# From Cloud to On-Premises: A Systematic Review of Cloud Repatriation Drivers, Strategies, and Governance Challenges

Amzari Mohd Roslan[1], Fazlina Mohd Ali[2], Faizan Qamar[3], Liyana Safra[4], Nur Arzilawati Md Yunus[5]
Faculty of Information Science and Technology (FTSM), Universiti Kebangsaan Malaysia (UKM), Selangor, Malaysia[1, 2, 3]
Faculty of Artificial Intelligence (FAI), Universiti Teknologi Malaysia (UTM), Selangor, Malaysia[4]
Faculty of Computer Science and Information Technology (FSKTM), Universiti Putra Malaysia (UPM), Selangor, Malaysia[5]

***Abstract*—Cloud repatriation is the migration of workloads from public cloud to private, on-premises, and hybrid clouds. Despite the growing adoption of cloud computing, there are many issues associated with operational expenditure, the unpredictable performance of cloud services, compliance concerns, vendor dependency, and data sovereignty concerns. Thus, cloud repatriation has become a strategic solution, especially in the public sector where governance and regulatory requirements are paramount. Previous studies on cloud repatriation are predominantly descriptive, with limited focus on predictive models that include cost assessment, security compliance, governance maturity, and workload mobility. Moreover, empirical studies are still limited, particularly in the context of public sector settings and regulatory constraints and sovereignty requirements. This study aims to provide a systematic literature review of the factors, solution approaches, and limitations of cloud repatriation towards on-premises transition. The review offers three main contributions: factors driving cloud repatriation, the synthesis of limitations and solution strategies for each factor, and an analysis of current trends across academic and industry literature. Major databases and selected industry reports were used to gather academic and industry sources. From an initial set of 124 articles published between 2021 and 2025, 20 key studies were selected. The results are broken down into five main factors: cost and economic factors, data security and sovereignty, vendor lock-in and portability, performance and latency needs, and governance and exit strategies. The review underscores the need for integrated governance-driven frameworks to enable secure, sustainable, and policy-compliant digital transformation.**

***Keywords*—Cloud repatriation; on-premises transition; systematic literature review; data security; hybrid cloud; data sovereignty; vendor lock-in; governance; implementation limitations**

## I. Introduction

The adoption of cloud computing has been a key pillar of global digital transformation for over a decade. Beginning with the promise of lower costs, operational flexibility, and rapid scaling capabilities, the public cloud has attracted the attention of organizations across a variety of sectors, including finance, healthcare, education, and government [1], [2]. Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform have emerged as major players in the market, offering infrastructure and platforms that are seen as capable of replacing traditional data centres [3].

However, after a more extended period of adoption, more and more organizations are beginning to realize that reality does not always align with initial expectations [4]. This phenomenon has led to a resurgence of interest in cloud repatriation (CR), the process of relocating workloads from public clouds to private or hybrid environments [5], [6]. According to a 2023 study by IDG & Lufthansa Industry Solutions, the cloud repatriation phenomenon is not just a theory. Approximately 28% of enterprises in Germany have already moved workloads back from the cloud to on-premises infrastructure due to specific reasons including security, data compliance, and migration complexity [7].

The recent Cloud Migration and Repatriation Study 2025 by IDG/LHIND [8], as illustrated in Fig. 1, indicates that over 80 percent of all surveyed companies have done or intend to do repatriation in the near-mid-term.

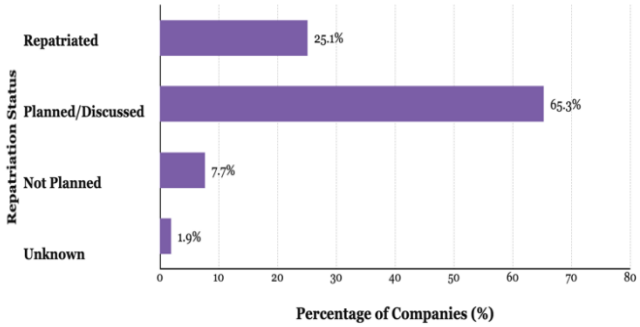


Fig. 1. Germany cloud repatriation study in 2025.

GEICO, a major insurance company in the United States, adopted a partial workload repatriation to gain economies of scale and have more control over important applications. This choice can illustrate how economic reasons and compliance by the organization can become an impetus to repatriate from the cloud [32]. More broadly, industry reports show that the repatriation phenomenon is becoming more pronounced. A Puppet study [10] found that 86% of CIOs plan to move at least some workloads from the public cloud back to private or on-premises infrastructure. These statistics confirm that repatriation is not an isolated phenomenon, but an emerging global trend. Several instances of CR were summarised in Table I.

TABLE I. CASE STUDIES OF CLOUD REPATRIATION DRIVING FACTORS

| Citation | Organization | Factors |
|---|---|---|
| [7], [8] | IDG/LHIND | Security factors, data compliance, migration complexity, and vendor lock-in. |
| [9] | 37signals (USA) | Hidden costs, inconsistent performance in public clouds. |
| [32] | GEICO (USA) | Cost savings, critical application control, organizational compliance. |
| [12] | Dropbox (USA) | High cost of public cloud operations, performance control, and reliability. |
| [13] | X (USA) | High cloud costs, control over data and performance, the need to reduce storage size and processing loads, optimizing infrastructure. |
| [33] | Global Research (CIO Survey) | Cost, security, compliance, and vendor lock-in. |

Cloud repatriation does not signify the decline of cloud computing; rather, it represents a maturation of workload-mobility strategies. Posey et al. [6] argue that CR should be seen as part of the concept of "workload mobility", which is the flexibility to place applications and data in the most suitable environment, whether in a public cloud, private cloud, organizational data center, or hybrid location. The strategic flexibility of a firm is enhanced by its preparedness to shift workloads off-cloud [4]. This approach enables organizations to adopt the "best execution place" principle, where each workload is assigned according to its cost, performance, security, regulatory, and compliance requirements [11].

Among the most dominant factors driving cloud repatriation is uncertain and unexpected costs. Studies show that most organizations experience cloud spending that exceeds budget by 30–40% due to overprovisioning, data egress fees, and unmanaged resources [1], [2], [3]. Upon leaving AWS and creating its own infrastructure, Dropbox, in particular, saved more than USD 75 million [12]. Meanwhile, social media company X (Twitter) saved cloud operating expenses to the tune of USD 60 million annually following the relocation of media storage in-house [13]. As Murugesan [3] notes, although cloud will decrease operational expenditure (OpEx). In fact, the organization is usually bound to incur high long-term costs; therefore, the Total Cost of Ownership (TCO) analysis needs to be more comprehensive.

Besides cost consideration, CR is also being pushed by security and compliance considerations. Financial and banking institutions are also subject to strict regulations like the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI-DSS) that mandate rigorous rates of encryption and incessant auditing [14], [15]. According to Everest Group [15], in the case of the banking industry, the aspects of data sovereignty and access control are of primary importance because any breach of the data may have legal consequences and a tarnished reputation. According to Priyanka Gowda [14], the migrations of the cloud in the banking industry are often faced with the difficulty of connecting the old system with the new systems, which heightens the chances of disruptions and impacts business-related essentials. Although cloud providers possess excellent security controls, the actual issues are presented by the vulnerability of governance and distributed responsibility frameworks whose implications are not always well-known by users [16], [17]. A study by the Ponemon Institute [17] revealed that the mean cost per annum of a cloud account breach is USD 6.2 million, and the mean application downtime is 138 hours per year. This implies that as much as the cloud provides a highly effective infrastructure, the success or failure of any organization is a major factor of organizational governance.

Another important driver of cloud repatriation is vendor lock-in and limited workload portability. eG Innovations [2] has reported that workload mobility is not easily achieved because of dependence on proprietary APIs and data formats. Räisänen [18] declared that the failure to have an effective exit strategy puts the organization at risk of losing strategic control and escalating expenses in the process of leaving a specific provider. To this end, a large number of organizations are currently pursuing multi-cloud or hybrid solutions to reduce the vendor lock-in risk. According to the BigID report [19], it is observed that 68% of the organizations currently operate in multi-cloud setups, and on average, there are four different types of providers who serve various important applications.

Moreover, the factors of performance and latency are also important triggers of the repatriation process. As Flores [20] discovered, data-intensive workloads, especially in the healthcare and media sectors, fail to reach optimum performance levels when they are deployed in the structure of a public cloud. As Posey et al. [6] noted, many organizations are shifting to a hybrid model because of the different needs posed by the development and production environment. The use of a phased migration strategy supported by middleware was reported by Priyanka Gowda [14] as the most common approach adopted in the financial services industry to address operational disruptions. Other new paradigms like edge computing are also gaining more academic interest, with the ability to handle data in real-time near the data source, which helps to reduce the issue of latency.

Considerable concern has also been raised regarding governance and exit strategies. Grabski and Schmidt [16] suggested a two-tier model of governance which is grounded on the TOE framework, and it indicates the necessity of collective responsibilities between the CSU and CSP. They pointed out that any organization needs to develop new governance policies whenever it decides on a repatriation, the definition of Service Level Agreements (SLAs), security control, and data backup procedures. Forbes [21] also pointed out that repatriation is not only a technical choice, but it is a way to gain control, data ownership, and bargaining power over cloud providers.

However, despite various studies and reports, several critical limitations remain unaddressed. Longitudinal studies measuring the cost, performance, and security impacts of repatriation over a five-to ten-year period are almost non-existent [5], [22]. Furthermore, existing models lack integration across cost evaluation, security compliance, governance maturity, and workload mobility, particularly within public sector contexts. Therefore, this study presents a systematic literature review that addresses these limitations through three focused contributions: identifying the key factors influencing cloud repatriation, examining solution strategies proposed in academic and industry literature, and revealing the implementation limitations between

theoretical models and real-world on-premises transition practices.

## II. Methodology And Article Selection

This study employs a Systematic Literature Review (SLR) method to collect the extant literature regarding cloud repatriation, including the problems and factors involved in the process of workload migration between the public clouds and on-premises or hybrid cloud settings. The review process was guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework. The aim is to bring together theoretical and practical knowledge that will describe the state of research and practice in cloud repatriation.

### A. Research Design

The methodological flow involves four stages:

*1) Identification* – Articles were found in reputable academic databases such as IEEE Xplore, SpringerLink, ScienceDirect, and Scopus, and reputable sources in the industry such as eG Innovations, Everest Group, Forbes Tech Council, and BigID Blogs. The search was conducted using the following keywords: 'cloud repatriation', 'cloud exit strategy', 'hybrid cloud', 'data segregation', 'cloud governance', and 'multi-cloud migration'. This initial search yielded a total of *124 records.* Search execution differed by source type. For academic databases, the six keywords identified above were combined using Boolean operators (AND/OR) within each platform's advanced search interface to maximize retrieval precision, with syntax adjusted to suit the specific search conventions of each platform. For industry sources without advanced Boolean search functionality, individual keywords were searched separately using each platform's native search or blog search function, and the keyword yielding results most topically relevant to cloud repatriation was retained per source. Retrieved records across all sources were consolidated before the deduplication step described in the Screening stage. The search and screening process was conducted over the weeks preceding the recorded extraction date of 8 December 2025, which is reported in Fig. 2 as the reference date for the record count at the point of extraction.

*2) Screening* – The 124 records were first screened for duplicate entries, resulting in 106 unique records retained for further review. These records then underwent systematic title and abstract screening, during which 71 records were excluded based on the identified reasons. Following this screening process, 35 articles were forwarded for full-text eligibility assessment, as illustrated in Fig. 2.

*3) Eligibility* – The 35 remaining articles underwent comprehensive full-text review against the defined inclusion criteria, which required coverage of topics related to cloud repatriation factors, migration strategies, data security, performance, or governance, published between 2021 and 2025. During this stage, 15 articles were excluded, and the remaining 20 studies were retained for final synthesis.

*4) Inclusion* – The final 20 studies were categorised into two groups: Theoretical Findings (TF), comprising 9 peer-reviewed academic publications sourced from journals and conference proceedings, and Real-Life Use Cases (RLUC), comprising 11 industry articles, reports, and technical blogs. This dual classification ensures a balanced representation of both theoretical constructs and practical applications in the analysis of cloud repatriation.

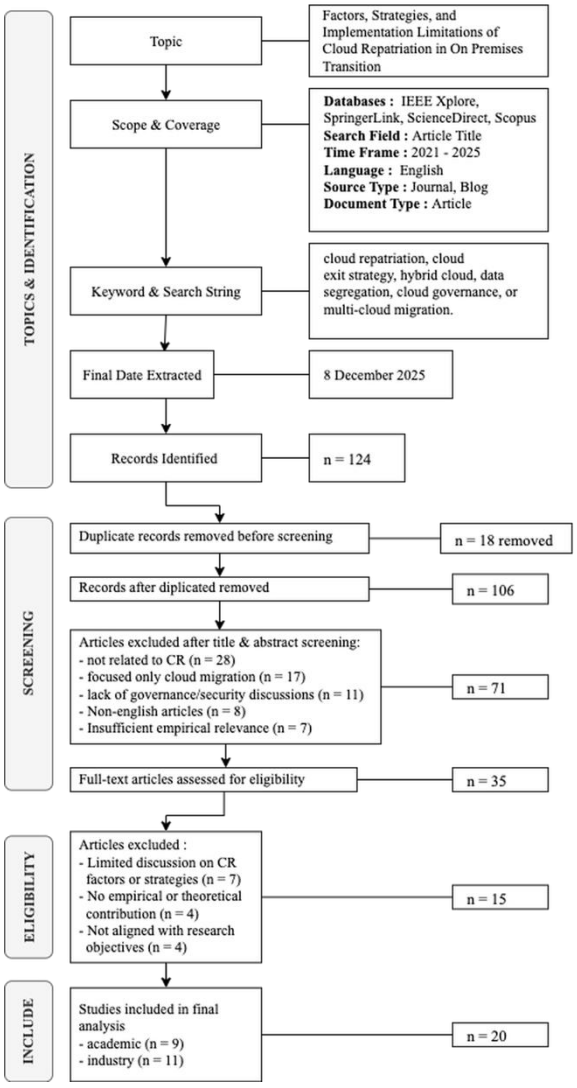


Fig. 2. PRISMA flow of article selection.

### B. Research Questions

The review is guided by three Research Questions (RQs) designed to clarify the study's analytical focus:

- RQ1: What are the factors driving cloud repatriation in recent academic studies and industrial real-life use cases?
- RQ2: What are the limitations and solution strategies for each factor driving cloud repatriation towards on-premises transition?
- RQ3: What is the current trend of cloud repatriation in academic and industry literature?

These questions direct the synthesis and appropriateness in the alignment of the literature evidence to the study objectives.

### C. Article Categorization

To differentiate between theoretical and applied contributions, the chosen works were broken down into two major groups: 1) Theoretical Findings (TF), and 2) Real Life Use Cases (RLUC). These measures are based on the final 20 articles included in the PRISMA process that identified the inclusion of the relevant studies in a systematic way that was validated. While this dual classification distinguishes theoretical from applied contributions, sources within each category carry differing levels of evidential strength. Peer-reviewed articles and conference proceedings (the TF category) have undergone formal editorial and peer review, whereas industry reports, company blogs, and white papers (the RLUC category) are not academically peer-reviewed and may reflect commercial or promotional framing associated with their originating organizations. This review retains these source types for the practitioner-level insight they offer, but findings drawn from lower-scrutiny sources are treated with appropriate interpretive caution throughout Section IV and corroborated against peer-reviewed evidence where available.

This dual classification allows establishing a balanced comparative position between the perspectives of real use cases and the practical elements of the academic field, to identify the most important limitations and trends. The distribution of selected articles, as illustrated in Fig. 3, indicates that even though academic discourse continues to be dominant, more and more industry-based evidence is emerging to corroborate theoretical knowledge with practical application. The balance between these two categories strengthens this review by ensuring that the aggregate outcomes are not biased toward the literature alone, but also provide practitioners and policymakers with practical perspectives.

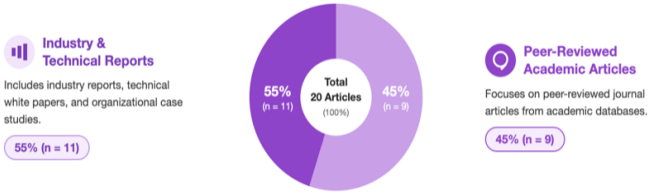


Fig. 3. Classification of selected articles and distribution of related studies.

TABLE II. THEORETICAL FINDINGS IN ACADEMIC STUDIES

| Author | Publication Source | Number of Factors |
|---|---|---|
| [3] | IEEE Xplore | 1 |
| [14] | Scopus Journal | 1 |
| [16] | HICSS Conference | 1 |
| [18] | Conference Paper | 1 |
| [23] | IEEE Conference | 3 |
| [24] | Journal Article | 2 |
| [25] | IEEE Conference | 2 |
| [26] | Springer | 1 |
| [12] | Journal Article | 1 |

TABLE III. REAL-LIFE USE CASES, INDUSTRY REPORTS, BLOGS, AND ONLINE PUBLICATIONS

| Author | Publication Source | Number of Factors |
|---|---|---|
| [6] | Industry Report | 1 |
| [15] | Industry Report | 1 |
| [2] | Industry Blog | 1 |
| [19] | Industry Report | 1 |
| [22] | Industry Blog | 1 |
| [21] | Forbes Council | 1 |
| [7] | Industry Survey | 1 |
| [5] | White Paper | 1 |
| [11] | Industry Report | 1 |
| [10] | Industry Blog | 1 |
| [4] | White Paper | 1 |

The scholarly and theoretical contributions identified through this review process are summarised in Table II, which presents the academic publications selected for analysis, while Table III presents the corresponding industry-based sources. As illustrated in Fig. 4, academic studies tend to contribute a higher number of CR factors. In contrast, all 11 industry sources each contribute a single CR factor, reflecting a more targeted focus in industry literature. Collectively, the 20 selected studies contribute a total of 22 identified CR factors, forming the thematic foundation for analysis in this review.

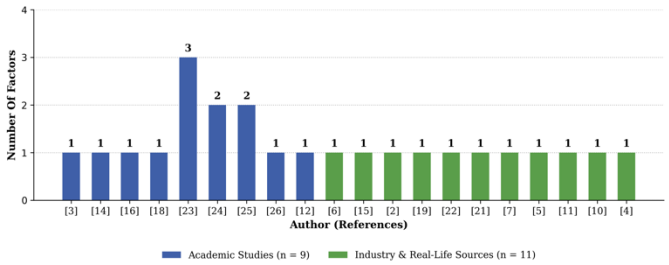


Fig. 4. Numbers of factors identified in each study by author.

### D. Quality Assessment Criteria

Each included study was assessed using three quality dimensions to ensure the validity and relevance of the review outcomes. Completeness refers to the availability of clear findings, models, or empirical evidence that directly addresses the defined research questions. Credibility concerns the source authenticity and peer-review status of both academic and industry materials included in the review. Relevance requires direct alignment with the topics of cloud repatriation, hybrid migration, or related keywords as defined in the search strategy. Only studies meeting all three criteria were included in the final synthesis to maintain methodological rigour and ensure trustworthy interpretation of the results. Instead of a numerical scale, a binary pass/fail system was used for each dimension; if a study explicitly addressed the dimension, it was deemed to satisfy it (Yes); if it did not, or if it did but only superficially, or if it did but could not be independently verified, then it was deemed not to satisfy it (No). Thirty-five articles were selected for full-text review, of which only those that received a "Yes"

for all three dimensions were retained for final synthesis. These classifications were made by the lead author and then re-evaluated and confirmed by co-authors before finalization. This process does not begin with independent parallel coding by multiple reviewers, so this does not constitute formal interrater reliability verification and is discussed further as a methodological limitation in Section III-F.

### E. Synthesis Approach

All included materials were analysed using thematic coding and classified across five factors derived from both theoretical and practical insights:

- Cost and Economic Considerations.
- Security, Compliance, and Sovereignty.
- Vendor Lock-In and Portability.
- Performance and Latency Requirements.
- Governance and Exit Strategy.

This approach integrates quantitative data with qualitative insights, aligning academic concepts with real-world practices. By combining rigorous research with industry relevance, the study offers a comprehensive understanding of the strategies, factors, and limitations associated with cloud repatriation.

## III. Related Works

This section critically reviews state-of-the-art academic literature, industry reports, and real-life cases addressing the principal factors and limitations associated with cloud repatriation. Rather than presenting the selected studies as an isolated list, each subsection examines how the identified limitations inform the analytical framework of this review. A cross-factor comparison is subsequently presented in Table IV.

TABLE IV. Summary of Related Works By Factor

| Factor | Author | Strengths | Limitation | Contributions |
|---|---|---|---|---|
| Cost & Economics | [3], [22], [23], [24], [21] | Cost unpredictability and TCO as repatriation drivers<br>Hybrid deployment for cost control<br>Dropbox, X/Twitter confirm post-CR savings | Descriptive analyses; no data-driven cost models<br>No standardised TCO benchmarking framework<br>Limited public sector validation | Synthesises cost factors across academic and industry sources<br>Identifies TCO modelling as a key limitation<br>Establishes cost as a core CR framework dimension |
| Security, Compliance, Sovereignty | [24], [14], [19], [15] | GDPR, PCI-DSS compliance as repatriation triggers<br>Sovereignty and encryption as recurring concerns<br>Data residency confirmed as industry driver | Prescriptive and conceptual; no implementation plans<br>No unified compliance-into-repatriation model<br>Security and governance treated separately | Maps security factors across academic and industry sources<br>Highlights missing compliance-governance integration<br>Informs policy-driven CR framework for regulated sectors |
| Vendor Lock-In & Portability | [6], [18], [11], [16] | Proprietary APIs and vendor contracts as portability barriers<br>TOE-based multi-cloud governance proposed<br>Hybrid adoption to reduce lock-in risk | Conceptual frameworks; no reusable blueprints<br>Public sector constraints underrepresented<br>Multi-cloud cost-complexity trade-offs unexplored | Consolidates lock-in factors from theory and practice<br>Identifies portability gap in public sector context<br>Supports portable-by-default architectural standards |
| Performance & Latency | [25], [26], [12], [3] | On-premises outperforms public cloud in latency-intensive workloads<br>Selective repatriation and load-balancing proposed<br>Latency variability across cloud regions | Simulation-based; no cross-industry validation<br>No standardised cloud vs. on-premises benchmarking<br>Cost-latency trade-offs underexplored | Consolidates pre- and post-CR performance evidence<br>Flags benchmarking absence as implementation limitation<br>Supports selective repatriation as a performance strategy |
| Governance & Exit Strategy | [16], [1], [7], [10], [15] | Structured exit planning recognised as critical enabler<br>TOE-based and shared-responsibility models introduced<br>Governance maturity correlates with repatriation readiness | Descriptive models; no implementation roadmaps<br>No quantifiable governance maturity metrics<br>No replicable blueprint for hybrid or public sector | Synthesises governance factors across all source types<br>Identifies exit governance gap as critical limitation<br>Establishes governance as dominant CR factor |

### A. Cost and Economic Considerations

Several studies have examined cost as a primary driver of cloud repatriation. Murugesan [3], Linthicum [22], and Kumar [5] identify increased operational expenditure and uncertain Total Cost of Ownership (TCO) as key concerns when workloads remain on public cloud platforms. Hui Chang [23] and Forbes Tech Council [21] further argue that transitioning to hybrid or on-premises environments offers greater long-term capital expenditure control. Real-world cases corroborate these findings, with Dropbox reporting annual savings of USD 75 million post-repatriation [12], and X (Twitter) reducing cloud costs by USD 60 million annually [13]. However, most existing studies rely on descriptive or anecdotal cost analyses rather than data-driven models. Kumar [5] proposes a Cloud Right framework but lacks cross-industry empirical validation, while Linthicum [22] and Murugesan [3] do not quantify cost-performance trade-offs. No standardised TCO benchmarking framework currently exists, particularly for non-technical and public sector contexts. This absence of a standardised, data-driven TCO framework is a central gap that this review responds to by consolidating disparate cost evidence (Sections IV and Table IV) into a single comparative synthesis rather than treating each case in isolation.

### B. Security, Compliance, and Sovereignty

Security and compliance concerns are widely recognised as significant factors influencing cloud repatriation decisions. Abied et al. [24] and Priyanka Gowda [14] highlight that e-government and Banking, Financial Services and Insurance (BFSI) environments require strict data privacy, trust, and governance compliance. Industry reports by BigID [19] and Everest Group [15] confirm that data sovereignty and encryption integration are common repatriation triggers in regulated sectors. Despite this, existing works remain largely prescriptive, presenting conceptual models without practical implementation plans. Abied et al. [24] focus on security awareness without operational guidance, while BigID [19] discusses compliance trends without demonstrating real-world applicability. Furthermore, no unified policy-based model currently integrates compliance controls directly into repatriation workflows, particularly for public sector environments. This separation of prescriptive security models and operational implementation is exactly what this review aims to bridge by correlating security factors to specific solution approaches (Table VII) instead of compliance requirements and technical controls as separate discourses.

### C. Vendor Lock-In and Portability

Vendor dependency and lack of portability are consistently reported challenges in cloud repatriation literature. Posey et al. [6], Räisänen [18], and Jewargi [11] highlight that proprietary APIs and storage formats reduce workload flexibility and increase switching costs. Grabski and Schmidt [16] extend this by proposing a TOE-based multi-cloud governance model that promotes shared responsibility across providers. However, these studies largely overlook the operational complexity and cost of managing multi-cloud environments. Posey et al. [6] and Jewargi [11] describe avoidance strategies without providing reusable architectural blueprints, and most academic works focus on identifying risks rather than prescribing standardised interoperability models. Public sector constraints, including procurement regulations and data residency requirements, remain underrepresented in existing portability frameworks. Existing research does not extend beyond the identification of risk, so this review aggregates lock-in evidence from both theoretical and practical sources to identify areas where public sector portability needs are not met (Table IV).

### D. Performance and Latency Requirements

Technical performance, particularly latency and scalability, is a well-documented repatriation trigger in enterprise contexts. Mallikarjuna and Kumar [25], Sandhiya and Suresh [26], and Korada and Sikha [12] demonstrate that on-premises and private cloud environments consistently outperform public cloud configurations in high-computation and latency-intensive workloads. Murugesan [3] and Hui Chang [23] further note that latency directly impacts resource efficiency and user experience. Nevertheless, most performance analyses are context-specific, relying on simulation-based or single-case validations. Mallikarjuna and Kumar [25] assess performance parameters without standardised benchmarking tools, while Sandhiya and Suresh [26] propose load-balancing algorithms that lack cross-industry scalability validation. A related strand of work by Mohd Ali et al. [27] proposes a multi-factor replica placement strategy to mitigate resource failure in cloud replication environments, addressing scalability and reliability concerns from a data-placement perspective. This approach was later extended by Mohd Ali et al. [28] through a multi-factor replica placement strategy for resource failure extenuation. However, both approaches were validated using CloudSim and have not been benchmarked against repatriated on-premises or hybrid infrastructure. Their applicability to real-world cloud repatriation therefore remains insufficiently validated across industries. No widely accepted benchmarking standard currently exists for comparing repatriated versus cloud-hosted workload performance. This lack of a shared benchmarking standard motivates the cross-study performance synthesis undertaken in this review (Table VI), which consolidates otherwise incomparable simulation-based findings into a single qualitative before-and-after comparison.

### E. Governance and Exit Strategy

Governance and exit planning are recognised as critical enablers of successful cloud repatriation. Grabski and Schmidt [16] propose a two-tier TOE-based governance model that assigns distinct technical and functional responsibilities across multi-cloud environments. eG Innovations [1] and Puppet [10] advocate for proactive exit planning to prevent uncoordinated transitions, while IDG/LHIND [8] and the Everest Group [15] demonstrate a strong correlation between governance maturity and repatriation readiness. In the Malaysian public sector context, Sallehudin et al. [29] similarly identified organisational, technological, and environmental readiness factors as key determinants of successful cloud implementation, offering an early empirical foundation for governance-driven adoption decisions. This TOE-oriented perspective has since been extended by Mohd Noh et al. [30], who applied a resource-based and TOE framework to model cloud adoption governance in the Malaysian healthcare sector, reinforcing the relevance of organisational readiness constructs beyond adoption into repatriation contexts. However, existing governance models are predominantly descriptive, offering best practices without implementation roadmaps or quantifiable maturity metrics. Mallam Ibrahim et al. [31] further note that governance and human-organisational factors remain under-modelled even in cloud adoption studies within academic institutional settings, echoing the same descriptive gap observed in repatriation-specific governance frameworks. Comparative analyses across sectors are lacking, and there is no replicable blueprint of governance that can be generalised to hybrid or public sector settings. This is the most consistent gap identified in this study and is used as the main organising theme for the integrated framework proposed in Section IV, as governance models are descriptive and non-quantifiable in all sources reviewed.

### F. Synthesis and Research Limitations

Collectively, the reviewed studies demonstrate that cloud repatriation studies have evolved across five major dimensions, as summarised in Table IV. While scholarly contributions provide theoretical insight and conceptual elaboration, industry studies offer empirically grounded operational observations. Despite this, a significant limitation remains in the literature itself: existing research has not produced a unified framework applicable to public sector contexts, where heightened data sensitivity, regulatory compliance requirements, and national

sovereignty concerns necessitate dedicated governance and security conventions. It is equally acknowledged that this review, consistent with the nature of a systematic literature review, does not itself generate new empirical or predictive data; its contribution lies in the structured cross-source synthesis of existing theoretical and industry evidence rather than in novel primary measurement. To partially offset this methodological boundary, Table IV and Table VI advance beyond simple narrative summary by cross-tabulating strengths, limitations, and solution strategies across all 20 studies, an analytical step (Section IV) that surfaces patterns, such as the disproportionate concentration of governance-related gaps, that are not explicit in any single source reviewed. Building on this synthesis, this review addresses the identified literature gaps through three contributions: the identification of CR factors, the synthesis of solution strategies, and the mapping of implementation limitations between theoretical models and real-world on-premises transition practices.

A further methodological limitation concerns the verification process underlying both the quality appraisal (Section II-D) and the thematic coding used in Fig. 6 (Section IV). In both cases, initial classification was performed by the lead author and subsequently reviewed and validated by co-authors, rather than through fully independent parallel coding from the outset. While this collaborative validation step provided a degree of cross-checking, it does not constitute formal inter-rater reliability verification. Future replications of this review would benefit from a fully independent dual-coding protocol at both the quality-appraisal and thematic-classification stages to further strengthen methodological rigour.

A related limitation concerns the heterogeneous evidential strength of the synthesized sources, which span peer-reviewed publications, industry reports, blogs, and self-published white papers with differing levels of editorial scrutiny. No differential weighting was applied based on source type; industry-reported statistics are presented alongside peer-reviewed findings as complementary rather than equivalent evidence, and readers should interpret figures from industry or vendor-affiliated sources with awareness of potential promotional framing.

### G. Cross-Factor Gap Analysis

To complement the narrative synthesis above, a Solution-to-Limitation Ratio (Gap Ratio) is computed for each CR factor by dividing the number of solution strategies proposed (Table VII) by the number of limitations identified (Fig. 8), as summarised in Table V. A ratio of 1.00 indicates that the literature has proposed at least one corresponding strategy for every limitation identified, while a ratio below 1.00 signals that limitations have outpaced concrete solution development. As shown in Table V, Cost and Economic Considerations, Security, Compliance and Sovereignty, and Vendor Lock-In and Portability each reach a Gap Ratio of 1.00, whereas Performance and Latency and Governance and Exit Strategy both return 0.75. However, this numerical parity masks a qualitative difference: Performance limitations are largely technical and partially mitigated by emerging approaches such as edge computing and selective repatriation, whereas Governance limitations are organisational and procedural, compounded by the finding that 45% of organisations lack any formal exit strategy [10]. Governance and Exit Strategy is therefore treated as the highest-priority gap for future CR framework development, consistent with the trend analysis in Section IV (RQ3). This analysis is a modest extension beyond descriptive synthesis rather than new primary empirical data, offering a reproducible basis for prioritising future research and policy attention across the five CR factors.

TABLE V. SOLUTION-TO-LIMITATION GAP RATIO ACROSS THE FIVE CR FACTORS

| CR Factor | Limitations (LC) | Solution Strategies (SC) | Gap Ratio (SC/LC) | Priority For Future Research |
|---|---|---|---|---|
| Cost and Economic Considerations | 4 | 4 | 1.00 | Moderate |
| Security, Compliance and Sovereignty | 4 | 4 | 1.00 | Moderate |
| Vendor Lock-In and Portability | 3 | 3 | 1.00 | Moderate |
| Performance and Latency | 4 | 3 | 0.75 | High |
| Governance and Exit Strategy | 4 | 3 | 0.75 | Highest |

### H. Contradictory Evidence and Interpretive Tensions

While the twenty studies reviewed are broadly consistent in identifying cloud repatriation as a strategically beneficial response to cost, security, and governance pressures, closer examination reveals three interpretive tensions that a purely convergent synthesis would obscure. First, a proactive-versus-reactive tension emerges around cost-driven decisions. Kumar [5] proposes the Cloud Right framework as a proactive workload suitability assessment conducted before migration, yet the case evidence in Fig. 5 and the account provided by Murugesan [3] show that organizations such as Dropbox, X, GEICO, and 37signals repatriated only after costs had already exceeded expectations, reflecting a reactive correction rather than proactive modelling. Second, security is simultaneously described as technically well-managed by cloud providers and as the most frequently cited repatriation trigger, accounting for 35 percent of coded mentions in Fig. 6. This is resolved on closer reading: the underlying concern is not the technical adequacy of provider security controls, but the lack of clarity in shared-responsibility arrangements between Cloud Service Providers and Cloud Service Users. Third, sources disagree on the extent of intervention needed to address vendor lock-in. BigID [19] treats existing multi-cloud adoption, already practiced by 68 percent of organizations, as a sufficient mitigation, whereas Räisänen [18] argues that without a formal exit strategy, organizations remain exposed to loss of strategic control. This review does not resolve which position holds more broadly, noting instead that the appropriate degree of intervention likely depends on organizational context and workload criticality.

These tensions indicate that the reviewed literature converges on repatriation as a significant trend but does not speak with one voice on when it should occur, what precisely

motivates security-driven decisions, or how completely vendor lock-in can be mitigated short of full repatriation. Acknowledging this strengthens rather than weakens the review's synthesis.

## IV. Findings and Discussion

This section discusses the key findings derived from the analysis of 20 selected studies related to cloud repatriation (CR). The discussion is organised around five major factors, as outlined and discussed in this study. Each factor is examined in relation to the three research questions (RQ1–RQ3) to highlight the primary factors driving CR, the limitations and solution strategies for each CR factor, and the current trends of CR studies across academic and industry literature.

RQ1: What are the factors driving cloud repatriation in recent academic and industrial studies?

Five prominent factors were identified across the recent academic and industrial studies:

*1) Cost and Economic considerations:* In both scholarly and industrial studies, cost is one of the most frequently identified drivers of cloud repatriation. George [4], Flores [20], and Murugesan [3] point out that it is a common experience in organizations to underestimate the cost of operation of the hyperscale cloud platform, and actual expenditure may exceed initial estimates by 30–40%. Egress charges, auto-scaling anomalies, orphaned resources and complex OpEx billing designs are also leading sources of cost volatility that organisations, particularly those in the public sector, cannot easily manage. Institutions that are owned by the government have another limitation, which is a rigid procurement process and an inflexible system of depreciation [32], [33], further complicating cost predictability of a cloud service in the long-term.

The empirical importance of cost-related motivations is demonstrated in Fig. 5, which compares annual savings reported by organizations that repatriated critical workloads. After departing from AWS, Dropbox reported savings of USD 75 million per year, while X (Twitter), GEICO, and 37signals each reported significant reductions in cloud operating costs following their respective repatriation initiatives [9], [13], [33]. The cost savings presented in Fig. 5 are individually reported figures drawn directly from each organization's own case-study disclosure rather than statistically pooled or averaged. As these figures originate from different reporting periods, organizational scales, and workload profiles, they are juxtaposed for side-by-side comparison and should be interpreted as illustrative case-level evidence rather than a representative or generalizable benchmark of expected repatriation savings. These practical outcomes support the literature in affirming that repatriation decisions tend to be reactive responses to accrued financial inefficiencies rather than the result of proactive economic modelling. Taken together, the findings validate that cost unpredictability, driven by egress charges, overprovisioning, and complex billing structures, remains one of the core triggers of cloud repatriation. Therefore, this financial pressure has compelled many organizations, particularly those in the public sector with rigid procurement constraints, to reassess their cloud dependencies and transition critical workloads back to on-premises infrastructure as a more cost-predictable and financially sustainable alternative.

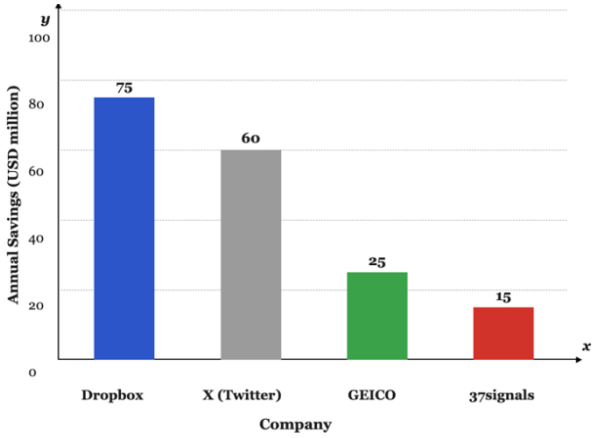


Fig. 5. Cost savings achieved through CR by various companies.

*2) Security, compliance, and sovereignty:* Security, compliance, and sovereignty are still coming out as the most powerful factors in cloud repatriation, especially in highly regulated industries. Priyanka Gowda [14] and the Everest Group [15] emphasize that companies that are under strict regulatory requirements, like the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI-DSS), must have robust auditability, end-to-end encryption, and strict data sovereignty requirements. These needs are usually beyond the capability of organizations to impose uniformly in the multi-tenant public cloud landscape. Even sovereignty issues are supported by the fact that 23% of organizations interviewed by Posey et al. [6] state that data sovereignty conflicts were a prominent factor in deciding to repatriate workloads on-premises. Also, there is a longstanding lack of clarity in shared-responsibility approaches between Cloud Service Providers (CSPs) and Cloud Service Users (CSUs), which leads to gaps in governance, particularly in such aspects as access control, data lineage, and cross-cloud visibility.

The empirical relevance of these security-related issues can be seen in Fig. 6, which summarizes the most commonly reported factors of repatriation: data sovereignty (35%), regulatory compliance (30%), data breaches and misconfigurations (20%), and vendor responsibility gaps (15%). The security-concern distribution presented in Fig. 6 was derived through thematic synthesis rather than extraction from any single source. Findings from six studies explicitly addressing security-related repatriation drivers, Posey et al. [6], Priyanka Gowda [14], Everest Group [15], BigID [19], Grabski and Schmidt [16], and the Ponemon Institute [17] were reviewed and coded into these four recurring thematic categories, and the resulting thematic frequencies were expressed as percentages of the total coded mentions across these six sources. This initial coding was performed by the lead author and subsequently reviewed and validated by co-authors; a fully independent dual-coding protocol with inter-rater

reliability verification was not conducted, and this is noted as a limitation in Section III-F. This is a reinforcement of trends evident in the literature that regulatory pressure and sovereignty assurance are the key triggers in motivating decisions of security-motivated repatriation.

*3) Vendor lock-in and portability:* Vendor lock-in is an intractable barrier to cloud agility. According to Räisänen [18] and Murugesan [3], proprietary cloud application programming interfaces (APIs), storage formats, and management tools impede workload migration and give rise to high switching costs. In the case of public-sector organizations, the problem is exacerbated by long-term vendor contracts, tough procurement policies, and data-residency requirements, all of which limit mobility. As a result, vendor lock-in represents both a technical and governance barrier that undermines organisational autonomy, reduces bargaining power, and complicates regulatory compliance.

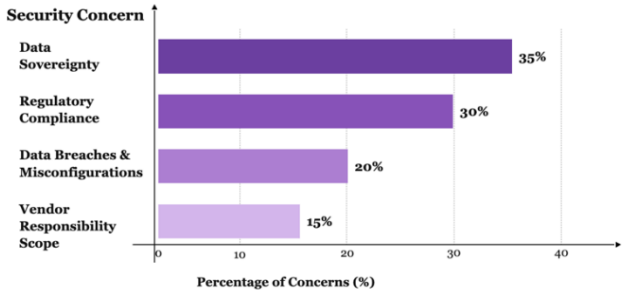


Fig. 6. Distribution of security concerns identified in CR studies.

*4) Performance and latency requirements:* The latency and performance requirements of latency-sensitive applications such as real-time analytics, artificial-intelligence inferencing, financial operations, and Internet of Things (IoT) applications are difficult to implement in public clouds due to performance and latency requirements. Latency variability is reported to range between 40 and 60 ms between cloud regions [25], [26], and Grabski and Schmidt [16], Murugesan [3] and Räisänen [18] report such inefficiencies as resource contention and multi-tenant virtualization overheads. As such, organizations are progressively embracing the idea of selective repatriation, which moves only the latency-sensitive workloads on-premises to restore deterministic performance. Table VI presents a qualitative, direction-of-change comparison synthesized from the empirical patterns and discussion described across four major works [3], [12], [25], [26]. As these studies each report performance findings using different metrics, testing environments, and measurement instruments, this review does not derive or report pooled numerical ranges. Table VI summarizes the consistent directional trend, whether improvement or deterioration, that these studies collectively describe for each metric, without implying a specific quantified magnitude common across sources. Taken together, these papers reveal that cloud-hosted workloads generally have increased latency, jitter, and packet loss as well as response time due to multi-tenant contention, hypervisor overhead, distributed routing, and unpredictable resource scheduling in the environments of a public cloud. Both Mallikarjuna and Kumar [25] and Sandhiya and Suresh [26] prove that they have lower transfer rates, lesser throughput, and worse performance under cloud congestion, which is the baseline of Before CR conditions. On the other hand, based on evidence that is given by Korada and Sikha [12]enterprises turn to the implementation of their own clouds with an express objective to achieve low latency, greater throughput, considerably better IOPS, and more predictable storage and network performance-qualifications that define the after CR values. Murugesan [3] goes on to substantiate this distinction by reporting real-life repatriation experience (Dropbox, 37signals, X/Twitter) in which enhanced control over hardware, data locality, and system configuration directly correlated to enhanced reliability, faster processing time, and cost performance optimization. Collectively, these four studies describe a consistent directional shift from the variable, contention-affected profile characteristic of multi-tenant public cloud environments toward the more predictable, locality-enhanced profile associated with repatriated on-premises or private-cloud infrastructure. It is this consistent direction of improvement, rather than any specific quantified magnitude, that constitutes the primary empirical pattern supported by the reviewed literature.

TABLE VI. QUALITATIVE PERFORMANCE COMPARISON BEFORE AND AFTER CR

| Metric | Before CR | After CR | Authors |
|---|---|---|---|
| Latency | Elevated and variable, driven by multi-tenant contention and distributed routing | Reduced and more deterministic due to local network paths | [25],[26],[12] |
| Latency Jitter | Higher variability under shared-tenancy congestion | More stable due to dedicated infrastructure | [25],[26] |
| Throughput | Constrained by shared network and storage resources | Improved via local storage and reduced contention | [25] |
| IOPS (Storage Performance) | Limited by shared multi-tenant storage backends | Higher and more predictable with dedicated enterprise storage | [12] |
| Application Response Time | Slower due to hypervisor overhead and network hops | Faster due to local infrastructure control | [25],[3] |
| Network Packet Loss | Higher due to WAN routing and cloud congestion | Lower due to local LAN environments | [25],[26] |
| Service Uptime | Subject to shared-infrastructure availability constraints | Improved through dedicated control and predictable infrastructure | [25],[3] |
| Data Processing Time | Slower, reflecting combined latency/throughput/IOPS constraints | Faster, reflecting improvements across all underlying metrics | [12],[3] |

*5) Governance and exit strategy:* The maturity of governance is always a controlling factor that spells out the success of cloud repatriation results. Grabski and Schmidt [16] highlight the use of a two-level TOE-based governance framework whereby the technical and functional roles have to be distinctly allocated in order to embrace accountability in the multi-cloud settings. But the industrial experience indicates that the structure of governance is not in general satisfactory, as a matter of fact. According to Puppet [10], about 45% of organisations do not have any formal exit strategy, and as a result, configuration drift, lack of compliance confidence, and incomplete data validation have been observed when organisations repatriate workloads. These circumstances demonstrate that one of the most prevalent underlying factors of failed or ineffective repatriation processes is governance weaknesses rather than technological constraints. The concept flow of the governance activities mentioned throughout the literature is presented in Fig. 7, which demonstrates a governance lifecycle with policy development, implementation, constant monitoring, evaluation, and a cyclic review.

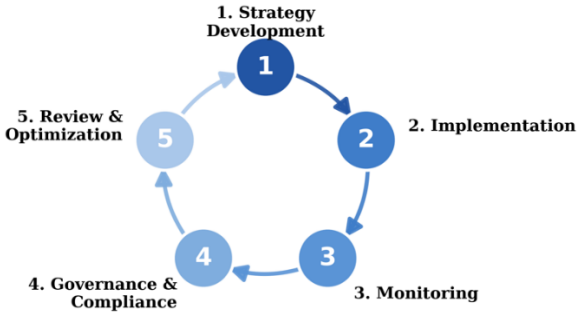


Fig. 7. Governance lifecycle.

This lifecycle underscores the fact that successful repatriation cannot work without governance as an iterative and policy-based activity as opposed to an administrative exercise that is one-time. The absence of such organised governance systems validates the obstacles mentioned in numerous research works and highlights the necessity to have standardised and actionable governance models in hybrid and multi-cloud settings.

RQ2: What are the limitations and solution strategies for each factor driving cloud repatriation towards on-premises transition?

In this section, RQ2 is addressed by systematically examining the limitations identified within the reviewed literature and the solution strategies proposed for each of the five CR factors. The consolidated findings are illustrated in Fig. 8, which contrasts theoretical limitations with real-life implementation challenges, and further mapped to the corresponding solution strategies in Table VII, which presents the corresponding solution strategies for each CR factor.

Fig. 8 illustrates the implementation gap between theoretical knowledge and industry practice across the five CR factors. Theoretical Findings (TF) from academic literature predominantly reveal conceptual and prescriptive limitations, while Real-Life Use Cases (RLUC) from industry practice expose more complex, context-specific challenges that existing frameworks have yet to adequately resolve. This juxtaposition confirms a consistent theory-practice gap, wherein academic models may underestimate the operational, contractual, and governance complexities encountered in real-world repatriation scenarios. Notably, this gap is most evident in the governance and security dimensions, where the absence of standardised implementation roadmaps and unified compliance models renders existing theoretical prescriptions insufficient for direct operational deployment.

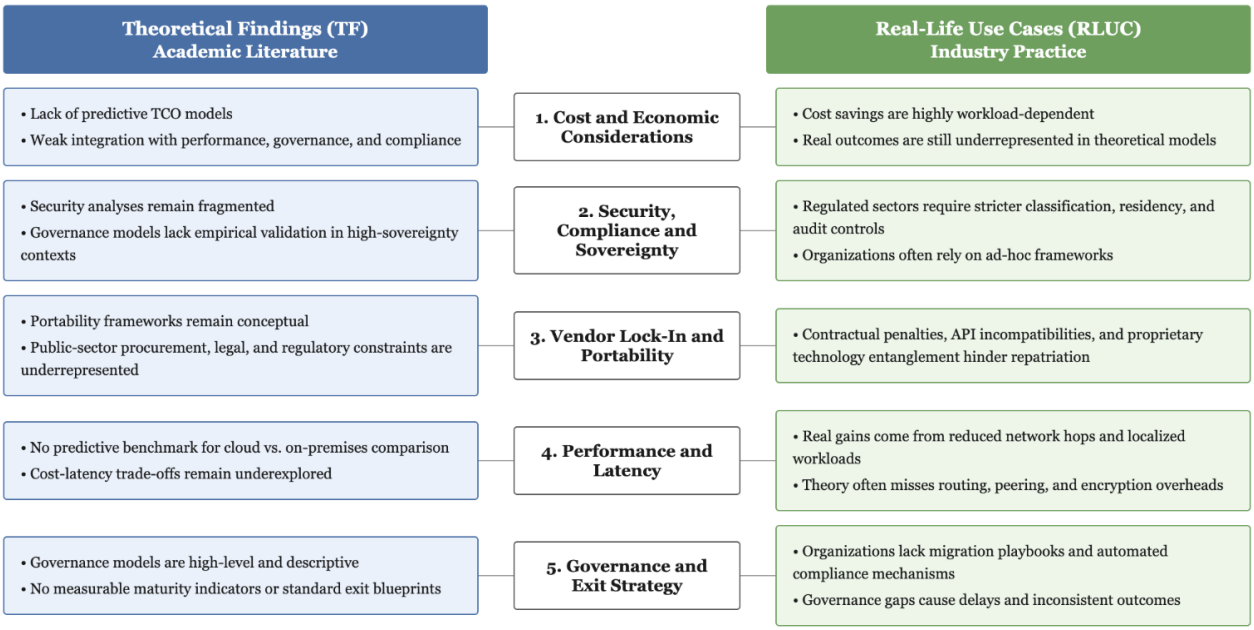


Fig. 8. Implementation limitations: theoretical findings vs real-life use cases.

TABLE VII. SOLUTION STRATEGIES CORRESPONDING TO THE FIVE CR FACTORS

| CR Factor | Solution Strategies Proposed | Authors |
|---|---|---|
| Cost and Economic Considerations | - Cloud Right methodology for workload suitability assessment<br>- Comparative TCO modelling: cloud vs. on-premises<br>- Resource rightsizing automation for continuous cost governance<br>- Balance short-term OpEx against long-term CapEx investment | [3], [5], [11] |
| Security, Compliance and Sovereignty | - TOE-based co-governance framework (CSP–CSU responsibility distribution)<br>- Sector-specific sovereign cloud models for regulated industries<br>- Automated data discovery, classification, and end-to-end encryption<br>- Continuous compliance auditing and proactive sovereignty governance | [14], [15], [16], [17], [19] |
| Vendor Lock-In and Portability | - Hybrid and multi-cloud deployment to reduce vendor dependency<br>- Cloud-agnostic technologies: Kubernetes, open APIs, and IaC<br>- Contractual portability and post-termination repatriation clauses | [6], [11], [16], [18] |
| Performance and Latency | - Selective repatriation of latency-sensitive workloads to on-premises<br>- Data locality enforcement to minimise network latency<br>- CDN, edge computing, and AI-assisted workload orchestration | [5], [6], [20], [22], [23], [26] |
| Governance and Exit Strategy | - Two-tier TOE-based governance with distinct technical and functional accountability<br>- Repatriation readiness embedded in cloud contracts (portability and audit clauses)<br>- Lifecycle-based governance: procurement, deployment, auditing, and exit planning | [1], [2], [15], [16] |

Building upon the limitations identified, Table VII consolidates the solution strategies proposed across the five CR factors, drawing from both academic recommendations and industry-based evidence. Each strategy is directly mapped to its corresponding CR factor, ensuring that the proposed interventions are specific, actionable, and responsive to the gaps identified in Fig. 8. The solution strategies presented in Table VII constitute an integrated and mutually reinforcing strategic foundation for CR decision-making. Cost strategies establish the financial justification for transition, while security and sovereignty strategies define the regulatory boundaries within which repatriation must be executed. Vendor lock-in strategies preserve organisational autonomy, performance strategies determine the technical suitability of workloads, and governance strategies provide the procedural infrastructure required to manage the entire repatriation lifecycle. Collectively, these five strategic dimensions confirm that cloud repatriation is not merely a technical migration exercise, but a multifaceted organisational policy decision that must be harmonised across regulatory, financial, operational, and technical priorities. This integrated approach is especially critical for public sector organisations, where regulatory obligations, procurement constraints, and national sovereignty requirements impose additional complexity that demands purpose-built, policy-driven frameworks.

RQ3: What is the current trend of cloud repatriation in academic and industry literature?

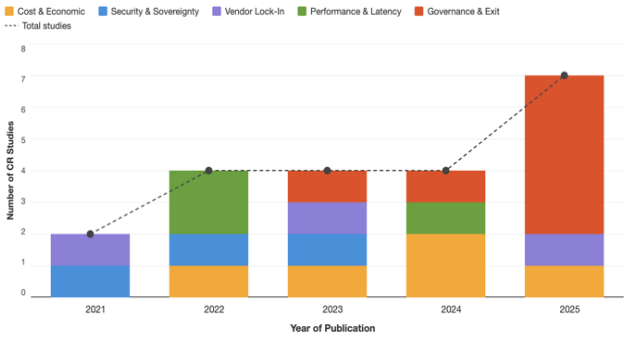


Fig. 9. Trend of CR studies by factor across academic and industry literature (2021 – 2025).

The analysis of 20 selected studies published between 2021 and 2025 reveals a discernible evolution in cloud repatriation studies, reflecting shifts in both academic focus and industry priorities across the five identified CR factors. As illustrated in Fig. 9, the distribution of CR-related studies across the review period demonstrates a progressive transition from performance and security-centred concerns toward governance and cost-driven imperatives.

### A. Trend Analysis Across the Review Period

*1) Early recognition of sovereignty and portability concerns:* In 2021, CR research was primarily represented by a small number of foundational studies. Posey et al. [6] introduced the concept of workload mobility and vendor lock-in as early drivers of repatriation interest, while Gowda [14] highlighted security and compliance challenges in BFSI cloud migrations. These early works established sovereignty and portability as the initial academic triggers of CR discourse, though empirical evidence remained limited at this stage.

*2) Performance and security as dominant themes:* The year 2022 witnessed a notable increase in academic contributions, particularly from IEEE conference publications. Mallikarjuna and Kumar [25] and Sandhiya and Suresh [26] demonstrated measurable performance superiority in on-premises environments, while Abied et al. [24] and Chang [23] examined security and service differentiation between cloud and traditional infrastructure. This period reflects a growing academic interest in empirically validating the technical limitations of public cloud environments as justification for repatriation.

*3) Cost and vendor lock-in gain industry momentum:* By 2023, industry-driven evidence began to dominate CR discourse. Jewargi [11], BigID [19], and Forbes Tech Council [21] collectively highlighted escalating cloud costs, vendor dependency, and compliance obligations as compelling repatriation triggers. The IDG/LHIND survey [8] further confirmed that security, data compliance, and migration complexity were primary motivators among enterprise decision-makers. This shift marked a transition from purely academic performance analysis toward commercially grounded

cost and portability concerns, signalling that CR was becoming a mainstream strategic consideration across multiple industries.

*4) Cost optimisation and real-world validation:* In 2024, the focus consolidated around cost optimisation and real-world repatriation outcomes. Murugesan [3] provided a comprehensive review of cloud services, highlighting the financial inefficiencies of long-term public cloud dependency, while Korada and Sikha [12] documented enterprise motivations for building private cloud infrastructure post-public cloud adoption. Flores [20] further examined the strategic and technical implications of CR for DevOps and security practices. Collectively, these works validated the financial and operational case for repatriation through empirical and case-based evidence, reinforcing cost unpredictability as a core repatriation trigger.

*5) Governance emerges as the dominant theme:* The most significant trend observed across the review period is the sharp rise in governance-oriented publications in 2025. Grabski and Schmidt [16], eG Innovations [1], [2], Puppet [10], Räisänen [18], and the IDG/LHIND study [8] collectively position governance maturity, exit strategy formalisation, and lifecycle-based compliance as the most critical enablers of successful repatriation. This concentration of governance-focused works in 2025 reflects a maturation of CR studies, moving beyond the identification of repatriation drivers toward the prescription of structured, policy-driven frameworks for managing the transition process.

## B. Overall Trend Synthesis

The longitudinal analysis of CR literature from 2021 to 2025 reveals three distinct phases of evolution in CR studies. The first phase (2021–2022) is characterised by foundational recognition of performance, security, and portability as primary repatriation triggers, predominantly within academic contexts. The second phase (2023–2024) reflects a convergence of academic and industry perspectives, with cost unpredictability and vendor lock-in emerging as dominant real-world drivers, validated through high-profile organisational cases such as Dropbox, X (Twitter), and GEICO. The third phase (2025) marks a governance turn in CR studies, wherein the field transitions from descriptive analysis of repatriation factors toward the development of prescriptive, policy-compliant frameworks suitable for regulated and public sector environments.

This evolutionary trajectory underscores the growing recognition that cloud repatriation is not a reactive technical decision, but a strategically planned organisational transition requiring integrated governance, cost modelling, and sovereignty-aware frameworks. The distribution of CR factors across the review period, as synthesised in Fig. 9, further confirms that Cost and Economic Considerations (22.7%) and Governance and Exit Strategy (22.7%) collectively represent the most critical priorities in the literature, while Security, Compliance and Sovereignty (18.2%), Performance and Latency (18.2%), and Vendor Lock-In and Portability (18.2%) reflect equally weighted but complementary dimensions of the CR research landscape. The complete classification of CR factors and their associated solution strategies is consolidated in Fig. 10, providing a structured taxonomy of the CR literature landscape identified in this review. It is acknowledged that the trend patterns described above are derived from publication counts within a bounded set of sources rather than a comprehensive bibliometric analysis, and may be influenced by factors beyond genuine shifts in research focus, such as database indexing lag and the growing tendency of industry organizations to publish repatriation-related commentary as the topic gains broader market attention. Consequently, the apparent 'governance turn' identified in 2025, and the broader three-phase trajectory described above, should be interpreted as a pattern observed within the reviewed evidence base rather than a definitive claim about the actual pace or sequence of change in cloud repatriation practice.

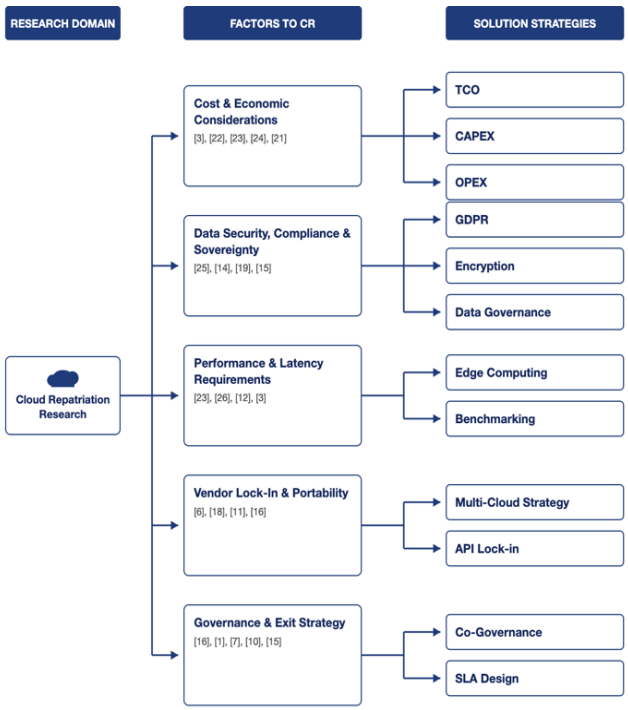


Fig. 10. CR factors and associated strategies.

# V. Conclusion and Future Works

This study conducted a systematic literature review of the factors, solution strategies, and implementation limitations associated with cloud repatriation towards on-premises environments. Based on 20 academic and industry studies published between 2021 and 2025, the findings were synthesised into five thematic areas: cost and economic considerations; security, compliance, and sovereignty; vendor lock-in and portability; performance and latency; and governance and exit strategy.

The results validate the existence and development of cloud repatriation as an organised policy decision, rather than just a technical change process. The two highest-priority areas in the reviewed studies are Cost and Economic Considerations (22.7% of the evidence base) and Governance and Exit Strategy (22.7%), while security, compliance, performance, and portability remain complementary but equally important dimensions of the current literature.

With regard to RQ1, organizations are primarily driven toward cloud repatriation due to increasing cloud costs, data sovereignty requirements, regulatory compliance pressures, vendor dependency, and performance issues when it comes to latency-sensitive applications. In public sector settings, with inflexible procurement processes and no standardised frameworks of governance, these pressures are exacerbated in real-life examples such as Dropbox, X (Twitter), GEICO, and 37signals.

For RQ2, several solution strategies are identified for each CR factor. They include predictive TCO modelling and cost governance for economic factors, TOE-based co-governance and automated compliance auditing for security and sovereignty, cloud-agnostic architectures and contractual portability provisions to mitigate vendor lock-in, selective repatriation and edge computing integration for performance needs, and lifecycle-based governance frameworks to assist in exit strategy management. Combined, they represent an integrated strategy that recognizes the need to align financial, technical, regulatory, and governance priorities together for successful repatriation.

In the context of RQ3, the longitudinal trend analysis reveals three distinct phases of CR research evolution: foundational recognition of performance, security, and portability concerns (2021–2022), convergence of academic and industry perspectives driven by cost and vendor lock-in (2023–2024), and a governance turn marked by the dominance of governance-oriented publications (2025). This trajectory confirms that CR studies are maturing from descriptive factor identification toward prescriptive, policy-driven frameworks, particularly relevant for regulated and public sector environments.

Overall, the three contributions of this review, the identification of CR factors, the synthesis of solution strategies, and the mapping of implementation limitations, offer a solid foundation for creating integrated, policy-compliant and sovereignty-aware models of CR that can be applied in private and public sector settings.

Nevertheless, this review acknowledges several limitations. The analysis is bounded by English-language sources published between 2021 and 2025, which may exclude earlier foundational works and underrepresent CR studies from non-English-speaking regions. Additionally, the predominance of private sector and Western organizational contexts in the reviewed literature may limit the generalizability of findings across diverse regulatory environments and governance structures globally. Consequently, foundational governance and portability studies published before 2021, as well as non-English-language literature that may offer region-specific insights (e.g., from Asia-Pacific or Nordic public sectors), fall outside this review's scope and represent a direction for future comparative synthesis.

Building on the gaps identified in this review, future empirical research should prioritise: 1) the development and validation of a quantifiable Cloud Repatriation Governance Maturity Index across multiple regulated public sector organisations; 2) the establishment of longitudinal cost and performance measurement instruments to compare repatriated and cloud-hosted workloads over a three- to five-year period; and 3) the conduct of cross-national comparative studies to extend the current evidence base beyond its predominantly Western and private-sector orientation. Collectively, these research directions would strengthen the empirical basis for assessing the governance maturity, long-term economic viability, and operational effectiveness of cloud repatriation in regulated public sector environments.

## ACKNOWLEDGMENT

This study is supported by the National University of Malaysia (UKM). Sincerely grateful for the facilities and funding provided, which were essential for completing this research.

## REFERENCES

[1] eG Innovations Blog, “The importance of a cloud exit strategy: What it is, who needs it, and how to plan it.” [Online]. Available: https://www.eginnovations.com/blog/the-importance-of-a-cloud-exit-strategy-what-it-is-who-needs-it-and-how-to-plan-it/

[2] eG Innovations Blog, “On-premises, cloud-first or cloud repatriation.” [Online]. Available: https://www.eginnovations.com/blog/on-premises-cloud-first-or-cloud-repatriation/

[3] G. K. Murugesan, “Cloud Services — Boon or Bane: A Comprehensive Review,” in SoutheastCon 2024, Atlanta, GA, USA: IEEE, Mar. 2024, pp. 108–112. doi: 10.1109/SoutheastCon52093.2024.10500027.

[4] A. S. George, “The Cloud Comedown: Understanding the Emerging Trend of Cloud Exit Strategies,” Partners Universal International Innovation Journal (PUIIJ), vol. 2, no. 5, Oct. 2024, doi: 10.5281/ZENODO.13993933.

[5] Subhadip Kumar, “Cloud Repatriation: A Strategic Move to Optimize IT Infrastructure and Costs,” 2024, doi: 10.13140/RG.2.2.25731.07209.

[6] D. T. Melanie Posey, “Cloud repatriation: What it is, what it isn’t, and why it’s not going away,” 2021, [Online]. Available: https://www.spglobal.com/content/dam/spglobal/mi/en/documents/general/cloud-repatriation-what-it-is-what-it.pdf

[7] CIO, CSO and COMPUTERWOCHE Research Services in cooperation with and Lufthansa Industry Solutions, “Studie Cloud-Migration 2023,” CIO, CSO und COMPUTERWOCHE, 2023. [Online]. Available: https://www.lufthansa-industry-solutions.com/de-de/studien/folgestudie-cloud-migration-2023-von-cio-cso-und-computerwoche

[8] CIO, CSO and COMPUTERWOCHE Research Services in cooperation with and Lufthansa Industry Solutions, “Studie Cloud-Migration 2025,” 2025. [Online]. Available: https://www.lufthansa-industry-solutions.com/de-en/studies/cloud-migration-2025-foundry-study-2025

[9] Sunbird, “3 Companies That Repatriated Workloads from the Cloud and Their Results.” [Online]. Available: https://www.sunbirddcim.com/blog/3-companies-repatriated-workloads-cloud-and-their-results

[10] Puppet, “Cloud Repatriation: Examples, 2025 Trends & Tips for Reverse Migration.” [Online]. Available: https://www.puppet.com/blog/cloud-repatriation

[11] K. Jewargi, “Public Cloud to Cloud Repatriation Trend,” Sch J Eng Tech, vol. 11, no. 1, pp. 1–3, Jan. 2023, doi: 10.36347/sjet.2023.v11i01.001.

[12] Laxminarayana Korada and Vijay Kartik Sikha, “Why are large enterprises building private clouds after their journey on public clouds?,” Feb. 2024, doi: 10.5281/ZENODO.13326719.

[13] David Heinemeier Hansson, “X celebrates 60% savings from cloud exit.” [Online]. Available: https://world.hey.com/dhh/x-celebrates-60-savings-from-cloud-exit-7cc26895

[14] Priyanka Gowda Ashwath Narayana Gowda, “Migrating Banking Applications to the Cloud: Strategies and Best Practices,” Dec. 2021, doi: 10.5281/ZENODO.13950711.

[15] Everest Group, “Navigating cloud portability and exit strategies in banking and financial services.” [Online]. Available: https://www.everestgrp.com/it-services/navigating-cloud-portability-and-exit-strategies-in-banking-and-financial-services-blog.html

[16] S. Grabski and P. Schmidt, "Multi-Cloud Environments and Governance: Repatriation or Expansion?," presented at the Hawaii International Conference on System Sciences, 2025. doi: 10.24251/HICSS.2025.713.

[17] Ponemon Institute LLC, "The Cost of Cloud Compromise and Shadow IT," Ponemon Institute LLC, Apr. 2021. [Online]. Available: https://www.proofpoint.com/us/resources/analyst-reports/cost-of-cloud-compromise-and-shadow-it

[18] I. Räisänen, "Cloud Repatriation: factors and strategies for successfully and beneficially leaving the public cloud:," 2025, [Online]. Available: https://urn.fi/URN:NBN:fi:tuni-202502031930

[19] BigID Blog, "Cloud migration trends and statistics 2023." [Online]. Available: https://bigid.com/blog/cloud-migration-trends-and-statistics-2023/

[20] F. Jose Eduardo, "Cloud Repatriation: Strategic Considerations, Technical Impacts, and the Future of DevOps and Security," Sep. 2024, [Online]. Available: https://www.academia.edu/124182751/Cloud_Repatriation_Strategic_Considerations_Technical_Impacts_and_the_Future_of_DevOps_and_Security

[21] Forbes Tech Council, "The rise of cloud repatriation: Why companies are bringing data in-house." [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2023/04/18/the-rise-of-cloud-repatriation-why-companies-are-bringing-data-in-house/

[22] InfoWorld, "Why companies are leaving the cloud." [Online]. Available: https://www.infoworld.com/article/2336102/why-companies-are-leaving-the-cloud.html

[23] H. Chang, "The Differences and Advantages between Cloud Services and Traditional Services," in 2022 8th Annual International Conference on Network and Information Systems for Computers (ICNISC), Hangzhou, China: IEEE, Sep. 2022, pp. 497–499. doi: 10.1109/ICNISC57059.2022.00104.

[24] O. Abied, O. Ibrahim, and S. N.-I. Mat Kamal, "Adoption of Cloud Computing in E-Government: A Systematic Literature Review," JST, vol. 30, no. 1, pp. 655–689, Jan. 2022, doi: 10.47836/pjst.30.1.36.

[25] B. Mallikarjuna and M. Kumar, "Analysis of the Performance, Scalability, Availability, and Security of Cloud Computing in Different Cloud Environments," in 2022 International Conference on Futuristic Technologies (INCOFT), Belgaum, India: IEEE, Nov. 2022, pp. 1–7. doi: 10.1109/INCOFT55651.2022.10094446.

[26] V. Sandhiya and A. Suresh, "Analysis Of Performance, Scalability, Availability And Security In Different Cloud Environments For Cloud Computing," in 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India: IEEE, Jan. 2023, pp. 1–7. doi: 10.1109/ICCCI56745.2023.10128351.

[27] Fazlina Ali, M. M. Daud, H. Sallehudin, N. A. M. Yunus, A. Ahmad, and S. S. Hussein, "Multi-Factor Replica Placement Strategy for Resource Failure Extenuation in Cloud Replication Environment," IEEE Access, vol. 13, pp. 187552–187563, 2025, doi: 10.1109/ACCESS.2025.3625943.

[28] M. A. Fazlina, R. Latip, H. Ibrahim, and A. Abdullah, "Replication Strategy with Comprehensive Data Center Selection Method in Cloud Environments," Computers, Materials & Continua, vol. 74, no. 1, pp. 415–433, 2023, doi: 10.32604/cmc.2023.020764.

[29] H. Hasimi Sallehudin, R. Che Razak, M. Ismail, A. F. Md Fadzil, and R. Baker, "Cloud Computing Implementation in The Public Sector: Factors and Impact," APJITM, vol. 07, no. 02(02), pp. 27–42, Dec. 2018, doi: 10.17576/apjitm-2018-0702(02)-03.

[30] N. M. Noh, N. S. M. Satar, H. Sallehudin, I. H. Mallam, and S. S. Hussein, "Modelling Cloud Computing Adoption in the Malaysian Healthcare," International Journal of Advanced Computer Science and Applications, vol. 16, no. 7, 2025.

[31] H. M. Ibrahim, K. Ahmad, and H. Sallehudin, "Understanding the technology and humans as determinants of cloud computing adoption for digital preservation of research outputs in university libraries," Educ Inf Technol, vol. 30, no. 5, pp. 6163–6211, Apr. 2025, doi: 10.1007/s10639-024-13027-w.

[32] Edward Targett, "GEICO repatriates work from the cloud, continues ambitious infrastructure overhaul." [Online]. Available: https://www.thestack.technology/warren-buffetts-geico-repatriates-work-from-the-cloud-continues-ambitious-infrastructure-overhaul/

[33] Antony Panteli, "Why cloud repatriation is back on the CIO agenda." [Online]. Available: https://www.cio.com/article/4061031/why-cloud-repatriation-is-back-on-the-cio-agenda.html