystems such as RSA and ECC, prompting the development of transition strategies toward post-quantum schemes [19].

2. *Authentication and Access Control Methods*

1. *Mutual Authentication and Key Splitting:* These methods ensure pre-migration authentication, protecting data using shared symmetric keys [17].
2. *Secure Socket Layer (SSL) and Migration Tickets:* Provide a security framework for privacy protection during data migration, strictly separating sensitive data from non-sensitive data [11].
3. *Zero Trust Architecture:* emerges as a key model for migration processes, promoting continuous verification, multifactor authentication, and dynamic identity-based policies [20].

3. *Artificial Intelligence Integration*

Machine-learning-based solutions can detect anomalous patterns in real time during migration, anticipating risks during virtual machine transfers and preventing unauthorized access [21].
Recent research highlights that AI-powered security systems can adjust cryptographic parameters, strengthen access policies, and execute automated responses to suspicious behaviors, increasing the resilience of the migration process

4. *Future Challenges and Solutions*

1. *Data Protection and Privacy:* Challenges include unauthorized access and the disclosure of sensitive information. Encryption-based methods and enhanced data protection mechanisms are proposed as effective solutions [23].
2. *Integrated Frameworks for Secure Migration*: Recent studies suggest integrated frameworks that combine probabilistic encryption, automated auditing, logical data separation, and continuous monitoring to provide more secure end-to-end migrations [24].
3. *Future Trends:* Emerging technologies are expected to continue improving data protection in cloud-computing environments [25].
   Anticipated advancements include:

   - full automation of the migration process,
   - accelerated adoption of post-quantum cryptography,
   - blockchain-based traceability,

- serverless and edge-computing architectures,
- AI-driven adaptive security systems.

These emerging directions point toward an ecosystem in which security is proactive, autonomous, and deeply integrated into every stage of the migration process.

6. CONCLUSIONS

Secure database migration to the cloud is a complex process that demands a comprehensive and well-structured strategy. To ensure success, it is critical to address technical, operational, and security challenges from a proactive perspective. Careful planning, assessing infrastructure readiness, and implementing robust security measures, such as encryption of data at rest and in transit, are essential pillars for protecting information during and after migration.

In addition, taking a proactive approach to threat management, through continuous monitoring and early detection of vulnerabilities, allows potential risks to be mitigated. Effective communication between technical teams, stakeholders, and cloud service providers is equally critical to aligning expectations and ensuring a smooth transition.

A key aspect that should not be overlooked is the shared responsibility model, which clearly defines the security obligations of both the cloud provider and the customer. Understanding and applying this model is critical to ensuring regulatory compliance and maintaining data integrity and confidentiality.

In today's landscape, security in data migration to the cloud is being strengthened thanks to the adoption of advanced technologies. The use of state-of-the-art encryption techniques, multi-factor authentication methods, and the integration of artificial intelligence for anomaly detection are transforming the way data is protected. These innovations not only address security and privacy challenges but also enable a faster and more efficient response to potential threats.

In conclusion, a secure migration to the cloud not only involves moving data but also ensuring its continuous protection in a dynamic and constantly evolving environment. The combination of rigorous planning, implementation of advanced technologies, and effective collaboration between all parties involved is the key to minimizing risks and maximizing the benefits of the cloud. As organizations continue to adopt cloud solutions, it is imperative to maintain a proactive and adaptive approach to meet emerging challenges and make the most of the opportunities offered by this environment.

7. REFERENCES

[1] E. Ortiz, C. Villacorta, and A. Mendoza, "Seguridad de la Información en la Nube: Una revisión sistemática", **Revista Científica Ciencias Ingenieriles**, vol. 4, no. 1, 2024, pp. 69–78. DOI: 10.54943/ricci. v4i1.383.

[2]]D. Seddiki, S. G. Galán, J. E. M. Expósito, M. V. Ibañez, T. Marciniak, and R. J. -Pérez de Prado, "Sustainable expert virtual machine migration in dynamic clouds", **Computers and Electrical Engineering,** vol. 102, 2022, p. 10825. DOI: 10.1016/j.compeleceng.2022.108257.

[3] K. N. Gottipati, N. Peddisetty, S. Pothireddy, G. Botta, P. Yellamma, and G. Swain, "A Study on Data Security and Privacy Issues in Cloud Computing," in **Proceedings of the 3rd International Conference on Artificial Intelligence and Smart Energy**, ICAIS 2023, 2023. DOI: 10.1109/ICAIS56108.2023.10073721.

[4] Amazon Web Services, "Migración de bases de datos a la nube, AWS Database Migration Service (AWS DMS)". Disponible: https://aws.amazon.com/es/dms/.

[5] Amazon Web Services, "Migración de bases de datos de Microsoft SQL Server a la nube AWS - AWS Guía prescriptiva". Available: https://docs.aws.amazon.com/es_es/prescriptive-guidance/latest/migration-sql-server/welcome.html

[6] R. Zmigrod, S. Alamir, and X. Liu, "Translating between SQL Dialects for Cloud Migration," 2024. DOI: 10.1145/3639477.3639727.

[7] M. Fahmideh, F. Daneshgar, G. Beydoun, and F. Rabhi, "Challenges in migrating legacy software systems to the cloud an empirical study," 2020, Accessed: Jan. 14, 2025. Available: http://arxiv.org/abs/2004.10724

[8] M. S. Jawed y M. Sajid, "A Comprehensive Survey on Cloud Computing: Architecture, Tools, Technologies, and Open Issues," International Journal of Cloud Applications and Computing (IJCAC), vol. 10, no. 1, 2020, pp. 1-25. DOI: 10.4018/IJCAC.2020010101.

[9] D. C. Marinescu, Cloud Computing. **Elsevier**, 2013. DOI: 10.1016/C2012-0-02212-0.

[10] F. F. Alruwaili y T. A. Gulliver, "Secure Migration to Compliant Cloud Services: A Case Study," **IEEE Access**, vol. 6, 2018, pp. 12345-12356. DOI: https://doi.org/10.1016/j.jisa.2017.11.004

[11] S. Shakya, "An Efficient Security Framework for Data Migration in a Cloud Computing Environment," **International Journal of Computer Applications**, vol. 178, no. 9, 2019, pp. 1-6. DOI: https://doi.org/10.36548/jaicn.2019.1.006

[12] A.A. Hussein y A. A. Hussein, "Data Migration Need, Strategy, Challenges, Methodology, Categories, Risks, Uses with Cloud Computing, and Improvements in Its Using with Cloud Using Suggested Proposed Model" **Journal of Computer and Communications**, vol. 8, no. 12, pp. 1-15, 2020. DOI: 10.4236/jis.2021.121004

[13] J. Njoku, "A Proactive Approach to Addressing Security Challenges in Cloud Migration," Advances in Multidisciplinary and scientific Research Journal Publication, vol. 2, no. 2, pp. 89–96, 2023. DOI: 10.22624/AIMS/CSEAN-SMART2023P11.

[14] G. Madhukar Rao et al., "A Secure and Efficient Data Migration Over Cloud Computing," **IOP Conference Series: Materials Science and Engineering**, vol. 1099, no. 1, p. 012082, 2021. DOI: 10.1088/1757-899X/1099/1/012082.

[15] C. Wagner, A. Hudic, S. Maksuti, M. Tauber, and F. Pallas, "Impact of Critical Infrastructure Requirements on Service Migration Guidelines to the Cloud," **in 2015 3rd International Conference on Future Internet of Things and Cloud**, **IEEE**, pp. 1–8, 2015. DOI: 10.1109/FiCloud.2015.79.

[16] M. G. Aruna and K. G. Mohan, "Secured cloud data migration technique by competent probabilistic public key encryption," **China Communications**, vol. 17, no. 5, pp. 168–190, 2020. DOI: 10.23919/JCC.2020.05.014.

[17] C. Gudisagar, B. R. Sahoo, M. Sushma, and C. D. Jaidhar, “Secure data migration between cloud storage systems,” **in 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE**, pp. 2208–2212, 2017. DOI: 10.1109/ICACCI.2017.8126173.

[18] J. R. N. Sighom, P. Zhang, and L. You, “Security Enhancement for Data Migration in the Cloud,” **Future Internet 2017**, Vol. 9, Page 23, 2017. DOI: 10.3390/FI9030023.

[19] Y. Baseri, A. Hafid y A. H. Lashkari, “Future-Proofing Cloud Security Against Quantum Attacks: Risk, Transition, and Mitigation Strategies”, 2025. **arXiv**. https://arxiv.org/abs/2509.15653.

[20] The Cloud Security Alliance (CSA), "**The Cloud Security Alliance (CSA**)" 2025. Available: https://cloudsecurityalliance.org/.

[21] H. Kaur and S. Gargrish, “Evaluation of Secure Methods for Migrating Virtual Machines to the Cloud,” **Proceedings - International Conference on Computing, Power, and Communication Technologies, IC2PCT 2024**, pp. 1961–1968, 2024. DOI: 10.1109/IC2PCT60090.2024.10486614.

[22] S. M. Shaffi, S. Mohamed, S. Data, R. Vijayan, S. Vengathattil y J. N. Sidhick, “AI-Driven Security in Cloud Computing: Enhancing Threat Detection, Automated Response, and Cyber Resilience”, 2025. **arXiv**. https://arxiv.org/abs/2505.03945

[23] P. Yang, N. Xiong, and J. Ren, “Data Security and Privacy Protection for Cloud Storage: A Survey,” **IEEE Access**, vol. 8, pp. 131723–131740, 2020. DOI: 10.1109/ACCESS.2020.3009876.

[24] S. Ahmadi y M. Salehfar, “Privacy-Preserving Cloud Computing: Ecosystem, Life Cycle”, **Layered Architecture and Future Roadmap**, 2022. **arXiv**. Https://arxiv.org/abs/2204.11120

[25] R. Li, “Analysis of Key Technologies for Data Security Protection Based on Cloud Computing,” **International Journal of Computer Science and Information Technology**, vol. 4, no. 1, pp. 243–252, 2024. DOI: 10.62051/IJCSIT.V4N1.30.