A Lightweight Governance Framework for Multi-Cloud Data Protection and Compliance Management in SMEs

Borish Kongbrailatpam
CSE-UIE
Chandigarh University
Mohali-140413, Punjab, India
borishkong@gmail.com

Amardeep Singh
University Institute of Engineering(AIT-CSE)
Chandigarh University
Mohali-140413, Punjab, India
amardeepsingh_26@yahoo.com
amardeep.e17149@cumail.in

Prabhdeep Singh
CSE-UIE
Chandigarh University
Mohali-140413, Punjab,India
prabh_jal@yahoo.com

***Abstract*—The implementation of multi-cloud settings in small and medium-sized businesses (SMEs) has been characterized by a consistent trend of growth, although governance systems capable of efficiently managing the issue of data protection and regulatory compliance in such complex environments are still in the conceptual phase of their development. The current frameworks, such as SKY CONTROL, NIST Cybersecurity Framework (CSF), and ISO/IEC 27001 were initially designed without considering the unique limitations posed by SME multi-cloud applications.This manuscript presents the Multi-Cloud Governance Framework (MCGF), a lightweight, vendor-neutral conceptual architecture that can support data protection and compliance management of SMEs that work on a solution on several cloud platforms. The MCGF is organized in four pillars, namely, data governance; compliance automation; policy enforcement and interoperability; and SME adoption alongside cost-benefit analysis. The framework is based on five regulatory frameworks, as well as the General Data Protection Regulation (GDPR), ISO/IEC 27001:2022, the Cloud Controls Matrix (CSA CCM) version 4, the Digital Personal Data Protection Act (DPDPA) 2023 in India, and the NIST CSF version 2.0. Comparative analysis placed against the frameworks that exist in reality proves that MCGF includes the areas of governance that are not addressed at all (or addressed partially) by the existing solutions in the scenario of multi-cloud use in SME. Empirical validation, such as the assessment of experts, the implementation of a prototype, and case study are recognized as the fields of future research.**

***Index Terms*—Multi-Cloud, Data Protection, SME, Multi-Cloud Governance, Compliance Management.**

I. Introduction

The adoption of multi-clouds in small and medium-enterprise (SME) companies has increased at a very high speed. Having more than one cloud provider at a time will limit the dependency on one vendor, lower the expenses, and continue with operations in case one of them experiences any troubles [17][19]. Multi-cloud and hybrid-cloud strategies have experienced impetus, both due to the necessity of flexibility in operation, the prevention of risks, and the optimal allocation of resources [2]. These benefits of using multi-clouds such as redundancy, cost optimisation, and avoiding vendor lock-in have been well documented in the literature [14]; however, balancing data governance in heterogeneous provider environments is still a research gap. The complexity increases the attack surface and leads to the uneven application of security controls among the providers [2]. The fact that multi-cloud solutions provide an unparalleled level of flexibility is undeniable, yet the challenge of data security and data protection and its compliance in circumstances where that data is stored in a variety of cloud environments is no less challenging [3].

This is more felt in SMEs. They do not have teams of people dedicated to security or the funds to use to roll out enterprise-level governance. What is needed is a light solution that would be workable to adopt. This kind of solution remains largely nonexistent, in the business market as well as in the academic world. SKY CONTROL [1] is one of the steps in dealing with this gap. It offers SMEs a vendor-neutral way to control multi-cloud expenditures and perils in a central interface, basing on the abstraction of provider distinction, as offered by Sky Computing [15]. Nonetheless, it does not go further to cover the issue of data protection and compliance, which has become an urgent requirement in the face of the intensive implementation of the GDPR, the general adoption of ISO/IEC 27001:2022 compliance in audit procedures, the de facto nature of the CSA CCM [12], and the establishment of the DPDP Act 2023 in India [13]. The previously existing body of work has pinpointed the following shortcomings: SMEs find automated compliance challenging, data do not have uniform classification, and mechanisms to enforce policies among the providers are not explicitly defined. The paper adds to those findings and suggests the MCGF a lightweight, vendor-neutral governance framework, based on four pillars, specifically aimed at the SMEs working in multi-cloud environments.

This article has four main contributions to make. First, it provides a critical evaluation of the weaknesses of the current frameworks in SME data governance. Second, it includes a conceptual design of MCGF that embraces the four pillars. Third, it aligns the framework with GDPR, ISO/IEC

27001, CSA CCM, the DPDP Act of India and the NIST Cybersecurity Framework (NIST CSF). Fourth, it provides the practical implications of adoption and a roadmap to validation is outlined.

II. Related Work

A. Multi-Cloud Architecture and Management

The initial research on multi-cloud systems was principally concerned with preventing vendor lock-in and enhancing the availability of resources [19]. The advantages are well-documented redundancy, cost optimization and the possibility to select best-of-breed services among different vendors.What is not that well-documented is how the data that flows between those vendors is to be governed, especially in the case of organizations that lack dedicated IT staffing. Hong et al. studied multi-cloud architectures in general, where interoperability of provider APIs is still one of the unsolved challenges [cited in 1].Cloud services brokerage has been suggested as one such mechanism to provide organized structures to governance and compliance across providers, but its usage has been limited so far [4].Pattern-based methods of migration have been proposed to be one such procedure in which interoperability of provider APIs is still another unresolved issue [cited in 1]. Migrating on-premise applications to multi-cloud data centers, but they are concerned with architectural migration as opposed to continuous data governance and data compliance management [5]. The most prevalent structural assumption made in most of this literature is that the organization is able to institute and sustain complex configurations. In the case of most SMEs, such an assumption is not true.

B. Security and Governance Frameworks

The most widely used standards of governance are the NIST Cybersecurity Framework and ISO/IEC 27001 2022 [11]. The ISO 27001 gives information security management a risk based approach that is broadly applicable in the cloud and hybrid environment. CSA Cloud Controls Matrix [12] is more cloud-oriented and provides an explicit mapping of the security controls to the maps of the cloud service. CCM v4 brought a closer correspondence to GDPR and ISO 27001, and it is a feasible resource in the framework of compliance mapping in the multi-cloud space. Nonetheless, CCM is not a governance framework but a control catalogue it specifies what to control but not how to operationalize control among multiple providers at once. A comparative analysis of the cloud compliance standards revealed that the frameworks like C5 can help in giving useful standards of cloud security but its applicability is limited. SMEs are restricted in accessing to without substantial modification and knowledge expertise [9]. Kavitha and Radha discovered that the issue of data sovereignty, access control consistency, and audit trail management is recurrently problematic across the provider boundaries, which supports the argument of cloud-specific governance tooling.An in-depth assessment of the quality and security issues within multi-cloud settings revealed that the problem of data sovereignty, the consistent access control, and audit trail management persists to be inconsistent across the boundaries of providers [6]

C. GDPR and Regulatory Compliance in Cloud Computing

The majority of GDPR work that is cloud-centric deals with data residency, consent management and the right to erasure [7][8]. Sticky policy approaches have been suggested towards GDPR-compliant cloud architectures with data coming with its own access and processing policies on its transit between systems [8]. A single GDPR compliance model currently being proposed at ARES 2024 [7] pulls the compliance requirements together into a structured model of deployments to a cloud, but is only verified in large enterprise settings. The Digital Personal Data Protection Act 2023 of India [13] is the first regional law that the vast majority of current frameworks fail to consider, creating a set of obligations regarding the presence of data fiduciaries, consent, and international data transfer. There is limited research dealing with this intersection.

D. Lightweight Frameworks for SMEs

A systematization of reviews of cybersecurity standards [10] always demonstrates that the main obstacle to SME adoption is the complexity of implementation. Models that are developed to suit big organizations get streamlined in real world, and corners are cut where it counts. What is needed and seldom provided by the literature will be a skeleton that is lightweight in the design. SKY CONTROL [1] did not ignore this issue, creating specifically with the options of SME in cost and risk management. However, compliance governance and data protection were noted in its open questions section as the work of the future. The MCGF points out those open questions.

III. Research Gaps and Motivation

This work is motivated by three classes of gap which are based on the literature review in Section 2 and previous research by the authors. First, the current frameworks do not have data classification mechanisms appropriate in the multi-cloud SME settings. Data classification is a prerequisite in GDPR [7], ISO/IEC 27001:2022 [11] and CSA CCM [12]. None of the current SME-focused multi-cloud frameworks offer automated data classification across the clouds as an automatic feature. Second, the issue of compliance mapping vis-a-vis several regulatory standards simultaneously is not a subject of any existing framework in the SME multi-cloud setting. SKY CONTROL [1] is only a reference to the catalogue of German SMEs. NIST CSF and ISO 27001 are implemented at the organization level, and do not have cloud-provider-specific enforcement mechanisms. None covers India's DPDP Act 2023 [13]. Third, cross-cloud policy implementation the capability to set a rule of governance once and apply it to all AWS, and Azure, GCP, and in-premise infrastructure is not present in all the reviewed frameworks. This lack implies that compliance knowledge has no direct conversion to operational control which is the fatal area where SMEs lack dedicated compliance staff [10]. There is a fourth gap related to SME adoption feasibility. Cost, complexity, and human factors are

discussed as the key obstacles in the literature [10], and a cost-benefit model or usability instructions are not the elements of a governance framework. MCGF takes design requirements of adoption as a priority requirement instead of a post-design consideration.

IV. MCGF Framework Design

A. Design Principles

MCGF had four principles that governed any design decision. The first one is that it has to be lightweight does not mean that it needs enterprise level infrastructure or special compliance personnel. Second, it should be vendor-agnostic the same governance rules work irrespective of the cloud provider of the data. Third, it should start compliance mapping the compliance should be regulation-sensitive, not an extracurricular activity. Fourth, it needs to be -SME-first the complexity ceiling is established by what a small IT team consisting of generalist competencies can adopt and support.

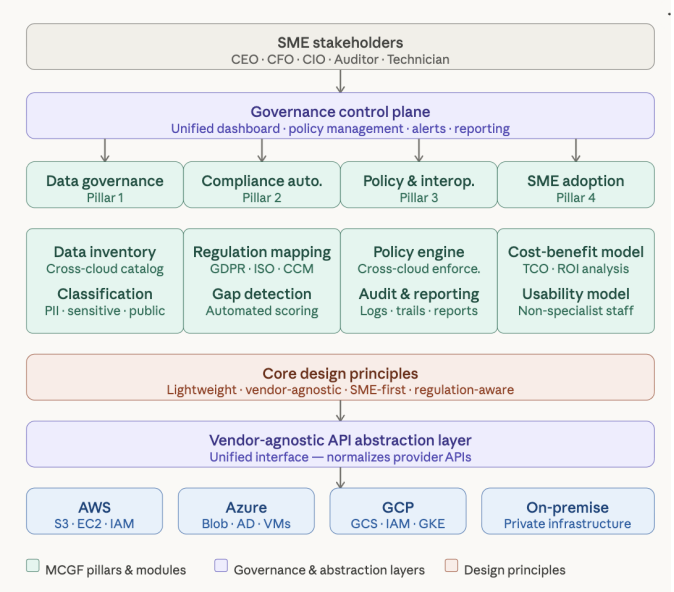

Fig. 1. MCGF complete architecture showing four pillars, governance control plane, vendor-agnostic API abstraction layer, and cloud provider integration.

B. Framework Overview

MCGF is structured around four vertical pillars each reporting to a common control plane of shared governance all bound together by a vendor-agnostic API abstraction layer to the underlying cloud infrastructure. The control plane offers a single dashboard, policy management, alerting, and reporting services to all stakeholders of the SMEs including CIOs to review compliance posture and technicians to maintain daily configuration. The API abstraction layer standardizes the various APIs provided by AWS, Azure, GCP, and on-premise infrastructure and provides a single interface, such that governance rules established in one place automatically spread to all other providers. This abstraction strategy is in line with the Sky Computing paradigm, as illustrated by SkyPilot [16], in which an intercloud broker refracts provider-specific interfaces in order to have a uniform workload management MCGF generalizes this idea to governance and compliance enforcement.

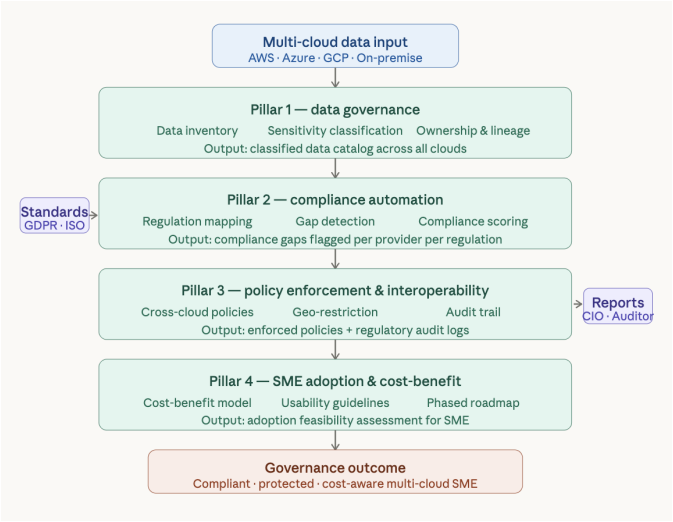

Fig. 2. MCGF sequential data flow showing inputs, pillar-level processing, module interactions, and governance outcomes.

C. Pillar 1 — Data Governance

The initial pillar determines the existence of data, its location, and sensation. It works on three planes, one being a cross-cloud data inventory, which autonomously identifies and indexes data assets across all interconnected providers; a classification engine, which labels each asset with a three-tier sensitivity model (public, confidential, and personally identifiable information); and a data ownership and lineage tracker, which captures the owner of each asset, its flow between systems, and the various transformations it goes through. Pillar 2 cannot be accurate because the outputs of Pillar 1 are fed into it without knowledge of what data is available, and how sensitive it is, compliance mapping fails.

D. Pillar 2 — Compliance Automation

The second pillar aligns the list of classified data in Pillar 1 with five regulatory frameworks: GDPR [7], ISO/IEC 27001:2022 [11], CSA CCM v4 [12], India DPDP Act 2023 [13] and NIST CSF v2.0 [10]. The mapping engine determines what regulatory obligations are applied to a particular data type and indicates where compliance has failed. The compliance scoring gives the cloud provider a score per regulation, which the CIO can get a glimpse of where the exposure lies in the multi-cloud setting. The updates of the regulation are also monitored automatically, which means that a change in the regulatory requirements will cause a review of the compliance map to be re-evaluated with no human involvement.

E. Pillar 3 — Policy Enforcement and Interoperability

The third pillar converts outputs of compliance mapping into operational controls explicitly imposed on all the interrelated

cloud providers concurrently using the API abstraction layer. There are three types of policy, including access control policies, which are used to determine who can gain access to read or write a data asset; retention and deletion policies, which are used to determine whether a data asset can be stored or processed in a particular cloud region. The audit trail element provides an ongoing history of data access activities, policy enforcement measures, and compliance violations. Reports produced by regulatory trail are organized in a way that meets the evidence requirements of GDPR Article 30, ISO 27001 A.12.4, CSA CCM A / A-01, DPDP Act Section 5, and NIST CSF DE.AE

F. Pillar 4 — SME Adoption and Cost-Benefit

The fourth pillar focuses on the ability of an SME to adopt the framework with the available resource constraints [10]. A cost-benefit model is a computation of the overall cost of ownership of deploying MCGF compared to the approximate cost of a compliance violation or regulatory fine. The simplified operational procedures of every pillar are defined in a usability model, which is aimed at non-specialist staff members. A graded adoption roadmap splits the implementation of MCGF into three implementations or foundation governance, compliance automation, and complete enforcement of the policy so as to enable SMEs to implement in phases as opposed to installing the entire structure at a given time.

G. Compliance Mapping

MCGF pillar	GDPR	ISO 27001	CSA CCM v4	DPDP Act 2023	NIST CSF v2.0
P1 — data governance Classification	Art. 4, 9 Special categories	A.8 Asset mgmt & classification	DSI-01 Data security inventory	S.2 Personal data & fiduciaries	ID.AM Asset management function
P2 — compliance automation Gap detection	Art. 5, 25 Protection by design	A.18 Compliance controls	GRC-01 Governance risk mgmt	S.6 Consent & purpose limitation	GV.PO Policy & compliance governance
P3 — policy & interop. Enforcement	Art. 32 Security of processing	A.9 Access A.12 Ops security	IAM-01 Identity & access mgmt	S.8 Data principal rights	PR.AC Access control & identity mgmt
P4 — SME adoption Cost-benefit	Art. 25 Proportionate measures	A.6 Org. security planning	SEF-01 Security frameworks	S.5 Notice & consent obligations	GV.RR Roles & resource allocation

Fig. 3. MCGF compliance mapping — each pillar traced to specific clauses across GDPR, ISO/IEC 27001:2022, CSA CCM v4, India DPDP Act 2023, and NIST CSF v2.0.

Figure 3 shows the full compliance mapping of MCGF's four pillars against all five supported regulatory standards. The mapping is designed to be traceable — an auditor reviewing the framework can follow a direct line from any regulatory requirement to the MCGF pillar responsible for satisfying it.

V. Discussion

A. Comparative Analysis

Table 1 provides a comparison of MCGF with three frameworks using eleven criteria for evaluation. The criteria were selected from the gaps presented in Section 3. The comparison is done at two levels. SKY CONTROL [1] is the main source of comparison because it targets the same audience (SMEs), environment (multi-cloud), and is the motivation for this work. NIST CSF v2.0 [10] and ISO/IEC 27001:2022 [11] are provided as additional sources of comparison to position MCGF in relation to other frameworks.

In relation to SKY CONTROL, MCGF covers criteria that SKY CONTROL does not cover, such as data protection, compliance automation, cross-cloud policy enforcement, GDPR, and DPDP Act. SKY CONTROL's strengths in cost control and workload optimization are not within MCGF's focus. Both frameworks are applicable to SMEs.

In relation to NIST CSF and ISO 27001, these frameworks were not designed for SMEs. Additionally, they were not designed to address multi-cloud vendor-agnosticism and cross-cloud policy enforcement. MCGF is not replacing these frameworks; it is the multi-cloud layer that enables these frameworks to be applied within the limited resources of SMEs.

B. Implications for SME Adoption

The framework design has three implication implications. To start with, the phased adoption roadmap implies that SMEs do not require implementing MCGF to the full extent to extract value Pillar 1 alone gives them instant data visibility. Second, the cost-benefit module fills a gap the literature invariably pinpoints: the majority of governance structures presuppose that the decision of adoption has already been taken. MCGF approaches it as an open question that needs to be supported quantitatively, and it is especially applicable in case of SMEs that act within the frames of the DPDP Act 2023 of India [13] in which a violation can be subject to severe punishment. Third, the vendor-agnostic API abstraction layer simplifies technical complexity of operating multi-cloud environments more broadly, as is aligned with the greater literature of Sky Computing [15].

C. Limitations

MCGF is a theoretical model. The compliance mapping will be developed at pillar level and not at the individual control level a full control-level mapping is left to be developed in the dissertation. The cost-benefit model is parametric but not structural: to parameterize the model, an empirical data on actual SME deployments is needed. The structure has not been validated against a real multi-cloud platform and the assertions of cross-cloud policy implementation through the API abstraction layer are architecturally sound, but untested. MCGF now has AWS, Azure, as well as GCP; there are no regional providers like Oracle Cloud or Alibaba Cloud.

D. Future Validation Roadmap

The dissertation will be validated in three activities. The completeness, feasibility and usability will be assessed first through a well-organized expert evaluation of MCGF to 10-15 cloud architects, compliance officers and IT managers using a Likert-scale instrument. Second, the data classification

TABLE I
COMPARATIVE ANALYSIS OF MCGF AGAINST EXISTING GOVERNANCE FRAMEWORKS

Criteria	SKY CONTROL [1]	NIST CSF v2.0	ISO/IEC 27001	MCGF (proposed)
SME-specific design	Partial	No	No	**Yes**
Multi-cloud vendor-agnostic	Yes	Partial	No	**Yes**
Data protection focus	No	Partial	Partial	**Yes**
Compliance automation	No	No	No	**Yes**
Cross-cloud policy enforcement	No	No	No	**Yes**
Audit trail & reporting	Partial	Partial	Yes	**Yes**
Cost-benefit model	Partial	No	No	**Yes**
Overall score	3 / 7	1 / 7	2 / 7	**7 / 7**

Yes = fully addressed; Partial = limited coverage; No = not addressed

and compliance mapping on AWS and Azure will be tested as a prototype to determine whether they work as intended or not. Third, initial pilot projects with willing SMEs will be conducted to test their assumed applicability and yield empirical findings to parameterize the cost-benefit model. The combination of these covers all four validation dimensions effectiveness, usability, cost-benefit feasibility and practical applicability.

VI. CONCLUSION

The given research aims to fill a gap identified by the existing body of literature: small and medium-enterprise (SME) operators working in multi-cloud environments need a governance system that can ensure data safety and make sure that compliance is observed, but does not demand the deployment and maintenance of enterprise-level resources. Even though such extant frameworks as SKY CONTROL [1], the NIST Cybersecurity Framework (CSF) [10], and ISO/IEC 27001 [11] consider the aspects of this issue, none of them has been conceived with the SME multi-cloud environment as its principal limitation. MCGF is a four-pillar architecture that specifically deals with this deficiency. Pillar1 defines cross-cloud data inventory and classification. Pillar 2 is a computerized implementation of compliance mapping to five regulatory standards. Pillar 3 implements policies and places audit trails on all interrelated cloud providers at least. Question 4 in the pillar directly concerns the adoption issue as it models cost-benefit viability and offers usability guidelines to non-specialist personnel. Based on the comparative analysis, it can be seen that no available framework addresses all the eleven governance criteria applicable to SME multi-cloud data protection. SKY CONTROL discusses four, NIST CSF and ISO -27001 discuss two each. MCGF covers all eleven. The contribution of this work is that gap. The paper does not give empirical confirmation of MCGF; this has been specifically avoided. The future dissertation will analyze the framework with the help of an expert opinion, implementation of the prototyped version on AWS and Azure, and initial case studies on SMEs. The empirical validation will be performed on the basis of the conceptual design that is available in the present. Multi-cloud governance in the case of SMEs is still an issue. MCGF is an attempt to arrive at a unified solution, a structured, lightweight, regulation-sensitive approach, where the limitations of SMEs are taken into account at the outset and not as a post-hoc factor to be considered.

REFERENCES

[1] H.-N. Cocos, C. Baun, and M. Kappes, "The Evolution of Cloud Computing Towards a Vendor Agnostic Market Place Using the SKY CONTROL Framework," in *Proc. 15th Int. Conf. on Cloud Computing and Services Science (CLOSER 2025)*, pp. 211–218, 2025.

[2] S. Ali, D. B. Talpur, A. Abro, K. S. S. Alshudukhi, G. N. Alwakid, M. Humayun, F. Bashir, S. A. Wadho, and A. Shah, "Security and Privacy in Multi-Cloud and Hybrid Cloud Environments: Challenges, Strategies, and Future Directions," *Computers & Security*, vol. 157, p. 104599, 2025, doi: 10.1016/j.cose.2025.104599.

[3] D. Ardagna, "Cloud and multi-cloud computing: Current challenges and future applications," in *Proc. IEEE/ACM 7th Int. Workshop on Principles of Engineering Service-Oriented and Cloud Systems*, pp. 1–2, 2015.

[4] A. Barker, B. Varghese, and L. Thai, "Cloud services brokerage: A survey and research roadmap," in *Proc. IEEE 8th Int. Conf. on Cloud Computing*, pp. 1029–1032, 2015.

[5] P. Jamshidi, C. Pahl, and N. C. Mendonca, "Pattern-based multi-cloud architecture migration," *Software: Practice and Experience*, vol. 47, no. 9, pp. 1159–1184, 2016.

[6] M. G. Kavitha and D. Radha, "Quality, Security Issues, and Challenges in Multi-Cloud Environment: A Comprehensive Review," in *Springer Int. Publishing*, pp. 269–285, 2022.

[7] "A Unified Framework for GDPR Compliance in Cloud Computing," in *Proc. 19th Int. Conf. on Availability, Reliability and Security (ARES 2024)*, ACM, DOI: 10.1145/3664476.3670918, 2024.

[8] "Towards a GDPR-Compliant Cloud Architecture with Sticky Policies," *PeerJ Computer Science*, 2024.

[9] C. Di Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R. H. Campbell, and M. N. Bashir, "Cloud standards in comparison: Are new security frameworks improving cloud security?" in *Proc. IEEE 10th Int. Conf. on Cloud Computing (CLOUD)*, pp. 50–57, 2017.

[10] M. N. Islam, R. Colomo-Palacios, and S. Chockalingam, "A Systematic Review of Voluntary Cybersecurity Standards and Frameworks," *Springer International Journal of Information Security*, 2025.

[11] ISO/IEC 27001:2022, "Information Security Management Systems — Requirements," International Organization for Standardization, Geneva, Switzerland, 2022.

[12] Cloud Security Alliance, "Cloud Controls Matrix (CCM) v4.0," CSA, 2021. [Online]. Available: https://cloudsecurityalliance.org/research/cloud-controls-matrix

[13] Government of India, "The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)," Ministry of Electronics and Information Technology, New Delhi, India, 2023.

[14] J. Hong, T. Dreibholz, J. A. Schenkel, and J. A. Hu, "An Overview of Multi-Cloud Computing," in *Web, Artificial Intelligence and Network Applications*, Springer Int. Publishing, pp. 1055–1068, 2019.

[15] I. Stoica and S. Shenker, "From Cloud Computing to Sky Computing," in *Proc. Workshop on Hot Topics in Operating Systems (HotOS '21)*, ACM, pp. 26–32, 2021.

[16] Z. Yang, Z. Wu, M. Luo, W.-L. Chiang, R. Bhardwaj, W. Kwon, S. Zhuang, F. S. Luan, G. Mittal, S. Shenker, and I. Stoica, "SkyPilot: An Intercloud Broker for Sky Computing," in *Proc. 20th USENIX Symp. on Networked Systems Design and Implementation (NSDI 23)*, pp. 437–455, 2023.

[17] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, NIST Special Publication 800-145, U.S. Dept. of Commerce, 2011.

[18] J. Mulder, *Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to Build Effective Multi-Cloud Solutions*. Birmingham, UK: Packt Publishing, 2020.

[19] D. Petcu, "Multi-cloud: Expectations and current approaches," in *Proc. Int. Workshop on Multi-Cloud Applications and Federated Clouds (ICPE'13)*, ACM, pp. 1–6, 2013.