An Analysis of Enterprise-Level Cloud Transition Barriers within the Technology-Organization-Environment (TOE) Framework and Strategic Solution Proposals

Araştırma Makalesi/Research Article

Baris CELIKTAS[1], Berat BIRGIN[2]*, Mevlut Serkan TOK[3]

[1]Department of Computer Engineering, Isik University, Istanbul, Turkey
[2]Department of Computer Engineering, Isik University, Istanbul, Turkey
[3]Department of Information Security, Gazi University, Barikat Siber Güvenlik, Ankara, Turkey

baris.celiktas@isikun.edu.tr, 24sibe5002@isik.edu.tr, mevlutserkan.tok@gazi.edu.tr
(Geliş/Received:17.04.2025; Kabul/Accepted:07.10.2025)
DOI: 10.17671/gazibtd.1678237

***Abstract*—** Enterprise-level transitions to cloud service providers are frequently delayed or disrupted due to the multi-layered nature of technical, organizational, and legal barriers. This study classifies these obstacles within the Technology-Organization-Environment (TOE) theoretical framework and provides a comprehensive analysis. Methodologically, a triangulated data source approach was adopted, combining systematic literature review, the 2025 Flexera Cloud Report, and Cloud Adoption Framework (CAF) documentation from major providers such as AWS, Azure, and Google Cloud. Findings indicate that technological barriers particularly cryptographic complexity, cost unpredictability, and weak system integration, are the most dominant. These barriers were visually modeled, and the structural interdependencies among five core cryptographic components (key management, secure computation, algorithm selection, access control, and regulatory compliance) were illustrated through a flow diagram. By aligning FinOps and compliance-oriented solution strategies with the TOE framework, the study offers a strategic roadmap for decision-makers and cloud architects planning cloud adoption. It links conceptual models to applied practices, providing structured support for organizations seeking to mature their cloud strategy.

***Keywords*—** cloud computing, technology-organization-environment (TOE) framework, cryptographic challenges, FinOps strategies, regulatory compliance, system integration

Kurumsal Düzeyde Bulut Servis Sağlayıcılarına Geçiş Süreçlerinde Teknoloji-Örgüt-Çevre Çerçevesiyle Engellerin Analizi ve Stratejik Çözüm Yaklaşımları

***Özet*—** Kurumsal düzeyde bulut servis sağlayıcılarına geçiş süreçleri, teknik, örgütsel ve yasal boyutlarda karşılaşılan çok katmanlı engeller nedeniyle sıklıkla yavaşlamakta ya da sekteye uğramaktadır. Bu çalışma, söz konusu engelleri Teknoloji-Örgüt-Çevre (TÖÇ) çerçevesi kapsamında sınıflandırmakta ve bütüncül bir analiz sunmaktadır. Araştırma yöntemi olarak, sistematik literatür taraması, 2025 Flexera Cloud raporu ve AWS, Azure, Google Cloud gibi önde gelen bulut servis sağlayıcıların Cloud Adoption Framework (CAF) dokümanları temel alınarak üçlü bir veri kaynağı yaklaşımı benimsenmiştir. Bulgular, özellikle kriptografik karmaşıklık, maliyet belirsizliği ve sistem entegrasyonundaki zayıflıklar gibi teknolojik engellerin en baskın kategoriler olduğunu ortaya koymaktadır. Bu engellerin dağılımı görsel olarak modellenmiş, ayrıca anahtar yönetimi, güvenli hesaplama, algoritma seçimi, erişim kontrolü ve regülasyon uyumluluğu gibi beş temel kriptografik unsur arasındaki yapısal bağımlılıklar bir akış modeliyle ortaya konmuştur. Çalışma, TÖÇ çerçevesiyle hizalanan FinOps ve yasal uyum odaklı çözüm stratejilerini bir araya getirerek, bulut geçişini planlayan karar vericilere ve çözüm mimarlarına stratejik bir yol haritası sunmaktadır. Kavramsal çerçeveleri uygulamaya dönük modellerle ilişkilendirerek, bulut stratejisini olgunlaştırmak isteyen karar vericilere ve mimarlara yapısal bir destek sunmaktadır.

***Anahtar Kelimeler*—** bulut bilişim, teknoloji-örgüt-çevre çerçevesi, kriptografik zorluklar, FinOps stratejileri, regülasyon uyumu, sistem entegrasyonu

1. INTRODUCTION

Cloud computing has revolutionized how organizations manage IT infrastructure by providing on-demand access to shared, scalable resources via the internet [1], [2], [3]. Its core advantages (scalability, cost-efficiency, and elasticity) have attracted a diverse spectrum of users, ranging from large enterprises to small and medium-sized enterprises (SMEs) and independent developers [2], [4], [5]. Despite this promise, cloud adoption remains complex due to technical and organizational uncertainties such as integration challenges, regulatory obligations, and internal resistance [4], [6], [7]. NIST defines five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [3]. However, studies suggest these features alone do not ensure success, particularly in security-sensitive sectors like healthcare and finance [5], [8], [9]. The true strength of the cloud lies in its architecture: virtualization, orchestration, and automation decouple services from physical hardware, enabling operational efficiency [1], [2], [3], [10]. This shift has transformed the IT roles, pushing traditional administrators toward service-focused analysis [4], [11].

Cloud services are commonly delivered through three main models: Infrastructure as a Service (IaaS), which provides virtualized hardware resources; Platform as a Service (PaaS), which offers a development environment with tools and libraries; and Software as a Service (SaaS), which delivers ready-to-use applications managed by the provider [1], [3]. In terms of deployment, private clouds are used exclusively by single organization and offer greater control; public clouds are shared across multiple users and optimized for cost-efficiency; hybrid clouds combine private and public infrastructures to balance security and scalability; and community clouds serve a group of organizations with shared goals or compliance needs [3], [12], [13]. Financially, the pay-as-you-go model reduces capital expenditure and supports flexible resource allocation [1], [2], [9].

While cloud models promise architectural flexibility and economic benefits, their implementation in real-world settings is often far more complicated. Despite the cloud's architectural advantages and economic appeal, significant barriers persist. These include vendor lock-in, performance volatility, data loss risks, and cryptographic limitations [7], [8], [13], [14]. Most critically, data security and privacy concerns remain the top inhibitors, up to 88% of organizations cite them as reasons for delayed adoption [9], [15], [16]. Moreover, internal resistance and poor change management can undermine otherwise technically ready transitions [4], [5], [6]. Legal frameworks like GDPR and HIPAA complicate compliance, turning cloud adoption into a strategic challenge rather than a merely technical one [10], [17], [18]. Emerging threats such as APTs, insider risks, and inter-tenant vulnerabilities have prompted the exploration of advanced cryptographic tools, including fully homomorphic encryption (FHE), attribute-based encryption (ABE), and zero-knowledge proofs (ZKP) [9], [13], [19], [20].

This study aims to identify key barriers to cloud adoption, evaluate academic and industrial solution strategies, and offer actionable recommendations for secure, scalable, and efficient implementation [2], [11], [21].

This study makes three key contributions to the literature:

- We propose a triangulated research methodology that integrates academic literature (2019–2025), industry insights (Flexera 2025), and provider-specific CAFs. While prior studies typically rely on single-source frameworks or isolated perspectives, this study introduces a TOE-anchored analytical model that unifies these three dimensions into a coherent, actionable structure for analyzing cloud transition barriers.
- While the traditional TOE framework effectively classifies barriers into technological, organizational, and environmental domains, it lacks the granularity needed to capture the cryptographic, compliance, and cost-governance dynamics critical in cloud-era migrations. We extend the classical TOE framework into a TOE-anchored analytical model by integrating cryptographic and regulatory sub-barriers. This approach deconstructs security into discrete, addressable components aligned with each TOE dimension, allowing a more precise and actionable barrier analysis.
- We benchmark the Cloud Adoption Frameworks (CAFs) of AWS, Azure, and Google Cloud against recent empirical case studies, including the Ukraine Government & Banking Migration, CLOUD Act compliance in EU institutions, NHS hybrid cloud transition, TSB Bank migration failure, and EU Banking Authority pilot projects. The comparison highlights unresolved gaps such as vendor lock-in, SLA opacity, and limitations in encryption-based data control. These insights strengthen the operational relevance of our TOE-anchored analytical model by linking its theoretical dimensions with empirically validated challenges in enterprise-level cloud adoption.

These contributions jointly address a critical gap in cloud migration research: the absence of an integrated, cryptographically-aware, and empirically grounded model that bridges theory with actionable practice.

The remainder of this paper is structured as follows:

- Section 2 explains the research methodology, including the data sources and use of the TOE framework.
- Section 3 classifies barriers to cloud adoption into technological, organizational, and regulatory categories, with a specific focus on cryptographic dependencies.

- Section 4 presents comprehensive, targeted solution strategies derived from literature, industry reports, and provider frameworks, each directly addressing the barriers identified in Section 3.
- Section 5 presents a barrier-solution mapping matrix aligned with TOE dimensions.
- Section 6 discusses the study's limitations, analytical implications, and the need for dynamic, sector-aware adaptation of the proposed model.
- Section 7 concludes with key insights and future research directions on trust, compliance, and sector-specific strategies.

2. METHODOLOGY

This study employs a hybrid qualitative research design structured in three interrelated phases:

- Systematic identification of barriers to the cloud adoption
- Development of solution strategies from diverse sources
- Cross-validation and mapping of the relationships between barriers and proposed solutions

The overall approach is grounded in the TOE framework and supported by thematic content analysis techniques.

2.1 Research Design

This study adopts a descriptive-exploratory approach grounded in qualitative content analysis. A total of 29 peer-reviewed academic studies (2019–2025) were selected from IEEE, ACM, SpringerLink, and Scopus based on credibility, cloud relevance, and empirical validity. While the primary dataset emphasizes post-2019 publications, a limited number of pre-2019 seminal works were retained due to their foundational influence on cryptographic models and cloud security paradigms [22], [23]. To strengthen practical applicability, data was triangulated with the Flexera 2025 industry report [24], CAF from AWS, Azure, and Google Cloud, and five international case studies. Certain operational data points, such as those reported in vendor case studies (e.g., Nordcloud for NHS), were not independently audited. These sources were cross-verified where possible, but may reflect provider perspectives and thus constitute a methodological limitation.

The analytical backbone of this study is the TOE framework, which enables a structured examination of cloud adoption challenges across three dimensions: technological, organizational, and environmental. Originally designed to assess innovation adoption, TOE is well-suited for analyzing complex transitions such as cloud migration due to its integrative structure.

In this study, the classical TOE model is extended into a TOE-anchored analytical model by incorporating two additional lenses: cryptographic sub-barriers and regulatory dependencies. This expanded structure allows for a more granular mapping of challenges that are both technical and institutional, particularly those related to encryption, key management, and compliance. Each barrier and corresponding solution (discussed in Sections 3 and 4) is evaluated through this enhanced TOE lens to preserve both analytical rigor and sectoral relevance.

2.2 Thematic Analysis Approach

Academic sources were analyzed thematically. Barriers were manually coded based on type, frequency, sectoral context, and proposed solutions. These codes were then grouped into four TOE-based categories: Technological, Organizational, Environmental/Regulatory, and Cryptographic-Security. The classification was cross-validated against prior taxonomies by Oliveira [25] and Gangwar [4] to ensure consistency. As illustrated in Figure 1, cloud computing adoption barriers are categorized under the TOE framework, which distinguishes challenges into technological, organizational, and environmental domains.

Each domain encapsulates thematically distinct challenges encountered by organizations during cloud migration. Technological factors include infrastructure, interoperability, and cryptographic issues. Organizational barriers stem from human, cultural, and financial immaturity. Environmental factors reflect legal, regulatory, and jurisdictional complexity.

To address the increasingly central role of encryption in cloud operations, this study extends the classical TOE framework by introducing a fourth analytical domain, referred to as Cryptographic Challenges. This new category captures sub-barriers such as key management, secure computation, and post-quantum uncertainty, which do not fully align with the traditional TOE triad but nonetheless critically influence adoption outcomes.

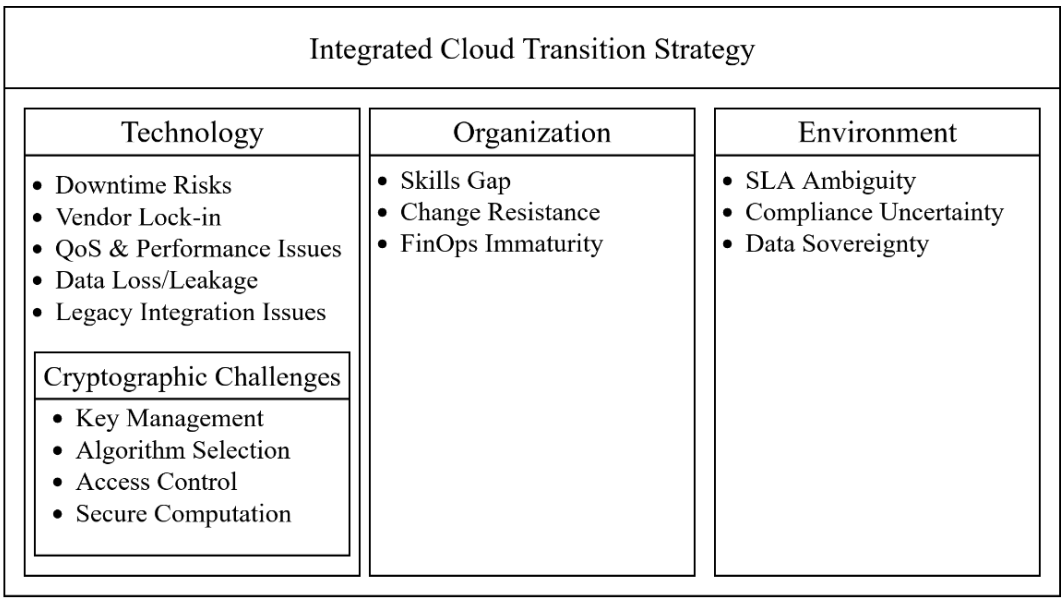

Figure 1. Cloud Adoption Barriers Classified under TOE Framework

Figure 2 indicates that technological challenges are weighted more heavily than organizational or environmental ones, particularly in areas such as performance and cryptography. Scores were normalized on a 1–5 scale using this study's thematic analysis, citation frequency, and Flexera 2025 insights.

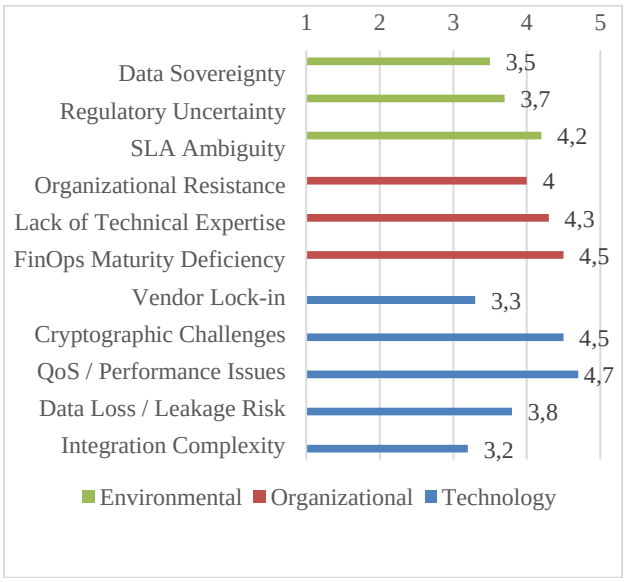

Figure 2. Weighted Distribution of Cloud Adoption Barriers by TOE Category

Figure 3. presents a comparative analysis of key cryptographic challenges in cloud adoption. Each sub-barrier is scored on a normalized 1–5 scale, based on this study's thematic focus, academic citation frequency, and Flexera 2025 insights. While all five are critical, regulatory compliance and key management stand out due to their combined technical complexity and organizational impact.

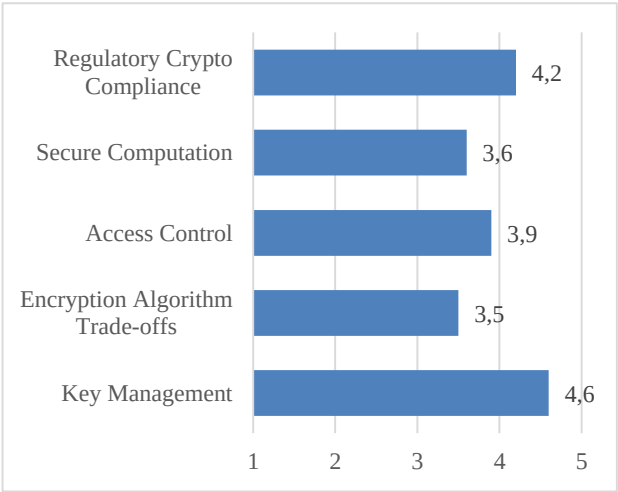

Figure 3. Weighted Evaluation of Cryptographic Adoption Challenges

2.3 Industry-Level Triangulation

To validate academic findings, the Flexera 2025 report, based on a global survey of 759 IT executives, was analyzed. Insights were mapped onto the academic taxonomy to reveal convergence and highlight underrepresented themes such as FinOps maturity and license waste. This step reinforced the practical relevance of the theoretical model.

2.4 Empirical Case Synthesis

To contextualize the identified barriers, five high-impact case studies were selected for their sectoral diversity and illustrative value: Ukraine Government & Banking Migration (data sovereignty and resilience under conflict),

CLOUD Act compliance in EU institutions (jurisdictional compliance and data access mandates), NHS Hybrid Cloud Transition in the UK (legacy integration and uptime management), TSB Bank Core Migration Failure (inadequate testing and vendor oversight), and EU Banking Authority pilot projects (multi-jurisdiction compliance and vendor lock-in). Each case was thematically mapped to the barrier taxonomy, strengthening the empirical grounding and validating the proposed solution model.

2.5 CAF Benchmarking

CAF documents from AWS, Azure, and Google Cloud were benchmarked based on their coverage of key barriers: fully addressed, partially addressed, or omitted. Azure leads in governance, SLA clarity, and regulatory compliance [76]. AWS excels in training and security but lacks legal and performance depth [75]. Google focuses on culture and resilience yet underrepresents technical and cryptographic concerns [77]. None sufficiently address vendor lock-in or homomorphic encryption.

Table 1 illustrates the relative strengths and blind spots of AWS, Azure, and Google CAFs across key evaluation dimensions such as cost governance, security depth, and cryptographic support. This benchmarking is based on a structured review of official provider documentation [75], [76], [77]. While each CAF provides value in specific domains, such as Azure in compliance, AWS in financial operations, and Google in organizational change, they all fall short in offering integrated strategies for cryptographic governance, SLA enforcement, and vendor neutrality. These gaps reveal the absence of a unified model capable of mapping real-world inhibitors to actionable solutions. Hence, this study proposes a TOE-anchored model to bridge the divide between provider guidance and operational realities.

Table 1. CAF Benchmarking Based on TOE-Anchored Evaluation Criteria

Evaluation Criteria	**AWS CAF [75]**	**Microsoft Azure CAF [76]**	**Google Cloud CAF [77]**
Security & Compliance	Strong in IAM and encryption guides; lacks legal compliance depth	Comprehensive governance module; strong in SLA/regulatory mapping	Cultural & team resilience focus; weaker on legal/technical measures
Cost Management	Provides CFM tools, basic budgeting	Mature FinOps structure, cost control dashboards	Basic recommendations; less structured
Organizational Readiness	Cloud fluency training; no detailed change management roadmap	Detailed change management, stakeholder alignment modules	Focus on “CCoE” and cultural readiness
Technical Depth	Strong on infra/security; weak on crypto & key management	Moderate technical detail; limited key lifecycle management	Lacks low-level technical/crypto support
Vendor Lock-in Strategy	Not directly addressed	Not addressed	Not addressed
Monitoring & Automation	Emphasizes automation and infrastructure templates	Integrated monitoring tools and automation patterns	Focuses on agility; lacks monitoring depth
Documentation Accessibility	Extensive, but modular and fragmented	Well-structured and scenario-oriented	Narrative-driven, use-case centric
Sectoral Fit	Enterprise and gov-centric	Enterprise, SME and hybrid-friendly	Startup and developer-oriented

2.6 Solution Strategy Extraction

Proposed solution strategies integrate findings from academic research, industry reports, CAFs, and case studies, ensuring recommendations are both theoretically grounded and practically relevant.

2.6.1 Academic Literature-Based Solutions

The reviewed literature not only identifies key technical and organizational barriers but also proposes recurring solutions. For technological issues, studies highlight infrastructure modernization, QoS-based performance models, and orchestration tools like Cloud Migration Orchestrator [26], [22]. Organizational gaps are addressed through training programs, managerial awareness campaigns, and structured change management strategies [27], [28], [29]. Simulation models such as HySOR are recommended to clarify SLA expectations and negotiate risk-sharing in hybrid contracts [30]. For cryptographic and data security challenges, advanced methods like Attribute-Based Encryption (ABE) and blockchain-based EHR systems offer fine-grained control and tamper-proof sharing [31], [32]. However, gaps remain. The literature provides limited guidance on vendor lock-in and SME-specific financial barriers, revealing a disconnect between theoretical models and practical implementation needs. The relationship between categorized barriers and corresponding solution domains is summarized in Table 2.

Table 2. Summary of Reviewed Studies: Limitations, Barriers, and Proposed Solutions

Citation	Study Limitation	Identified Barrier	Proposed Solution
İbrahim et al. (2025) [27]	Difficulty evaluating human-technology interaction	Lack of technical expertise, outdated software/hardware	Technical training and expert participation
Munjal et al. (2025) [33]	Complexity in trust-based multi-cloud resource allocation	Technical (Security, Latency, Distributed system complexity)	TASSO (Trust-Aware Spring Search Optimization)
El Skafi et al. (2025) [34]	Theoretical modeling, lack of real-world data	Security, compliance, complexity, management	Consulting, SLA transparency, technical training
Kitsiou et al. (2025) [36]	Inadequate developer tools	Privacy and technical design limitations	Developer tool upgrades and guideline development
Qatawneh (2024) [28]	Lack of empirical, user-supported public sector analysis	Complexity, security, cost, managerial gap	IT awareness training and infrastructure alignment
Soto et al. (2024) [29]	Education-sector-specific limited analysis	Budget constraints, lack of expertise, data sovereignty	Phased transition and staff training
Seifert & Kuehnel (2024) [30]	Hybrid cloud SLA unreliability and risk sharing	Environmental, SLA uncertainty	HySOR simulation model
Nowrozy et al. (2024) [31]	Limited health sector study	EHR security, organizational compliance issues	Attribute-based encryption, blockchain-based solutions
Kotulski et al. (2024) [35]	Sector-specific SLA requirements complexity	Digital sovereignty, Vendor lock-in, Sectoral requirements	Spectrum-based education model
Santos et al. (2024) [37]	Limited empirical content analysis	Security, compliance, complexity, management	Security framework design and regulatory-aligned strategies
Ukeje et al. (2024)[40]	Lack of solution suggestions in the literature	Data security, data privacy, legal compliance	Gap in literature (no solution)
Seifert et al. (2023) [12]	Lack of SLA standards, inadequate analytical depth	SLA standardization issues, QoS uncertainty	SLA templates, contract management tools
Guo et al. (2023) [38]	SME-specific generalization problems	Modularity, SME-specific resource issues	SOA modular architecture and strategic IT planning
Kavre et al. (2023) [39]	Lack of differentiation in integration issues	Technological diversity, strategic alignment	Blockchain and IoT integration, training programs
He et al. (2023) [41]	Overtechnical focus, usability limitations	Migration delays, risk of failure	Predictive algorithms, adaptive SON, SLA flexibility
Zhang et al. (2022) [11]	Specific, sector-based findings	Latency, bandwidth, multi-region challenges	VPN, fiber use, regional cloud distribution
Ahmad et al. (2021) [26]	Narrow case-based review	QoS gaps, poor dynamic management	VM optimization, energy-QoS tradeoffs
Akremi & Rouached (2021) [42]	Weak technical details in modeling	Lack of control, auditability, organizational concerns	Encryption-based governance models
Li et al. (2021) [43]	Omission of pricing factors	Weak infrastructure, poor cost governance	Standard service catalogs, agile pricing models
Mostajabi et al. (2021) [44]	Lack of field data	Data model mismatch, legacy systems	Unified data models and auto-conversion tools
Singh et al. (2021) [45]	Inapplicability due to sector-specific focus	Infrastructure immaturity, privacy, SLA conflict	Feasibility analysis, strategic roadmap
Alshdadi et al. (2020) [32]	Single case focus	Low cloud maturity, poor adaptation	SWOT-based CMRA analysis
Almaiah & Al-Khasawneh (2020) [46]	Limited sample from educational institutions	Security concerns, weak cloud perception	Cloud security awareness programs
Pei-Fang Hsu (2020) [47]	General application limitations	Security, lock-in, cost risk	Design guide, IT role restructuring
Anadiotis et al. (2020) [48]	Technical metrics insufficient for scaling	Elasticity problem, resource planning issues	Elastic resource allocation, new system architecture
Alassafi et al. (2019) [49]	Superficial analysis of security factors	Security weaknesses, limited encryption	Security architecture, user-defined encryption
Ahmed et al. (2019) [50]	General trust-based theory	Lack of federation support, transparency issues	Federated trust and transparency mechanisms
Hwang et al. (2016) [22]	Overly focused on large enterprise scale	Heterogeneous legacy issues	Cloud Migration Orchestrator (CMO), BPM support
Himmel & Grossman (2014) [23]	Compliance coverage weak	Hypervisor risks, multi-tenancy, flexibility limits	Security disclosures, SLA constraints, forensic controls
Note: The reviewed studies are organized in chronological order to illustrate the evolution of research perspectives between 2019 and 2025.			

2.6.2 Industry Reports Insights

The Flexera 2025 report, based on input from 750+ IT leaders, supports academic findings while offering actionable practices. It promotes forming FinOps teams, adopting Zero Trust models, accelerating certifications, and negotiating SLAs collaboratively. These strategies are crucial for SMEs and hybrid/multi-cloud users. Unlike theoretical models, Flexera provides tactical checklists with immediate organizational relevance.

2.6.3 Provider-Centric Frameworks (CAF)

Major providers (AWS, Azure, and Google Cloud) offer CAFs to guide cloud migration, but each has gaps:

- AWS emphasizes operations, IAM, encryption, and training via Cloud Financial Management. It lacks depth in vendor lock-in and cryptographic integration [75].
- Azure excels in governance, legal compliance, SLA templates, and FinOps. However, key management and encryption modeling are underdeveloped [76].
- Google Cloud focuses on cultural change (Learn & Lead, CCoE) but provides limited technical and regulatory guidance [77].

None adequately address vendor lock-in, data portability, or performance-security trade-offs like those in Fully Homomorphic Encryption (FHE). This underscores a disconnect between provider frameworks and real-world complexity.

2.6.4 Lessons from Real-World Case Studies

Empirical case studies provide essential validation for the proposed barrier–solution framework by demonstrating how migration challenges manifest in operational settings and how mitigation strategies are implemented under real constraints. The following high-impact cases, spanning government, healthcare, finance, and multi-jurisdictional governance, offer sector-specific evidence of how technological vulnerabilities, organizational readiness gaps, and environmental pressures interact. Each example integrates quantitative outcomes with TOE framework dimensions, strengthening both the practical applicability and the originality of this study's findings.

Table 3. Summary of selected real-world cloud migration cases.

Case	**Sector**	**Primary Barrier**	**Solution Strategy**
Ukraine Government & Banking Migration	Government / Finance	Data sovereignty, operational resilience under conflict	Multi-region redundancy, end-to-end encryption, conflict-specific disaster recovery
CLOUD Act Compliance in EU Institutions	Finance / Healthcare	Jurisdictional compliance, data access mandates	Sovereign cloud, localized key management, jurisdiction-specific access control
NHS Hybrid Cloud Transition (UK)	Healthcare	Legacy integration, uptime during migration	Zero-trust architecture, sector-specific encryption, staged migration
TSB Bank Core Migration Failure (2018)	Finance	Inadequate testing, weak rollback mechanisms	Phased migration, real-time rollback, vendor oversight
EU Banking Authority Pilot Projects	Finance	Multi-jurisdiction compliance, vendor lock-in	Advanced encryption, multi-cloud strategy, cross-border governance

2.6.4.1 Ukraine Government & Finance Migration

Following the escalation of the Russia–Ukraine armed conflict in 2022, Ukraine migrated over 4,000 essential public services to hyperscale cloud platforms within six weeks. These services included tax, healthcare, and national registry systems, ensuring data sovereignty and operational continuity amid kinetic and cyber threats. As documented by Aviv and Ferri (2023) [78], the strategy relied on multi-region redundancy, end-to-end encryption, and conflict-specific disaster recovery protocols, achieving 99.8% uptime in the first six months. This case illustrates the environmental dimension of the TOE framework through sovereignty safeguards, the technological dimension through resilience engineering, and the organizational dimension via rapid cross-agency coordination with private-sector partners.

2.6.4.2 CLOUD Act Compliance (USA)

The U.S. CLOUD Act introduced legal provisions enabling government agencies to request data stored overseas by U.S.-based cloud providers. This created immediate jurisdictional and compliance challenges for organizations handling sensitive or regulated data. Enterprises in finance, healthcare, and defense sectors responded by adopting sovereign cloud architectures, implementing localized encryption key management, and conducting legal risk assessments to align storage and access policies with jurisdiction-specific mandates. This case underscores the environmental dimension of the TOE model through regulatory pressures, as well as the technological dimension via secure key localization and data segmentation [79].

2.6.4.3 NHS Cloud Transition (UK)

The UK National Health Service (NHS) initiated a large-scale migration to hybrid cloud infrastructure to modernize patient data management and improve service availability. As reported by the UK National Audit Office (2022) [80], the project encompassed over 500 NHS organizations, aiming to integrate legacy electronic health record (EHR) systems with cloud platforms while maintaining

compliance with the Data Security and Protection Toolkit. Key measures included zero-trust network architectures, sector-specific encryption protocols, and staged migration schedules, which reduced service downtime to under 0.5% during critical phases. This case demonstrates the technological dimension via secure architecture deployment, the organizational dimension through coordinated change management, and the environmental dimension through adherence to healthcare data mandates.

2.6.4.4 TSB Bank Cloud Migration (UK)

In April 2018, TSB Bank initiated the migration of its core banking platform to a new IT infrastructure intended to improve scalability, resilience, and service delivery. However, the transition was marred by prolonged outages, transaction errors, and customer access failures, affecting millions of accounts. The FCA Final Notice (2024) [81] highlights deficiencies in pre-migration testing, risk assessment, and vendor oversight, as well as inadequate contingency planning. These operational weaknesses led to significant reputational damage, regulatory sanctions, and costly remediation programs. From a TOE perspective, this case exemplifies technological risks linked to insufficient system validation, organizational gaps in change governance, and environmental pressures from post-incident regulatory scrutiny [81].

2.6.4.5 European Banking Authority Pilot Projects (EU)

The European Banking Authority's (EBA) pilot initiatives on cloud adoption in the EU financial sector focused on ensuring compliance with multi-jurisdictional regulations, safeguarding sensitive financial data, and managing vendor concentration risks. Based on the EBA Guidelines on Outsourcing Arrangements [82], participating institutions were required to implement contractual clauses ensuring audit rights, establish robust data security controls, and maintain contingency plans for critical outsourced functions. These measures aimed to align cloud migration practices with the EU's prudential, operational, and data protection requirements, addressing both technological and environmental dimensions of the TOE model [82].

2.7 Mapping of Barriers and Solutions

In the final methodology stage, barriers were systematically mapped to corresponding solution domains, linking thematic findings to practical outcomes. Each technological, organizational, or regulatory barrier was paired with strategies from literature, industry reports, and CAFs. A matrix-style alignment table was used to visualize solution points. Cryptographic challenges were divided into five sub-barriers for detailed analysis. The full mapping appears in Section 5.

3. BARRIERS TO THE ADOPTION OF CLOUD

Cloud adoption is rarely seamless. Organizations face diverse barriers, ranging from system outages and cryptographic limits to managerial resistance and regulatory ambiguity. These challenges not only delay migration but also shape its risk profile and long-term viability. To systematically examine these issues, this section applies the TOE framework as an analytical lens. Each barrier is categorized under technological, organizational, or environmental domains, with an emphasis on cryptographic sub-barriers. This classification provides the foundation for the solution strategies proposed in Section 4.

3.1. Technological Barriers

Technological barriers are among the most immediate obstacles to cloud adoption, including challenges related to availability, performance, cryptography, and interoperability. These challenges pose direct operational risks such as downtime, data loss, and integration failures. Mitigating them requires resilient architectures, precise resource management, and robust cryptographic design. The following subsections examine each domain by impact and complexity.

3.1.1 Service Unavailability and Downtime Risks

High availability is a core expectation in cloud computing, yet real-world incidents often fall short of SLA promises like 99.99% uptime. For instance, the 2021 AWS Northern Virginia outage disrupted services for hours, exposing vulnerabilities even in leading platforms [11]. Common causes include power loss, hardware failure, software bugs, and faulty automation scripts [8], [38]. These interruptions threaten not only continuity but also data integrity, especially in real-time systems in healthcare or finance, where write operations during crashes can result in irreversible inconsistencies [5], [7], [19]. While providers offer SLA guarantees, many uses vague terms such as "reasonable efforts," limiting accountability and eroding user trust [2], [16], [30]. Technically, geographically distributed backups enhance fault tolerance [1]. Yet their high cost and complexity remain a barrier for SMEs [38]. Multi-tenant environments also suffer from resource contention, where one user's overuse may throttle access for others [11].
Ultimately, service accessibility is not solely a technical challenge, but also a matter of policy clarity, design philosophy, and preparedness for failures.

3.1.2 Vendor Lock-in and Lack of Data Portability

Cloud computing provides scalability and flexibility; however, these benefits are often undermined by the risk of vendor lock-in. Organizations that become deeply dependent on a specific provider's infrastructure, APIs, or proprietary tools may encounter significant technical and financial challenges when attempting to migrate [8], [16]. The lack of standardization in data schemas, API protocols, and interfaces further reinforces this dependency, making migration slower and more prone to risk [2], [47]. Moreover, some providers limit data export through

restrictive policies, high fees, or throttled bandwidth, often obscured in ambiguous contract terms [16], [30], [47]. At the application layer, PaaS and SaaS models exacerbate the issue by requiring vendor-specific development environments. Migrating these applications often demands major reengineering and toolchain changes [5], [7], [35]. Although decentralization models like Edge and Fog computing aim to reduce central dependency, they remain immature and pose scalability concerns [15]. Similarly, open standard APIs promise better interoperability, but provider competition hinders their adoption [7], [16], [41]. In sum, vendor lock-in and poor data portability are not just technical limitations but strategic constraints, especially for organizations pursuing hybrid or multi-cloud architectures.

3.1.3 Performance Unpredictability and QoS Limitations

Although cloud infrastructures are designed for dynamic resource management, performance often becomes unpredictable in multi-tenant environments. Simultaneous demands on compute, memory, or bandwidth lead to latency spikes, throttling, and processing delays, particularly problematic for real-time applications [11], [33]. These disruptions are linked to low-level issues such as fluctuating network latency, memory access variance, and live migration of virtual machines during load balancing [33], [41]. Even short-lived slowdowns from automatic reallocation can affect time-sensitive operations [34]. A major structural flaw lies in SLA documents, which typically promise performance based on average usage, ignoring peak-time bottlenecks. As Flexera (2025) reports, 46% of users report unmet QoS guarantees, highlighting the gap between SLA promises and operational realities [30]. This unpredictability critically impacts resource-heavy workloads, such as data analytics, video processing, and replication. Without QoS-based resource allocation, delays become common, and reliability suffers [16]. Adding to the issue, advanced encryption techniques like FHE and ABE, while secure, demand intensive processing. In latency-sensitive sectors like healthcare or finance, this creates a security–performance trade-off: optimizing for one often degrades the other [11], [20].

3.1.4 Data Loss and Leakage Risks

Migrating to the cloud entails ceding physical control over data, introducing risks to integrity, confidentiality, and availability, particularly in sectors handling sensitive information [9], [51]. Data loss often stems from weak backup strategies, hardware failures, or misconfigured replication. Without multi-region redundancy, such failures can result in permanent data destruction and legal liability [11], [40].

Data leakage, by contrast, frequently arises from access misconfigurations, poor encryption, or outdated security patches. In multi-tenant settings, a single tenant's error can expose other users' data. Similarly, weak encryption during transmission increases the risk of interception [11], [14], [18], [51], [20].

Insider threats further amplify exposure. Malicious or negligent actions by authorized users, especially in environments lacking auditing and monitoring, can lead to the serious breaches [40]. Therefore, encryption should be paired with behavioral analytics and real-time access monitoring to ensure enforcement [18].

Lastly, uncertainties in data deletion processes create long-term leakage risks. Without verifiable, tamper-proof deletion from physical media, residual data may persist and compromise confidentiality post-migration [38].

3.1.5 Cryptographic Challenges in Cloud Security

Cryptography is vital for protecting cloud data, whether at rest, in transit, or during processing. Yet, applying these mechanisms in cloud environments remains challenging due to implementation complexity, performance overhead, and architectural misalignment [11], [18]. Dynamic scaling, distributed systems, and shared responsibility models often clash with traditional cryptographic designs [51], [20]. Ensuring strong data confidentiality without compromising usability requires careful architectural planning. These challenges fall into five interdependent areas, each exposing a distinct cryptographic vulnerability in the cloud.

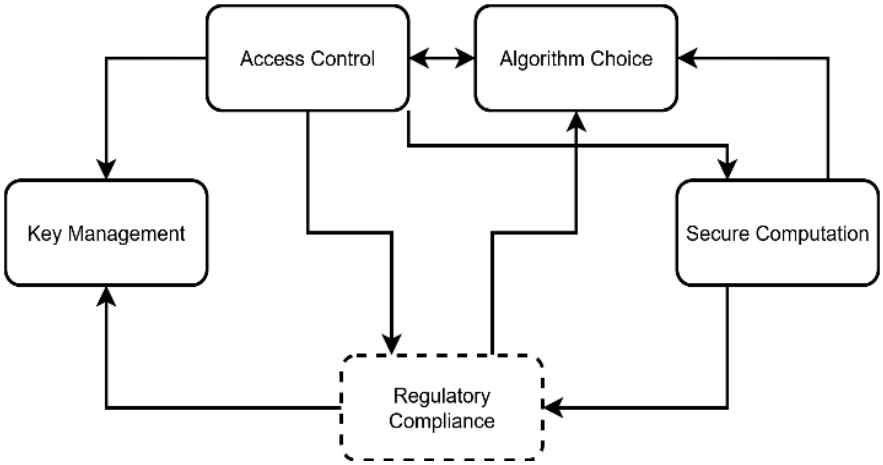

Figure 4. Interdependency Flowchart of Cryptographic Challenges in Cloud Adoption

As shown in Figure 4, the cryptographic challenges of cloud adoption form a structurally interdependent system, rather than existing as isolated components. Key management underpins both access control and the viability of secure computation, while algorithm choices impact performance and compatibility across these layers. Above all, regulatory compliance acts as a cross-cutting constraint, shaping what is architecturally and legally permissible. This web of dependencies underscores the need for integrated mitigation strategies, rather than siloed technical fixes.

3.1.5.1 Key Management Complexity

Managing cryptographic key lifecycles (generation, distribution, rotation, and deletion) is especially challenging in distributed, multi-user cloud systems [18], [20]. Organizations must navigate between centralized and decentralized models, each with trade-offs in scalability and control. While Hardware Security Modules (HSMs) offer strong protection, they often lack cloud-native scalability and cost-efficiency [11], [52]. Software-based Key Management Systems (KMS) raise trust concerns due to limited user visibility [18]. Key sharing across entities introduces risks of compromise, particularly in environments lacking clear separation of privileges. Manual or inconsistent lifecycle management can leave expired or orphaned keys active, creating hidden security vulnerabilities [11], [52]. Additionally, provider opacity around key storage locations and access conditions restricts users' ability to apply their own compliance policies [38].

3.1.5.2 Encryption Algorithm Trade-offs (Symmetric vs Asymmetric)

Selecting encryption algorithms in cloud environments presents a core barrier due to conflicting demands: performance versus security. Symmetric algorithms (e.g., AES) are efficient for large-scale encryption but suffer from key distribution challenges in multi-user systems. In contrast, asymmetric algorithms (e.g., RSA, ECC) offer secure key exchange but are computationally intensive, making them unsuitable for bulk data [11], [18], [20], [52]. This trade-off forces organizations to adopt hybrid encryption, which combines both methods but may introduce latency and compatibility issues, especially in high-throughput environments [51], [20], [38]. Additionally, algorithm selection is not purely technical. Legal compliance and sector-specific regulations further constrain available options, particularly in healthcare and finance [52].

3.1.5.3 Access Control and Authorization Issues

Access control is fundamental to cloud security, yet its implementation in dynamic, multi-tenant environments remain challenging [9], [18]. Misconfigured permissions can lead to unauthorized access and data breaches, particularly in large-scale systems. The two main models, Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), offer distinct trade-offs. RBAC uses predefined roles for access, making it simple but inflexible [11], [53], [54]. ABAC supports context-aware policies based on attributes like time or device type, offering finer control but adding complexity and potential performance issues in large environments [14], [17], [19], [51], [21], [20], [55]. Cryptographic alternatives such as Identity-Based Encryption (IBE) use user identities as public keys, simplifying distribution but introducing reliance on central authorities, which may become single points of failure [56-64]. Multi-Factor Authentication (MFA) enhances security but can impair usability, especially for mobile access [43], [54]. Another widespread issue is the lack of real-time access monitoring. Without audit trails and transparent logging, it becomes difficult to detect privilege misuse or insider threats. This poses serious compliance risks in regulated industries [18], [40].

3.1.5.4 Secure Computation and Search over Encrypted Data

Cloud platforms increasingly support not just storage but analytics, raising tension between privacy and functionality. Traditional encryption blocks operations on ciphertext, requiring decryption to compute [51], [65]. Fully Homomorphic Encryption (FHE) enables arbitrary computations on encrypted data but is too resource-heavy for real-time use [11], [65]. Partially Homomorphic Encryption (PHE), supporting basic operations, offers a more efficient alternative for secure analytics in domains like healthcare and finance [66], [67]. Searchable Encryption (SE) allows keyword queries on encrypted datasets, which is vital for SaaS platforms and medical systems. However, it is vulnerable to inference attacks based on query patterns [9], [18], [20]. Convergent Encryption, useful for deduplication, generates identical ciphertexts from the same plaintext. While space-efficient, it risks data exposure through hash comparison [18], [51]. Li et al. [68] propose a multi-bit dual-mode cryptosystem for efficient oblivious transfer, optimizing both communication and computation costs in cloud-based secure selection scenarios. These techniques extend cryptographic utility but bring trade-offs in performance, security, and suitability. As such, they require case-specific evaluation in cloud environments.

3.1.6 Integration Complexity with Existing Systems

Cloud adoption often builds on legacy infrastructure, introducing integration challenges like application dependencies, data mismatches, and conflicting security policies [16], [7]. These can delay migration, interrupt services, and elevate security risks. A major hurdle is the mismatch between legacy authentication systems (e.g., LDAP, Active Directory) and cloud-based IAM platforms, leading to policy inconsistencies and misconfigured access rights [20]. Workflow synchronization is difficult, as well. Tools like incident management systems often need reconfiguration to interact with cloud-based SaaS or PaaS services, requiring both technical and process-level alignment. Integration complexity spans infrastructure, identity, and operations. Without thorough planning and compatibility checks, it can derail migration goals.

3.2. Organizational Barriers

Cloud adoption is often hindered by internal dynamics, such as structural inertia, cultural resistance, and lack of readiness. Unlike technical challenges, these issues are rooted in human capital and institutional processes, making them harder to detect and resolve. This section examines how such barriers shape the success or failure of cloud integration.

3.2.1 Lack of Cloud-related Technical Expertise

Cloud adoption requires expertise in architecture, security, integration, and cost control. Many organizations, especially SMEs, lack these skills and continue to rely on legacy-focused IT staff [6], [34], [35], [27], [38]. Skill transformation is often slow. Teams unfamiliar with automation, DevOps, or CI/CD pipelines struggle with cloud-native workflows, resulting in delays and misconfigurations [4], [7], [16], [37]. Meanwhile, providers like AWS release hundreds of updates annually, which often outpace internal training efforts [47], [24]. According to Flexera (2025), 52% of firms cite the skills gaps as a major barrier. Ultimately, technical incompetence underlies broader failures, ranging from security misconfigurations to budget overruns.

3.2.2 Organizational Resistance and Inadequate Change Management

Cloud adoption often stalls due to weak executive involvement and employee resistance. Many leaders delegate cloud decisions solely to IT, ignoring strategic alignment in budgeting and planning. Flexera (2025) [24] reports that over 40% of failed cloud projects lacked executive sponsorship [4], [37], [69]. Employee resistance is driven by job security concerns, unclear roles, and disrupted workflows, particularly in public-sector and legacy-driven organizations [28], [29], [45]. Without structured change management, including communication, training, and inclusive transition plans, tensions escalate and rollouts falter. Technical setbacks, such as mismatched data models, compound these challenges [16], [37], [44].

3.2.3 Cost Management and FinOps Immaturity

Despite flexible pricing, cloud adoption is often hindered by unpredictable costs from resource sprawl, egress fees, and user growth [2], [47], [24]. FinOps addresses this by integrating finance, engineering, and operations to improve spending visibility and forecasting. However, many organizations lack the governance maturity for effective FinOps adoption [34], [47]. Weak cost control, due to poor tagging, untracked provisioning, and limited oversight, undermines ROI [35]. Costs may escalate even post-migration without ongoing optimization. FinOps is not a one-off fix but a continuous process critical to sustaining cloud efficiency [47], [24].

3.3. Environmental & Regulatory Barriers

Cloud adoption is shaped by legal, regulatory, and sector-specific constraints, often as critically as technical readiness. Industries like finance, healthcare, and public services face compliance demands that may delay or prevent migration. This section outlines how such environmental factors influence strategic planning and operational continuity.

3.3.1 Ambiguity in Service Level Agreements (SLAs)

SLAs define performance metrics, availability, and responsibilities between cloud providers and users. Despite their importance, many SLAs remain vague, skewed in favor of providers, and difficult to enforce, which poses barriers to adoption [34], [30], [35]. Providers often use ambiguous terms like “reasonable efforts” or “best possible care,” which dilute accountability during disruptions [16], [30], [24]. Critical guarantees, such as uptime, response time, data availability, or recovery time objectives (RTOs), are frequently missing, especially in high-dependency environments. This vagueness is compounded by users’ limited capacity to evaluate SLA terms. SMEs, in particular, may lack the legal or technical literacy to assess alignment with their risk thresholds [34], [35]. Even in large enterprises, undefined promises like “high availability” may mask tolerances for outages or degraded access. These issues are outlined in Section 3.1.1 [17]. Compensation clauses are often symbolic or absent altogether, offering little recourse after breaches [30], [40]. The lack of clear enforcement mechanisms erodes user trust, especially when providers retain broad discretion over obligations. Improving SLA transparency, aligning guarantees with risk profiles, and empowering users to interpret and negotiate terms are essential for trust and resilience in cloud services.

3.3.2 Regulatory Compliance and Legal Uncertainty

Cloud adoption is increasingly constrained by data protection laws, sovereignty rules, and compliance mandates that often conflict with the global nature of cloud infrastructure [31], [40]. In the EU, GDPR imposes consent, transparency, and data residency obligations, which force localization and increase deployment complexity [31], [40]. U.S. laws like HIPAA and FISMA require encryption, access control, and auditability, with heavy penalties for non-compliance [40]. Countries such as China, Russia, and Türkiye enforce data localization laws, requiring domestic storage of personal data and pressuring providers to build local infrastructure or exit markets [35], [31], [70]. Beyond statutory laws, adherence to standards like ISO 27001, SOC 2, and NIST entails recurring audits and documentation burdens, especially for SMEs [40], [50]. Academic institutions also report compliance-related hesitation, driven by mobile access concerns and data sensitivity [46]. Legal and regulatory ambiguity remains a pervasive barrier. It challenges both scalability and strategic cloud planning.

3.3.3 Data Sovereignty and Jurisdictional Risks

Jurisdictional uncertainty is a key barrier to cloud adoption, especially for multinational organizations navigating conflicting cross-border data protection laws [37]. Local residency requirements force providers to restructure services, increasing costs and limiting flexibility [7]. Legal accountability often rests with the country where data is stored, exposing users to overlapping or contradictory mandates such as GDPR and foreign surveillance laws. These risks make data sovereignty a persistent compliance challenge. Without region-aware deployments or legal due diligence, organizations face exposure to penalties, operational friction, and reputational harm.

4. TARGETED STRATEGIES TO ADDRESS CLOUD ADOPTION BARRIERS

As detailed in Section 3, the identified barriers form the structural basis for the practical strategies presented in this section. Each proposed measure directly addresses one or more barriers classified under the technological, organizational, and environmental dimensions of the TOE framework. These include issues related to service continuity, data portability, performance, security, and trust. Drawing from both academic research and industry reports, the proposed solutions are mapped to the technological, organizational, and environmental dimensions defined by the TOE framework. This alignment enables a more structured, role-specific approach for cloud providers and enterprise stakeholders seeking secure and scalable integration.

4.1. Redundant and Secure Infrastructure

Cloud service disruptions can stem from hardware failures, outages, or cyberattacks. Ensuring availability is thus both a performance and security imperative. Multi-regional data centers with automated synchronization are central to achieving high availability (e.g., 99.999% uptime), especially in sectors like finance or public infrastructure [11], [10], [22]. These setups support seamless failover during localized failures. Beyond physical redundancy, virtual isolation mechanisms (such as micro-segmentation and containerized deployments) limit lateral threat movement in multi-tenant environments [11], [14], [18]. Auto-scaling frameworks respond to usage surges, while real-time orchestration ensures efficient resource alignment [10]. To counter DDoS and similar threats, anomaly-based traffic monitors detect and respond early [22]. Additional layers like honeypots help deceive attackers and support forensic analysis [11]. Finally, transparency in SLAs is critical. Vague terms like “best effort” erode trust. Providers should offer clear, measurable guarantees for uptime and recovery [2]. In short, resilient cloud infrastructure demands a layered defense (redundancy, segmentation, orchestration, proactive monitoring), backed by clear service commitments.

4.2. Abstraction of Application and Cloud Data

Abstraction at the application and data layers helps mitigate vendor lock-in and improve cross-platform portability. Intermediate abstraction layers, often implemented using orchestration tools or container platforms like Kubernetes, decouple application logic from infrastructure, increasing flexibility [18], [34]. API standardization further enhances interoperability. While proprietary APIs lead to migration challenges and technical debt, open standards like REST and JSON schemas reduce integration costs [11], [18]. Data integrity during migration can be ensured via Change Data Capture (CDC) and cryptographic hash chains, which verify real-time changes and prevent tampering [11], [20]. Emerging paradigms such as Edge and Fog Computing introduce additional abstraction by processing data near the source, reducing central cloud dependency [15], [19]. However, these models face issues in scalability and standardization, particularly for large enterprises [19]. Security remains a concern. Open APIs, if unprotected, may expand the attack surface. Token-based authentication and encrypted communication are essential to safeguard interactions [13]. Ultimately, abstraction enables greater portability, autonomy, and long-term resilience in cloud ecosystems.

4.3. Trust Mechanisms in Cloud

Trust in cloud environments depends on transparency, user control, and regulatory alignment. Building this trust requires both technical safeguards and governance clarity. Transparency fosters confidence, especially when users have visibility into operations and data access [22]. Customer-Controlled Encryption (CCE) strengthens data sovereignty by letting users manage their own keys [13], while public-sector clients often demand tailored security frameworks [49]. Auditability through immutable logs and forensic tools supports compliance, particularly in regulated industries [13]. Third-party certifications like SOC 2, ISO 27001, and FedRAMP validate provider security practices [12]. Key management autonomy, via BYOK or HYOK, enhances control, though it may introduce operational complexity during high-load tasks [13]. Confidential Computing extends protection to the processing layer by keeping data encrypted during computation using Trusted Execution Environments (TEEs) [9]. Trust emerges from both infrastructure-level guarantees and user-centric policies, combining encryption, auditability, and accountability.

4.4. Preventing Data Loss and Leakage

Preventing data loss and leakage in cloud environments requires a layered approach, combining redundancy, access control, monitoring, and encryption. Geo-redundant backup architectures form the core of Disaster Recovery as a Service (DRaaS), ensuring data availability during outages caused by hardware failure or natural disasters [11]. Data Loss Prevention (DLP) systems classify data, monitor flows, and block anomalies in real time to reduce leakage risk [18]. Centralized access control using RBAC and ABAC models limits exposure while enabling

auditability [53], [54], [55], [54]. To preserve integrity, mechanisms like checksums, Merkle trees, and hash chains detect unauthorized modifications during storage and transfer [67]. End-to-End Encryption (E2EE) ensures confidentiality by preventing data decryption at intermediary nodes, protecting data both at rest and in transit [13], [57]. However, encryption alone is insufficient. Many built-in backup tools lack flexibility, highlighting the need for custom retention and classification policies [18]. Effective protection demands both technical implementation and policy-level enforcement, where resilience, privacy, and traceability reinforce one another.

4.5. Increasing Performance over Cloud

Cloud performance often suffers from demand fluctuations, resource contention, and cryptographic overhead. To counter this, elastic resource management dynamically adjusts compute, storage, and bandwidth based on workload intensity [3], [10], [48]. This elasticity requires real-time monitoring tools (e.g., APM) to track latency, memory usage, and bottlenecks [3], [48]. Since cryptographic methods like FHE and SMPC increase processing delays, hybrid encryption strategies are advised, reserving advanced methods for sensitive data and using standard encryption elsewhere [13], [67]. Caching systems (e.g., Redis, Memcached) reduce latency by storing frequently accessed data in memory [3]. Additionally, QoS-based resource reservation ensures bandwidth and compute capacity for mission-critical tasks [3], [48]. For low latency needs, Edge Computing brings processing closer to data sources, which is ideal for IoT and real-time applications [15].

In summary, performance optimization in cloud systems depends on layering: scalable infrastructure, active monitoring, encryption efficiency, and architectural decentralization.

4.6. Utilizing Cryptographic Methods for Enhancing Data Security in Cloud

Cryptographic risks in the cloud stem from both technical complexity and regulatory pressure. Effective mitigation demands integrated solutions that ensure data privacy without compromising system performance or compliance.

4.6.1 Data Protection with Hybrid Encryption

Selecting cryptographic algorithms in cloud environments is a balancing act between security, performance, energy efficiency, and feasibility integration. Decisions must move beyond theoretical strength to account for real-world constraints. Legacy asymmetric algorithms like RSA remain widely used but impose heavy computational loads. For example, a 224-bit ECC key offers comparable security to a 2048-bit RSA key, with up to 10× gains in speed and energy use [52]. ECC has thus been adopted by providers like Google, Apple, and AWS, particularly in TLS and mobile systems. Hybrid encryption models have become the default approach: asymmetric algorithms (e.g., ECC) handle key exchange and authentication, while symmetric ones (e.g., AES-256) encrypt data. This combination significantly enhances performance without sacrificing confidentiality. Gupta et al. observed up to 45% performance improvements using such schemes in multi-user cloud setups [18]. Algorithm selection must be context-aware:

- ECC + AES-GCM suits low-latency, low-power applications like IoT.
- RSA-3072 + AES-CBC is preferred in highly regulated sectors like healthcare.
- AES-256 with long key cycling fits archival storage with long-term confidentiality needs.

There is no universal best algorithm, only strategy portfolios tailored to specific constraints and compliance needs. Adaptive encryption policies are thus essential for sustainable and secure cloud operations.

4.6.2 Key Management

Effective key management is critical for cloud cryptographic security, especially where user control and compliance are priorities [18], [71]. Threshold-based key recovery models inspired by Shamir's secret sharing [72] are increasingly adopted in cloud-native architectures to distribute trust and mitigate single point of failure in key custody. Default provider KMS solutions often lack transparency, limiting auditability. The BYOK model gives users control over key generations, though storage remains with the provider. For full sovereignty, HYOK ensures keys are stored entirely on user-managed systems, eliminating provider access [13]. Hardware Security Modules (HSMs) offer tamper-resistant storage, with services like AWS CloudHSM and Azure Dedicated HSM widely used in regulated sectors [52]. Robust key management spans the entire lifecycle: rotation, expiration, revocation, and secure destruction in compliance with regulations like GDPR and HIPAA [52]. Monitoring access logs is essential for audit trails. Ultimately, the choice among BYOK, HYOK, and HSM depends on data sensitivity and threat context, and should be reinforced with automation and real-time policy enforcement.

4.6.3 Fine-Grained Access Control via Cryptographic Methods

Traditional access controls based on static credentials or roles often fall short in cloud environments with dynamic, multi-tenant structures. To address this, cryptography-driven, fine-grained authorization methods have emerged [9]. Attribute-Based Encryption (ABE) encrypts data according to user attributes (e.g., role, department, region), allowing context-aware access without constantly updating access lists. ABE is particularly effective in collaborative and privacy-sensitive environments. Proxy Re-Encryption (PRE) enables a third party to re-encrypt data for another user without exposing the plaintext. This is useful in SaaS models where data ownership shifts across users or departments [21]. For consistent policy enforcement, these cryptographic models should integrate with centralized Identity and Access Management (IAM) systems. IAM

platforms extended with attribute logic can unify organizational policy with encryption-layer authorization [13]. However, adoption challenges remain. Managing dynamic policies requires administrative effort, and current tooling lacks support for privacy-by-design principles in adaptive cloud applications [18], [36]. In essence, robust access control in the cloud demands a shift toward data-centric cryptographic enforcement. ABE and PRE offer strong technical foundations, but their real impact depends on IAM integration, policy governance, and organizational capacity.

4.6.4 Secure Computation over Encrypted Data

Traditional cryptography requires decryption before processing, exposing data to risks, especially in third-party cloud environments. Advanced methods now enable computations directly on encrypted data, preserving confidentiality end-to-end. Fully Homomorphic Encryption (FHE) allows arbitrary computation on ciphertext but remains too slow for real-time or large-scale use [51], [65]. More practical alternatives include Partially Homomorphic Encryption (PHE) for simple operations, and Secure Multi-Party Computation (SMPC), which enables joint computation without revealing inputs, ideal for privacy-critical domains like finance and healthcare [58], [67]. Although open-source libraries (e.g., SEAL, HElib) and cryptographic accelerators improve performance, challenges remain in scalability and system integration. Still, secure computation marks a paradigm shift, enabling privacy-preserving analytics, regulatory compliance, and zero-trust architectures.

4.7 Integration Strategies for Legacy Systems

Legacy systems, often monolithic and outdated, pose serious barriers to cloud migration due to limited compatibility and scalability. A modular integration strategy is essential to ensure continuity without disrupting existing operations. API Gateways act as translation layers between legacy protocols and modern cloud services [10], while the Strangler Pattern enables gradual replacement with microservices, minimizing risk and downtime [73]. Data consistency is maintained via ETL pipelines and Change Data Capture (CDC) mechanisms [10], [13]. For identity integration, federating systems like LDAP or Active Directory with cloud IAM platforms through Single Sign-On (SSO) ensure seamless access control [14]. Effective legacy integration demands layered coordination, including technical, procedural, and architectural aspects.

4.8 Change Management and Organizational Preparedness

Cloud adoption entails not just technical change but organizational transformation. Resistance often stems from job security fears, skill gaps, and disrupted workflows. To overcome this, executive sponsorship is critical, ensuring leadership support, budget continuity, and cross-functional coordination [46]. Upskilling programs such as cloud literacy and role-based competency mapping help realign employee capabilities [39], [46], while Change Communication Roadmaps reduce uncertainty by clarifying the transition process. Appointing internal "Cloud Champions" accelerates adoption through peer influence and mentorship [12].

Ultimately, successful change management depends on synchronized leadership, cultural alignment, and sustained reinforcement, without which technical readiness alone is insufficient.

4.9 FinOps Maturity and Cost Optimization

While cloud computing offers scalability, cost unpredictability remains a major concern. A structured FinOps model (uniting finance, engineering, and operations) is essential to improve budget visibility and accountability [74]. Core practices include auto-scaling, instance optimization (e.g., Reserved/Spot), and rightsizing based on usage patterns. Monitoring tools track CPU, network, and storage metrics to support real-time cost forecasting [10]. Dashboards like AWS Cost Explorer enable chargeback and showback mechanisms for departmental awareness.

As shown in Figure 5, FinOps maturity progresses through three concentric stages [74]:

- Crawl: Basic reporting and visibility.
- Walk: Team-level budgeting with integrated dashboards.
- Run: Automated policies, real-time optimization, and cost governance.

This model is adapted from the maturity framework proposed by Fuller et al. [74] and extended to align with TOE-based strategic indicators. It reflects not only technical capability but also organizational evolution, where cost becomes a shared, strategic metric aligned with business value and cloud governance priorities.

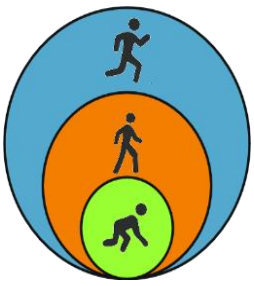

Figure 5. FinOps Maturity Progression Model

4.10 Regulation and Standard Compliance

Cloud-based cryptographic systems must comply with legal frameworks like GDPR, HIPAA and LPPD (Turkish Law of Personal Data Protection) which mandate encrypted, auditable, erasable, and geographically-bound data. Compliance requires generating detailed audit logs, enabling traceability and regulatory reporting [17]. Using NIST-approved algorithms boosts credibility and minimizes legal risk [52], [71]. Geo-compliance is achieved by offering data residency options, vital for multinational operations [35]. In local contexts such as Türkiye, compliance with LPPD mandates the use of

cryptographic strategies aligned with national privacy laws [71], [70]. Cryptographic key shredding, which destroys encryption keys upon deletion, enforces rights like the right to be forgotten [52]. Maintaining compliance also demands:

- Regular standard-aligned updates,
- Legal data handling training,
- Real-time compliance dashboards [36].

Ultimately, cryptographic compliance relies on a holistic approach, including standard-based design, operational transparency, and governance integration.

5. MAPPING BARRIERS TO SOLUTION STRATEGIES

This section presents the alignment between the barriers identified in Section 3 and the solution strategies outlined in Section 4. The resulting mapping (Table 4) provides a diagnostic scaffold that visualizes how specific barriers are addressed across technological, organizational, and environmental domains. However, this alignment also reveals substantial interdependencies and limitations that warrant further analysis.

While the TOE framework provides a useful structural lens, this mapping underscores its conceptual limitations. Many challenges (particularly cryptographic and regulatory) cannot be cleanly compartmentalized. For example, algorithm selection (technological) is often governed by compliance mandates (environmental), and its implementation hinges on in-house expertise (organizational). Thus, barriers must be treated as multi-dimensional constructs rather than isolated problems.

A key insight lies in the cryptographic convergence problem. Sub-barriers such as secure computation and key control are technically distinct but operationally inseparable. Implementing secure computation through Fully Homomorphic Encryption (FHE), for instance, impacts performance (technological), inflates cost (organizational), and demands legal clarity on data residency (regulatory). This necessitates portfolio-based implementation, where layered cryptographic strategies are evaluated jointly, not in isolation.

Additionally, while technical literature provides robust proposals for infrastructure and encryption solutions, it underrepresents organizational readiness. Recent empirical cases and the Flexera 2025 report indicate that non-technical inertia, such as insufficient training, leadership gaps, or resistance to workflow change, remains a primary cause of migration setbacks. These findings highlight a disconnect, as CAFs often assume institutional readiness and consequently omit actionable organizational guidance.

Another critical limitation is that this mapping remains inherently static. Cloud environments are fluid, regulated by evolving compliance frameworks such as GDPR, HIPAA, and LLPD, shifting threat landscapes, and maturing FinOps practices. A fixed mapping cannot fully capture dynamic changes in risk, cost-efficiency, or operational resilience. As such, mapping must evolve into a dynamic benchmarking model, periodically recalibrated to reflect industry trends and sector-specific needs.

In sum, the proposed TOE-anchored analytical model provides a foundational tool for diagnosing the multifaceted nature of cloud adoption barriers. Its core value lies not in providing rigid prescriptions. Instead, it guides adaptive strategies that enable organizations to align with technological evolution, regulatory shifts, and internal transformation.

Table 4. Barrier–Solution Mapping Based on TOE-Anchored Analytical Model

Barrier Category	Specific Barrier	Proposed Solution(s)
Technological	Service unavailability and downtime	Multi-regional redundancy, automated scaling, honeypots, anomaly-based monitoring
Technological	Vendor lock-in and lack of data portability	Abstraction layers (API/containerization), open standards, CDC, hash chain-based verification mechanisms
Technological	Performance unpredictability (QoS issues)	Auto-scaling, APM tools, cache-based architectures, hybrid encryption, edge computing
Technological	Data loss and leakage risks	DLP systems, geo-redundant backup, access control (RBAC/ABAC), checksum & E2EE
Technological	Key management complexity	HSM, BYOK/HYOK, lifecycle automation, key audit logging
Technological	Trade-offs in encryption algorithm selection	Hybrid encryption (AES + ECC), context-aware crypto strategies
Technological	Inadequate access control mechanisms	ABE, PRE, IAM integration
Technological	Inability to compute over encrypted data	FHE, PHE, SMPC, SE
Technological	Regulatory compliance of cryptographic operations	IBE, auditability, cryptographic key shredding, ISO 27001 alignment, confidential computing
Organizational	Lack of cloud-related technical expertise	Cloud literacy programs, certification paths, continuous training, technical upskilling
Organizational	Resistance to change & leadership inertia	Executive sponsorship, change roadmaps, “Cloud Champion” roles, psychological alignment
Organizational	Cost management immaturity	FinOps, budget forecasting, showback/chargeback, spot/reserved instance optimization
Environmental / Legal	SLA vagueness and lack of measurable guarantees	SLA clarification, legal auditability, third-party attestation (SOC 2, ISO 27001)
Environmental / Legal	Regulatory and compliance constraints (GDPR, HIPAA)	Region-based deployment, cryptographic key shredding, legal alignment modules in CAF
Environmental / Legal	Data sovereignty and jurisdiction risk	Data localization options, sovereign cloud strategies, multi-region control
Abbreviations: APM - Application Performance Monitoring, BYOK - Bring Your Own Key, ECC - Elliptic Curve Cryptography, HYOK - Hold Your Own Key,		

6. DISCUSSION

This study offers a barrier-solution mapping for cloud adoption through the lens of the TOE framework, enhanced with cryptographic analysis, FinOps maturity, and CAF benchmarking. While the TOE structure has been widely applied in literature to identify technological, organizational, and environmental determinants, this research extends its analytical precision by incorporating cryptographic sub-barriers, service-level agreement (SLA) opacity, and compliance mandates, which are dimensions often underrepresented in classical TOE applications.

Previous works, such as Oliveira et al. [25] and Gangwar [4], focused on general IT adoption, particularly among SMEs, without accounting for advanced security requirements, regulatory interdependencies, or financial governance models relevant to modern cloud transitions. Technical literature, including studies like Zhang et al. [13], provides detailed taxonomies of cryptographic approaches (e.g., ABE, FHE, multi-party computation), yet often lacks integration with organizational readiness and economic viability. This study addresses that gap by embedding encryption strategies into the TOE matrix while aligning them with FinOps-driven financial governance capabilities adapted from Fuller et al. [74]. In doing so, it connects cost visibility and operational efficiency with cloud readiness dimensions, creating a more granular and strategic diagnostic model compared to prior literature.

The integration of five real-world case studies demonstrates the framework’s practical applicability and highlights sector-specific barrier profiles. In the Ukraine public sector migration (2022), environmental factors such as geopolitical instability heightened the urgency for multi-region deployment and sovereign data hosting, while organizational readiness determined execution speed. The UK NHS adoption revealed how organizational inertia, including fragmented leadership and limited technical training, can delay migration despite available technical solutions. The CLOUD Act’s implications in the U.S. underscored environmental and legal constraints shaping encryption key management and data localization. The TSB Bank migration incident exposed the risk of aligning advanced technical strategies with insufficient organizational preparedness, resulting in prolonged outages. Finally, EBA-regulated financial transitions illustrated how compliance mandates act as both a catalyst and a bottleneck, necessitating phased cryptographic modernization and multi-layer governance.

Cross-case synthesis shows that technical readiness alone does not ensure successful cloud migration. Organizational and environmental dimensions frequently determine the effectiveness of technical solutions. Proactive alignment of

cryptographic migration plans with regulatory frameworks, supported by governance restructuring, staff training, and vendor oversight, reduces both technical complexity and operational risk. This aligns with industry observations that algorithmic readiness must be matched by institutional capability.

While the barrier-solution mapping clarifies alignment between challenges and interventions, the approach has limitations. The analysis is qualitative and based solely on secondary data; it lacks quantitative validation such as SLA adherence rates, cryptographic processing latency, or FinOps return on investment. Without migration telemetry, stakeholder interviews, or sector-specific KPIs, certain contextual variations may be underrepresented. This is especially true in high-stakes environments such as healthcare, finance, and defense. Additionally, some barriers, notably vendor lock-in and SLA opacity, remain strategically unresolved due to the absence of standardized industry solutions.

Another limitation lies in the static nature of the mapping. Given the rapid evolution of cryptographic standards, cost structures, and compliance landscapes, a fixed alignment risks obsolescence. Future research should focus on developing dynamic, data-driven barrier–solution models that treat TOE components as overlapping, reflecting the interdependencies between technical, organizational, and environmental domains.

Overall, the operationalization of the TOE framework into a cryptographically aware and financially informed decision-support model addresses a previously underexplored convergence of technical, organizational, and environmental factors. The framework's adaptability across sectors and alignment with empirical case findings positions it as a practical reference point for both policymakers and practitioners, while its identified limitations set the stage for further empirical validation and refinement.

7. CONCLUSION AND FUTURE RESEARCH DIRECTION

Cloud adoption is not merely a technical migration but a strategic transformation that reshapes systems, processes, people, and governance. This study applied an extended TOE framework, enriched with cryptographic sub-barriers, FinOps maturity, and CAF benchmarking, to identify and classify the barriers that hinder secure and scalable cloud transitions. By integrating literature synthesis, provider guidance, and five real-world case studies, the research bridges the gap between theoretical robustness and actionable practice.

Findings reveal that while cryptographic and technical challenges are the most visible, deeper and more persistent blockers lie in organizational resistance, governance gaps, and regulatory complexity. The case analyses show that sector-specific factors directly influence the success of technical interventions. Examples include geopolitical instability in the Ukraine migration, compliance-driven bottlenecks in EBA-regulated finance, and organizational inertia in the NHS adoption. Many migrations falter not due to the absence of tools, but because of inadequate change management, ambiguous SLAs, and immature cost governance.

This research contributes a visualized, structured barrier-solution matrix that aligns cryptographic readiness, financial governance, and compliance controls with migration strategies. Its value lies in adaptability: the model is designed not as a static prescription but as a foundation for continuous improvement, responsive to evolving cryptographic standards, regulatory landscapes, and cost structures. For policymakers, the framework offers a lens to identify systemic readiness gaps; for practitioners, it provides a decision-support tool to align technical execution with organizational and environmental realities.

Future research should extend this work by focusing on:

- Dynamic modeling of TOE interdependencies using system dynamics or graph theory to uncover feedback loops and hidden tensions between dimensions.
- Sector-specific adoption roadmaps tailored to regulated environments such as healthcare, finance, and public services, where compliance constraints dictate migration sequencing.
- KPI-driven simulation studies to empirically validate the barrier–solution matrix under operational constraints (e.g., SLA adherence, cost efficiency, cryptographic performance).
- Automated compliance intelligence through AI-powered monitoring systems that dynamically assess regulatory adherence and control gaps in multi-cloud environments.

Ultimately, the success of cloud adoption lies not in technological readiness alone but in the ability to synchronize secure technical execution with regulatory responsibility, financial stewardship, and cultural adaptation. The real challenge is not simply moving to the cloud, but maintaining resilience, compliance, and sustainability once there.

This study advances the classical TOE framework by embedding a dedicated cryptographic challenge layer, integrating FinOps maturity assessment, and aligning migration strategies with cross-provider Cloud Adoption Framework benchmarks. This integrated model, supported by empirical evidence from five multi-sector case studies, offers an actionable, adaptable diagnostic tool that has not previously appeared in the literature. By explicitly linking cryptographic regulatory compliance, governance maturity, and sector-specific readiness to targeted solution strategies, the framework delivers both analytical granularity and practical applicability, closing a critical gap between theoretical models and operational execution.

REFERENCES

[1] M. Armbrust et al., “A View of Cloud Computing”, Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[2] Pragati Priyadarshinee, Rakesh D. Raut, Manoj Kumar Jha, Bhaskar B. Gardas, Understanding and predicting the determinants of cloud computing adoption: A two staged hybrid SEM - Neural networks approach, Computers in Human Behavior, Volume 76, Pages 341-362, 2017.

[3] Peter M. Mell and Timothy Grance. SP 800-145. The NIST Definition of Cloud Computing. Technical Report. National Institute of Standards & Technology, Gaithersburg, MD, A.B.D., 2011.

[4] Gangwar, H., Date, H. and Ramaswamy, R., "Understanding determinants of cloud computing adoption using an integrated TAM-TOE model", *Journal of Enterprise Information Management*, Vol. 28 No. 1, pp. 107-130, 2015.

[5] B. M. R. Wilson, B. Khazaei and L. Hirsch, "Enablers and Barriers of Cloud Adoption among Small and Medium Enterprises in Tamil Nadu", **2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)**, Bangalore, India, pp. 140-145, 2015.

[6] W. Hadhri, T. Maherzi, and A. Ben Youssef, “E-Skills and the Adoption of Cloud Computing,” Thunderbird Int. Bus. Rev., vol. 59, no. 5, pp. 635–645, 2017.

[7] Ibrahim Shafiu, William Yu Chung Wang, and Harminder Singh. Drivers and barriers in the decision to adopt IaaS: a public sector case study. Int. J. Bus. Inf. Syst. 21, 2 (January 2016), 249–267, 2016.

[8] Al-Jabri, I.M. and Alabdulhadi, M.H. ‘Factors affecting cloud computing adoption: perspectives of IT professionals’, *International Journal of Business Information Systems*, Vol. 23, No. 4, pp.389–405, 2016.

[9] P. Yang, N. Xiong and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," in IEEE Access, vol. 8, pp. 131723-131740, 2020.

[10] T. Erl, Z. Mahmood, and R. Puttini, Cloud Computing: Concepts, Technology, & Architecture. Prentice Hall, 2013.

[11] S. Zhang et al., "Practical Adoption of Cloud Computing in Power Systems—Drivers, Challenges, Guidance, and Real-World Use Cases," in IEEE Transactions on Smart Grid, vol. 13, no. 3, pp. 2390-2411, May 2022.

[12] Michael Seifert, Stephan Kuehnel, and Stefan Sackmann. 2023. Hybrid Clouds Arising from Software as a Service Adoption: Challenges, Solutions, and Future Research Directions. ACM Comput. Surv. 55, 11, Article 228 (November 2023), 35 pages.

[13] L. Zhang, H. Xiong, Q. Huang, J. Li, K. -K. R. Choo and J. Li, "Cryptographic Solutions for Cloud Storage: Challenges and Research Opportunities," in IEEE Transactions on Services Computing, vol. 15, no. 1, pp. 567-587, 1 Jan.-Feb. 2022.

[14] R. Charanya and M. Aramudhan, “Survey on access control issues in cloud computing,” in 2016 **International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)**, Feb. 2016, pp. 1–4.

[15] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, “Fog Computing: A Platform for Internet of Things and Analytics,” 2014.

[16] Garrison, G., Kim, S., & Wakefield, R. L. (2012). Success factors for deploying cloud computing. Communications of the ACM, 55(9), 62–68.

[17] Huang, J., Nicol, D.M. Trust mechanisms for cloud computing. J Cloud Comp 2, 9 (2013).

[18] I. Gupta, A. K. Singh, C. -N. Lee and R. Buyya, "Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions," in IEEE Access, vol. 10, pp. 71247-71277, 2022.

[19] A. Ometov, O. L. Molua, M. Komarov, and J. Nurmi, "A Survey of Security in Cloud, Edge, and Fog Computing," Sensors, vol. 22, no. 3, p. 927, Jan. 2022.

[20] K. Sasikumar and S. Nagarajan, "Comprehensive Review and Analysis of Cryptography Techniques in Cloud Computing," in IEEE Access, vol. 12, pp. 52325-52351, 2024.

[21] D. Tiwari and G. R. Gangadharan, “SecCloudSharing: Secure data sharing in pubcloud using ciphertext-policy attribute-based proxy re-encryption with revocation,” Int. J. Commun. Syst., vol. 31, no. 5, p. e3494, 2018.

[22] J. Hwang, K. Bai, M. Tacci, M. Vukovic and N. Anerousis, "Automation and orchestration framework for large-scale enterprise cloud migration," *in IBM Journal of Research and Development*, vol. 60, no. 2-3, pp. 1:1-1:12, March-May 2016.

[23] M. A. Himmel and F. Grossman, "Security on distributed systems: Cloud security versus traditional IT," in *IBM Journal of Research and Development*, vol. 58, no. 1, pp. 3:1-3:13, Jan.-Feb. 2014.

[24] Internet: Flexera, State of the Cloud Report, https://info.flexera.com/CM-REPORT-State-of-the-Cloud, 10.04.2025.

[25] Tiago Oliveira, Manoj Thomas, Mariana Espadanal, “Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors,” Information & Management, Volume 51, Issue 5, 2014, Pages 497-510.

[26] A. Ahmad, S. U. Khan, H. U. Khan, G. M. Khan and M. Ilyas, "Challenges and Practices Identification via a Systematic Literature Review in the Adoption of Green Cloud Computing: Client’s Side Approach," in IEEE Access, vol. 9, pp. 81828-81840, 2021.

[27] Ibrahim, H.M., Ahmad, K. & Sallehudin, H. Understanding the technology and humans as determinants of cloud computing adoption for digital preservation of research outputs in university libraries. Educ Inf Technol 30, 6163–6211, 2025.

[28] Qatawneh, N. Building a framework to drive government systems' adoption of cloud computing through IT knowledge. Discov Sustain 5, 282, 2024.

[29] D. Soto, S. Shirai, M. Ueda, M. Higashida, Y. Uranishi and H. Takemura, "Cloud Computing Challenges and Needs in Higher Education Institutions in Post-COVID-19 Times: A Case of a Japanese Survey," in IEEE Access, vol. 12, pp. 168043-168059, 2024.

[30] Seifert, M., Kuehnel, S. HySOR: A Simulation Model for the Sharing of Risk in a Service Level Agreement-Aware Hybrid Cloud. Bus Inf Syst Eng (2024).

[31] Raza Nowrozy, Khandakar Ahmed, A. S. M. Kayes, Hua Wang, and Timothy R. McIntosh. 2024. Privacy Preservation of Electronic Health Records in the Modern Era: A Systematic Survey. ACM Comput. Surv. 56, 8, Article 204 (August 2024), 37 pages.

[32] Alshdadi, A.A., AlGhamdi, R., Alassafi, M.O. et al. A validation of a cloud migration readiness assessment instrument: case studies. SN Appl. Sci. 2, 1370 (2020).

[33] Munjal, S., Colaco, P., Sharma, D. et al. A novel approach for allocating resources in a multi-cloud environment. Int J Syst Assur Eng Manag (2025).

[34] M. Ahmad El Skafi, M. M. Yunis, A. Zekri and J. Bu Daher, "The Confluence of Big Data and Cloud Computing in SME Adoption Strategies," in IEEE Access, vol. 13, pp. 37789-37811, 2025.

[35] Kotulski, Z., Nowak, T., Sepczuk, M. et al. Keeping Verticals' Sovereignty During Application Migration in Continuum. J Netw Syst Manage 32, 67 (2024).

[36] Angeliki Kitsiou, Maria Sideri, Michail Pantelelis, Stavros Simou, Aikaterini–Georgia Mavroeidi, Katerina Vgena, Eleni Tzortzaki, and Christos Kalloniatis. 2024. Developers' mindset on self-adaptive privacy and its requirements for cloud computing environments: Developers' mindset on Self-Adaptive... Int. J. Inf. Secur. 24, 1 (Feb 2025).

[37] A. Santos, J. Martins, P. Duarte Pestana, R. Gonçalves, H. São Mamede and F. Branco, "Factors Affecting Cloud Computing Adoption in the Education Context—Systematic Literature Review," in IEEE Access, vol. 12, pp. 71641-71674, 2024.

[38] Guo, R., Tafti, A. & Subramanyam, R. Internal IT modularity, firm size, and adoption of cloud computing. Electron Commer Res 25, 319–348 (2025).

[39] Kavre, M.S., Sunnapwar, V.K. & Gardas, B.B. Cloud manufacturing adoption: a comprehensive review. Inf Syst E-Bus Manage (2023).

[40] Ukeje, N., Gutierrez, J. & Petrova, K. Information security and privacy challenges of cloud computing for government adoption: a systematic review. Int. J. Inf. Secur. 23, 1459–1475 (2024).

[41] Tianzhang He and Rajkumar Buyya. 2023. A Taxonomy of Live Migration Management in Cloud Computing. ACM Comput. Surv. 56, 3, Article 56 (March 2024), 33 pages.

[42] Aymen Akremi and Mohsen Rouached. 2021. A comprehensive and holistic knowledge model for cloud privacy protection. J. Supercomput. 77, 8 (Aug 2021), 7956–7988.

[43] Li, G., Zhou, M., Feng, Z. et al. Research on Key Influencing Factors of E-Government Cloud Service Satisfaction. Wireless Pers Commun 127, 1117–1135 (2022).

[44] F. Mostajabi, A. A. Safaei and A. Sahafi, "A Systematic Review of Data Models for the Big Data Problem," in IEEE Access, vol. 9, pp. 128889-128904, 2021.

[45] Jewan Singh, Vibhakar Mansotra, Shabir Ahmad Mir, and Shahzada Parveen. 2021. Cloud feasibility and adoption strategy for the INDIAN school education system. Education and Information Technologies 26, 2 (Mar 2021), 2375–2405.

[46] Almaiah, M.A., Al-Khasawneh, A. Investigating the main determinants of mobile cloud computing adoption in university campus. Educ Inf Technol 25, 3087–3107 (2020).

[47] Hsu, PF. A Deeper Look at Cloud Adoption Trajectory and Dilemma. Inf Syst Front 24, 177–194 (2022).

[48] Angelos-Christos Anadiotis, Raja Appuswamy, Anastasia Ailamaki, Ilan Bronshtein, Hillel Avni, David Dominguez-Sal, Shay Goikhman, and Eliezer Levy. 2020. A system design for elastically scaling transaction processing engines in virtualized servers. Proc. VLDB Endow. 13, 12 (August 2020), 3085–3098.

[49] M. O. Alassafi, R. AlGhamdi, A. Alshdadi, A. Al Abdulwahid and S. T. Bakhsh, "Determining Factors Pertaining to Cloud Security Adoption Framework in Government Organizations: An Exploratory Study," in IEEE Access, vol. 7, pp. 136822-136835, 2019.

[50] Usama Ahmed, Imran Raza, and Syed Asad Hussain. 2019. Trust Evaluation in Cross-Cloud Federation: Survey and Requirement Analysis. ACM Comput. Surv. 52, 1, Article 19 (January 2020), 37 pages.

[51] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," in Financial Cryptography and Data Security, 2010, pp. 136–149.

[52] E. Barker, "Recommendation for Key Management Part 1: General." 2016, doi: 10.6028/NIST.SP.800-57pt1r4.

[53] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," IEEE Trans. Inf. Forensics Secur., vol. 8, no. 12, pp. 1947–1960, Dec. 2013.

[54] L. Zhou, V. Varadharajan, and M. Hitchens, "Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 11, pp. 2381–2395, Nov. 2015.

[55] V. C. Hu et al., "Guide to Attribute Based Access Control (ABAC) Definition and Considerations." 2014.

[56] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in Advances in Cryptology, 1985, pp. 47–53.

[57] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in Advances in Cryptology - CRYPTO 2001, 2001, pp. 213–229.

[58] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues," 2001, vol. 2260, pp. 360–363.

[59] J. Horwitz and B. Lynn, "Toward Hierarchical Identity-Based Encryption," in Advances in Cryptology - EUROCRYPT 2002, 2002, pp. 466–481.

[60] C. Gentry and A. Silverberg, "Hierarchical ID-Based Cryptography," in Advances in Cryptology - ASIACRYPT 2002, 2002, pp. 548–566.

[61] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," in Advances in Cryptology -- EUROCRYPT 2005, 2005, pp. 440–456.

[62] C. Gentry and S. Halevi, "Hierarchical Identity Based Encryption with Polynomially Many Levels," in Theory of Cryptography, 2009, pp. 437–456.

[63] Craig Gentry and Brent Waters. 2009. Adaptive Security in Broadcast Encryption Systems with Short Ciphertexts. **In Proceedings of the 28th Annual International Conference on Advances in Cryptology - EUROCRYPT 2009** - Volume 5479. Springer-Verlag, Berlin, Heidelberg, 171–188.

[64] A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption,” in Advances in Cryptology - EUROCRYPT 2005, 2005, pp. 457–473.

[65] C. Gentry, “Fully Homomorphic Encryption Using Ideal Lattices,” in Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, 2009, pp. 169–178.

[66] Rivest, R.L., Adleman, L. and Dertouzos, M.L. (1978) On Data Banks and Privacy Homomorphisms. In: Foundations of Secure Computation, Academia Press, Ghent, 169-179.

[67] D. Boneh, E.-J. Goh, and K. Nissim, “Evaluating 2-DNF Formulas on Ciphertexts”, Theory of Cryptography, 2005, pp. 325–341.

[68] Li, Z., Ma, C., Zhao, M., & Choi, C. (2019). Efficient oblivious transfer construction via multiple bits dual-mode cryptosystem for secure selection in the cloud. *Journal of the Chinese Institute of Engineers*, 42(1), 97–106.

[69] Nouf Alkhater, Robert Walters, Gary Wills, An empirical study of factors influencing cloud adoption among private sector organisations, Telematics and Informatics, Volume 35, Issue 1, 2018, Pages 38-54.

[70] S. Gülburun and M. Dener, “Bulut Bilişim Güvenliğindeki Zorluklar ve Güncel Çalışmalar Üzerine Bir İnceleme,” *Bilişim Teknolojileri Dergisi*, vol. 15, no. 1, pp. 45–53, 2022.

[71] C. Paşaoğlu and E. Cevheroğlu, "Protection of Personal Data in the Cloud Computing Systems using Cryptology Methods," *Bilişim Teknolojileri Dergisi*, vol. 13, no. 2, pp. 183–189, 2020.

[72] Adi Shamir. 1979. How to share a secret. Commun. ACM 22, 11 (Nov. 1979), 612–613.

[73] L. Chen, M. Ali Babar and B. Nuseibeh, "Characterizing Architecturally Significant Requirements," in IEEE Software, vol. 30, no. 2, pp. 38-45, March-April 2013.

[74] J. Fuller, M. Bixby, and J. Stengel, Cloud FinOps: Collaborative, Real-Time Cloud Financial Management. Sebastopol, CA: O’Reilly Media, A.B.D, 2019.

[75] Internet: Amazon Web Services, AWS Cloud Adoption Framework, https://docs.aws.amazon.com/pdfs/whitepapers/latest/overview-aws-cloud-adoption-framework/overview-aws-cloud-adoption-framework.pdf, 16.04.2025.

[76] Internet: Microsoft, Microsoft Cloud Adoption Framework for Azure, https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/, 16.04.2025.

[77] Internet: Google Cloud, The Google Cloud Adoption Framework, https://services.google.com/fh/files/misc/google_cloud_adoption_framework_whitepaper.pdf, 16.04.2025.

[78] Itzhak Aviv, Uri Ferri, Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem, *International Journal of Critical Infrastructure Protection*, Volume 43, 2023.

[79] Internet: United States Congress. (2018). Clarifying Lawful Overseas Use of Data Act. Public Law No. 115-141, Division V, Sections 101–105. https://www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf, 10.08.2025.

[80] Internet: UK National Audit Office. (2022). Digital transformation in the NHS. https://www.nao.org.uk/wp-content/uploads/2019/05/Digital-transformation-in-the-NHS.pdf, 10.08.2025.

[81] Internet: Financial Conduct Authority. (2024). Final Notice: TSB Bank plc. https://www.fca.org.uk/publication/final-notices/tsb-bank-plc-2024.pdf, 10.08.2025.

[82] Internet: European Banking Authority. (2019). EBA Guidelines on outsourcing arrangements. https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf, 10.08.2025.