

Data Sovereignty over the Cloud: An Examination of the Cloud Environment in Qatar

Abdulrahman Mohammed M SH Al-Shafi

Masters of Public Policy (HBKU) - Director of Cyber Strategies and Policies Department
National Cyber Security Agency (NCSA)

Data Sovereignty over the Cloud: An Examination of the Cloud Environment in Qatar

Abdulrahman Mohammed M SH Al-Shafi

Masters of Public Policy (HBKU) - Director of Cyber Strategies and Policies Department
National Cyber Security Agency (NCSA)

ABSTRACT

This paper project delves into the evolving landscape of cloud data sovereignty in Qatar, scrutinizing the dynamic interplay between technological advancements and legal frameworks. The study focuses on understanding the critical aspects of data sovereignty in cloud computing, particularly under Qatar's rapidly developing digital infrastructure. Using a mixed-methods approach, the research incorporates insights from qualitative interviews with key industry and academic experts alongside a comprehensive review of 15 pertinent studies. The qualitative segment explores first-hand perspectives from government officials, legal experts, and technology professionals, uncovering themes around data localization, regulatory compliance, and the distinct nuances of private versus public cloud environments. The literature review supplements this by providing a broader understanding of global trends and contextualizing Qatar's unique challenges and opportunities within the global cloud computing scenario.

Findings reveal a complex tapestry of issues, ranging from regulatory challenges and privacy concerns to strategic implications for national security and economic development. The study underscores the need for robust legal and regulatory frameworks in Qatar to navigate the intricate world of cloud data sovereignty. It also offers practical recommendations for policymakers, cloud service providers, and end-users, aiming to foster an environment conducive to technological innovation while safeguarding data sovereignty. This paper contributes to the ongoing discourse on cloud computing in Qatar, providing a nuanced understanding of the intersection between technology, law, and policy in the digital age.

Keywords: Cloud Computing, Data Sovereignty, Digital Transformation, Technological Innovation, Legal and Regulatory Framework, Policymakers.

المُلخَص

سيادة البيانات على الحوسبة السحابية: دراسة لبيئة الحوسبة السحابية في دولة قطر

عبدالرحمن محمد آل شافي

مدير إدارة الاستراتيجيات والسياسات السيبرانية - الوكالة الوطنية للأمن السيبراني

يستكشف هذا المشروع البحثي المشهد المتطور لسيادة البيانات السحابية في قطر، ويفحص التفاعل الديناميكي بين التقدم التكنولوجي والأطر القانونية. تركز الدراسة على فهم الجوانب الحاسمة لسيادة البيانات في الحوسبة السحابية، وخاصة في ظل البنية التحتية الرقمية سريعة التطور في قطر. باستخدام نهج الأساليب المختلطة، يدمج البحث بعض من المقابلات النوعية مع خبراء الصناعة والأكاديميين الرئيسيين إلى جانب مراجعة شاملة لـ 15 دراسة ذات صلة.

يستكشف الجزء النوعي وجهات نظر مباشرة من المسؤولين الحكوميين والخبراء القانونيين ومحترفي التكنولوجيا، ويكشف عن موضوعات حول توطين البيانات والامتثال التنظيمي والفروق الدقيقة المميز لبيئات السحابة الخاصة مقابل العامة. تكمل مراجعة الأدبيات هذه من خلال توفير فهم أوسع للاتجاهات العالمية ووضع تحديات وفرص قطر الفريدة في سياق سيناريو الحوسبة السحابية العالمية.

تكشف النتائج عن نسيج معقد من القضايا، بدءاً من التحديات التنظيمية ومخاوف الخصوصية إلى الآثار الاستراتيجية على الأمن القومي والتنمية الاقتصادية. تؤكد الدراسة على الحاجة إلى أطر قانونية وتنظيمية قوية في قطر للتنقل في عالم السيادة على البيانات السحابية المعقدة. كما يقدم توصيات عملية لصناع السياسات ومقدمي خدمات الحوسبة السحابية والمستخدمين النهائيين، بهدف تعزيز بيئة مواتية للابتكار التكنولوجي مع حماية سيادة البيانات. يساهم هذا المشروع في الحوار المستمر حول الحوسبة السحابية في قطر، مما يوفر فهماً دقيقاً للتقاطع بين التكنولوجيا والقانون والسياسة في العصر الرقمي.

الكلمات المفتاحية: الحوسبة السحابية، سيادة البيانات، التحول الرقمي، الابتكار التكنولوجي، الأطر القانونية والتنظيمية، صناع السياسات.

1. Introduction

ICTs have transformed almost all sectors, especially the public sector, which uses them to improve efficiency, transparency, and service delivery. ICTs have enabled e-government, which is more efficient, resource-efficient, and public-engaged⁽¹⁾. This transformation is essential for the public sector to respond quickly to societal needs and increase access to digital tools in front-end services and data⁽²⁾. Cloud computing has become essential to ICTs, providing scalable and flexible solutions to meet changing public administration needs. Cloud computing allows online data storage, processing, and management without servers or hardware⁽³⁾. This savings helps public sector organizations deliver services cheaper, faster, and more agilely⁽⁴⁾. Cloud computing has the potential to revolutionize public administration through data-driven decision-making and service innovation. Cloud technologies enable government departments to share data and collaborate, thereby enhancing integrated service delivery and operational efficiency⁽⁵⁾. Data is not just important, it's crucial for urban management and policy applications in smart cities and digital governance⁽⁶⁾. Local laws ensure the protection of sensitive government data, meeting national security and data sovereignty requirements in the public sector⁽⁷⁾. A comprehensive understanding of the cloud is essential to meet administrative and citizen demands in this digital age. In the following paragraphs, we will delve into how cloud computing fits into public sector modernization using Qatari study case data, and how data-driven decision-making is shaping the future of public policies.

The study examines public sector ICT use, with a specific focus on the transformative role of cloud computing. The digitalisation of public services has led to a cloud-based approach to scaling and flexing IT resources. This is crucial for public administrations to enhance service delivery, citizen engagement, and efficiency⁽⁸⁾.

(1) J. C. Bertot, P. T. Jaeger, and J. M. Grimes, "Using ICTs to Create a Culture of Transparency: E-Government and Social Media as Openness and Anti-Corruption Tools for Societies," *Government Information Quarterly* 27, no. 3 (2010): 264–271.

(2) F. Bannister and R. Connolly, "ICT, Public Values and Transformative Government: A Framework and Programme for Research," *Government Information Quarterly* 31, no. 1 (2014): 119–128.

(3) S. Marston et al., "Cloud Computing—The Business Perspective," *Decision Support Systems* 51, no. 1 (2011): 176–189.

(4) Y. Alshamaila, S. Papagiannidis, and F. Li, "Cloud Computing Adoption by SMEs in the North East of England: A Multi-Perspective Framework," *Journal of Enterprise Information Management* 26, no. 3 (2013): 250–275.

(5) A. Chandrasekaran and M. Kapoor, "State of the Public Cloud: The Cloud Adoption Conundrum," *Infosys Labs Briefings* 9, no. 1 (2011): 3–10.

(6) T. Clohessy, T. Acton, and L. Morgan, "Smart City as a Service (SCaaS): A Future Roadmap for E-Government Smart City Cloud Computing Initiatives," *Digital Policy, Regulation and Governance* 19, no. 1 (2017): 58–69.

(7) H. Yang and M. Tate, "A Descriptive Literature Review and Classification of Cloud Computing Research," *Communications of the Association for Information Systems* 31, no. 1 (2012): 2–57.

(8) M. Janssen, E. Estevez, and T. Janowski, "Interoperability in Big, Open, and Linked Data—Organizational

As governments worldwide transition towards post-industrial infrastructures to meet rising citizen demands and the need for transparency and productivity, cloud computing emerges as a timely, cutting-edge research topic⁽⁹⁾. Modern public sector operations require a significant amount of data, and cloud computing provides the elasticity to host and store it. It simplifies data processing, thereby improving digital governance and decision-making. The cloud allows public sector entities to store and process data from the internet rather than on a local server, providing real-time information to inform policy decisions that enhance public service delivery⁽¹⁰⁾. This capability aids smart governance by enabling data-driven systems to better manage urban infrastructure and services⁽¹¹⁾.

The study meets the International Journal of Public Administration and Digital Administration (IJPADA) scope of innovative public sector management practices. The journal prioritises digital tools in public administration, particularly how they can improve governance (IJPADA n.d., 5). This paper explores the many uses of cloud computing in public sector management to improve administrative processes and service delivery. It examines public sector cloud adoption opportunities and challenges, including data security, privacy, and regulatory compliance. This mixed-method study examined cloud-based solutions' security and deployment challenges for public sector organisations⁽¹²⁾. It addresses IJPADA's digital transformation challenges in public administration and provides a deeper understanding of ICTs' barriers to IOS participation. This research also examines cloud computing's impact on public sector efficiency beyond IT, using case studies to show best practices and lessons learned. The study examines real-world applications and offers policymakers practical insights into digital service transformation⁽¹³⁾.

This study uniquely explores leadership styles in Qatari public sector cloud adoption, addressing a gap in research typically focused on technology and policy. Cloud leadership involves strategic vision, decision-making, and management

Maturity, Capabilities, and Data Portfolios,” *Government Information Quarterly* 31, no. 3 (2014): S57–S68.

(9) V. Weerakkody, M. Janssen, and Y. K. Dwivedi, “Transformational Change and Business Process Reengineering (BPR): Lessons from the British and Dutch Public Sector,” *Government Information Quarterly* 28, no. 1 (2016): 27–36.

(10) J. R. Gil-Garcia, N. Helbig, and A. Ojo, “Being Smart: Emerging Technologies and Innovation in the Public Sector,” *Government Information Quarterly* 31, no. S1 (2014): S2–S8.

(11) T. Nam and T. A. Pardo, “Conceptualizing Smart City with Dimensions of Technology, People, and Institutions,” in *Proceedings of the 12th Annual International Conference on Digital Government Research* (2011): 282–291.

(12) M. Almorsy, J. Grundy, and I. Müller, “An Analysis of the Cloud Computing Security Problem,” *Communications of the ACM* 59, no. 1 (2016): 38–46.

(13) A. Cordella and N. Tempini, “E-Government and Organizational Change: Reappraising the Role of ICT and Bureaucracy in Public Service Delivery,” *Government Information Quarterly* 32, no. 3 (2015): 279–286.

practices crucial for cloud computing adoption. The study examines how Qatari leaders navigate these dynamics, emphasizing strategic foresight, risk management, innovation, and compliance. Given that leadership drives digital transformation⁽¹⁴⁾, integrating cloud technologies into public administration supports Qatar's knowledge-based economy. This research highlights the importance of change management, stakeholder engagement, and ethics, showing that effective leadership is key to enhancing public sector productivity through cloud computing⁽¹⁵⁾.

This study also shows how leadership styles affect cloud computing resource management and strategic partnerships with cloud service providers. Leaders can improve service agreements, adapt to new technologies, and use outside experts better⁽¹⁶⁾. This collaborative leadership style is ideal for Qatari public sector organisations that hire foreign cloud service providers to set up and run their digital infrastructures. Qatar National Vision 2030 (QNV 2030) calls for a digital transformation, making it a good place to study cloud computing and data sovereignty. QNV 2030 aims to make Qatar a knowledge-based economy by 2030. This change will heavily involve ICTs. Qatar has invested heavily in digital infrastructure, including the Qatar Smart Program. Cloud computing improves public services and diversifies the economy⁽¹⁷⁾. Qatar's legal system blends Islamic and modern law. This makes data sovereignty discussions unique. The Personal Data Privacy Protection Law No. 13 of 2016 establishes a comprehensive data protection system similar to the EU's General Data Protection Regulation (GDPR) but tailored to Qatar's legal and cultural norms⁽¹⁸⁾. This dual legal system alters data sovereignty and makes it harder to enforce national and international laws⁽¹⁹⁾.

This case study extends beyond Qatar, offering insights for nations balancing data sovereignty with global cloud services. Qatar's experience aids in managing cross-border data flows, establishing compliance, and negotiating international agreements⁽²⁰⁾. This is vital for MENA markets with diverse legal systems⁽²¹⁾. Qatar's government-led digital transformation, supported by the QNV 2030, exemplifies

(14) J. D. Houghton, A. Carnes, and C. N. Ellison, "A Cross-Sectional Examination of Transformational Leadership and Transformational Leaders in the United States," *Leadership Quarterly* 26, no. 3 (2015): 437–447.

(15) I. Nurdiani, M. S. Börjesson, and L. Angelis, "A Systematic Mapping Study on the Combination of Agile Software Development and Leadership Styles," *Journal of Systems and Software* 161 (2020): 110459.

(16) R. Heeks and C. Stanforth, "Technological Change in Developing Countries: Opening the Black Box of Process Using Actor-Network Theory," *Development Studies Research* 2, no. 1 (2015): 33–50.

(17) Ministry of Transport and Communications, Qatar Smart Program (TASMU) (Ministry of Transport and Communications, 2019).

(18) Qatar Financial Centre, Personal Data Privacy Protection Law No. 13 of 2016 (Qatar Financial Centre, 2020).

(19) Baker McKenzie, "Qatar: Data Protection Overview," Baker McKenzie, 2021.

(20) M. Al-Naama, "Data Sovereignty in the GCC: Legal and Regulatory Perspectives," *Gulf Affairs*, 2022.

(21) GCC-STAT, GCC Statistical Centre: Data Sovereignty and Cloud Computing (GCC-STAT, 2022).

how public investment can enhance cloud computing while safeguarding data sovereignty. These strategies provide a model for countries with similar challenges, helping to shape policies that integrate legal, economic, and cybersecurity measures effectively⁽²²⁾. While cloud computing has been increasingly adopted by the public sector, there remains a significant gap in understanding how leadership styles influence the successful adoption and implementation of cloud technologies, particularly in regions like Qatar where digital transformation is driven by national strategies such as Qatar National Vision 2030. Current literature primarily focuses on technical aspects of cloud computing or general policy implications⁽²³⁾, but fails to explore the role of leadership in this transformation. This study aims to fill this gap by examining how different leadership styles within Qatari public sector organizations impact cloud adoption, data sovereignty, and public service delivery. Specifically, the research seeks to explore the strategic decisions leaders make, their approach to managing change, and how they foster collaboration with cloud service providers. This is crucial for understanding how leadership can drive innovation in public administration, and how such insights can be applied globally in similar contexts. By addressing this gap, the study contributes to the growing body of knowledge on public sector modernization and digital governance, providing a nuanced understanding of the leadership challenges and opportunities in cloud computing adoption.

Research Question

How does the adoption of cloud computing in Qatar's public sector influence leadership styles and data sovereignty while ensuring compliance with national and international regulations?

Revised Research Objectives:

1. **To Identify Key Leadership Traits:** Analyse specific leadership traits and decision-making strategies that facilitate the successful adoption and management of cloud computing in Qatar's public sector, focusing on their role in overcoming implementation challenges.
2. **To Evaluate the Impact of Cloud Computing on Data Sovereignty:** Assess how cloud computing adoption impacts Qatar's data sovereignty, specifically examining the balance between utilizing global cloud services and adhering to national data privacy laws and international regulations.
3. **To Explore Compliance Strategies:** Investigate the strategies used by Qatar's

(22) S. Chakraborty and K. Joseph, *ICT and Digital Transformation in the Middle East* (Routledge, 2021).

(23) Y. Alshamaila, S. Papagiannidis, and F. Li, "Cloud Computing Adoption by SMEs in the North East of England: A Multi-Perspective Framework," *Journal of Enterprise Information Management* 26, no. 3 (2013): 250–275

public sector to ensure compliance with both national and international data protection and privacy laws, particularly in the context of cross-border data flows enabled by cloud services.

The study will demonstrate how Qatar's government can use cloud computing to boost operational efficiency, data privacy, and digital transformation leadership. This study offers valuable insights for Qatari policymakers, public administrators, and IT leaders by analysing government cloud technology adoption. It highlights how public institutions can improve efficiency, security, and compliance with data sovereignty. The study provides a roadmap for balancing global cloud benefits with data sovereignty, aligning with Qatar's National Vision 2030, and offers recommendations for effective leadership and ICT integration in the public sector⁽²⁴⁾⁽²⁵⁾⁽²⁶⁾.

2. Literature Review

2.1. Evolution of Cloud Computing

The global rise of cloud computing, including in Qatar, marks a transformative shift in information technology, characterized by significant advancements and unique adaptations to meet evolving demands. This literature review explores cloud computing's evolution and Qatar's distinctive journey. Cloud computing originated from mainframes and evolved through grid and utility computing⁽²⁷⁾, transitioning from traditional on-premises IT to scalable, service-focused models. Zhang et al.⁽²⁸⁾ highlight how cloud computing minimizes the need for extensive hardware, enabling on-demand services. This shift has revolutionized business paradigms across industries⁽²⁹⁾, facilitating flexible, pay-as-you-go services⁽³⁰⁾. Mishra et al.⁽³¹⁾ discuss the importance of speed, scalability, and availability in public and multi-cloud systems. Qatar's cloud computing strategy, aligned with its ambitious digitalization

(24) P. Banerjee, "Governing the Cloud: Policy Strategies for Data Sovereignty and Digital Infrastructure," *Digital Policy, Regulation and Governance* 24, no. 2 (2022): 125–137.

(25) Q. Zhang, L. Cheng, and R. Boutaba, "Cloud Computing: State-of-the-Art and Research Challenges," *Journal of Internet Services and Applications* 1 (2010): 7–18.

(26) X. Zhu, H. Liu, and S. Wei, "Cloud Computing Adoption in the Public Sector: A Meta-Analysis of Antecedents and Outcomes," *Information Systems Frontiers* 23, no. 5 (2021): 1229–1248.

(27) D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," *Future Generation Computer Systems* 28, no. 3 (2012): 583–592.

(28) Q. Zhang, L. Cheng, and R. Boutaba, "Cloud Computing: State-of-the-Art and Research Challenges," *Journal of Internet Services and Applications* 1 (2010): 7–18.

(29) S. Marston et al., "Cloud Computing—The Business Perspective," *Decision Support Systems* 51, no. 1 (2011): 176–189.

(30) B. Biočić, D. Tomić, and D. Ogrizović, "Economics of Cloud Computing," in 2011 Proceedings of the 34th International Convention MIPRO (2011): 1438–1442.

(31) M. Mishra et al., "An Assessment of Cloud Computing: Evolution," *Journal of Cloud Computing: Advances, Systems and Applications*, 2020.

goals, is anchored in strategic vision, with investments in cutting-edge data centres and global tech partnerships⁽³²⁾.

Period	Key Developments	Significant Contributors	References
1960s-1970s	Concept of utility computing by John McCarthy; early forms of shared resource computing.	John McCarthy and others in the field of shared computing.	Peterson et al., 2011
1980s-1990s	The emergence of grid computing; early Internet-based computing developments.	Development of grid computing concepts by various researchers and technologists.	Zissis & Lekkas, 2012
The early 2000s	Cloud computing begins to take shape with the introduction of AWS, enabling more comprehensive access to computing resources.	Amazon Web Services (AWS) and other early cloud service providers.	Zhang et al., 2010
Late 2000s-2010s	Rapid expansion of cloud services; introduction of major platforms like AWS, Azure, and Google Cloud.	Major tech companies like Amazon, Microsoft, and Google are developing and expanding cloud platforms.	Marston et al., 2011; Biocic et al., 2011
2010s-Present	Advancements in cloud technology are increasing the focus on data sovereignty, privacy, security, and GDPR implementation.	Global policymakers, technologists, and organisations focusing on data security and sovereignty laws.	Banse, 2021; Giese & Anderl, 2022

Table 1. Evolution of Cloud Computing

Qatar's adoption of cloud computing has enhanced service delivery and spurred innovation⁽³³⁾, yet it faces significant challenges, particularly in data privacy and security. These challenges are unique due to the need to align rapidly evolving cloud technologies with Qatar's specific legal and cultural frameworks, such as the Qatar Personal Data Protection Law. Cloud computing has revolutionized IT, driving economic and strategic shifts globally⁽³⁴⁾. In Qatar, this transformation is further complicated by the need to balance digital advancement with stringent data protection and cultural sensitivities.

(32) M. S. Rehman and M. F. Sakr, "Teaching the Cloud: Experiences in Designing and Teaching an Undergraduate-Level Course in Cloud Computing at Carnegie Mellon University in Qatar," in 2011 IEEE Global Engineering Education Conference (EDUCON) (2011): 875–879.

(33) N. Sultan, "Cloud Computing: A Democratising Force?" International Journal of Information Management 33, no. 5 (2013): 810–815.

(34) S. Marston et al., "Cloud Computing—The Business Perspective," Decision Support Systems 51, no. 1 (2011): 176–189.

2.2. Data Sovereignty in Cloud Computing

Cloud computing "data sovereignty" has become a critical area of study due to the growing complexity of managing data across jurisdictions. This literature review explores global data sovereignty, with a particular focus on Qatar. Data sovereignty refers to the legal and practical control over data stored in the cloud. Peterson et al.⁽³⁵⁾ highlight the challenges of establishing control over virtualized and globally distributed data, which is complicated by decentralized cloud services. This is especially problematic in maintaining data within the correct legal jurisdiction.

Banse⁽³⁶⁾ discusses how the EU General Data Protection Regulation (GDPR), the European Cybersecurity Certification Scheme for Cloud Services (EUCS), and Gaia-X complicate data privacy in open cloud ecosystems. While protected enclaves and encrypted virtual machine memory offer new ways to safeguard data, they do not fully secure the system. Giese and Anderl⁽³⁷⁾ emphasize the importance of secure data sharing for virtual product development, particularly in controlling dispersed data in cloud environments. Sun et al.⁽³⁸⁾ examine software and hardware security challenges in cloud computing, underscoring the need for robust privacy measures. Irion⁽³⁹⁾ discusses data sovereignty in government cloud services, highlighting legal risks that technology and contracts alone cannot mitigate. Qatar, with its evolving technology and strict data control standards, must balance global technological standards with its own legal frameworks to manage cloud computing data sovereignty effectively.

2.3. Regulatory and Legal Framework

As digital data increasingly crosses borders, cloud computing data sovereignty regulations have become crucial. These frameworks address the complex legal, ethical, and technical challenges of storing and processing data in a global, decentralized cloud environment. The European Union's General Data Protection Regulation (GDPR) has significantly transformed global data protection standards, imposing

(35) Z. N. J. Peterson, M. Gondree, and R. Beverly, "A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud," in Proceedings of the 3rd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud '11) (2011).

(36) C. Banse, "Data Sovereignty in the Cloud—Wishful Thinking or Reality?" in Proceedings of the 2021 on Cloud Computing Security Workshop (2021): 153–154.

(37) T. Giese and R. Anderl, "Maintaining Control over Distributed Data through a Data Sovereignty Model," in 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA) (2022): 1–7.

(38) Y. Sun et al., "Data Security and Privacy in Cloud Computing," International Journal of Distributed Sensor Networks 10, no. 7 (2014): 190903.

(39) K. Irion, "Government Cloud Computing and National Data Sovereignty," Policy & Internet 4, no. 3-4 (2012): 40–71.

strict responsibilities on data controllers and processors while enhancing individual rights⁽⁴⁰⁾⁽⁴¹⁾. The GDPR's extraterritorial reach means that organizations outside the EU, including those in Qatar, must comply when handling EU residents' data, raising complex sovereignty issues⁽⁴²⁾. In Qatar, the GDPR's relevance is twofold: Qatari organizations dealing with EU data must align with GDPR standards, necessitating an international compliance strategy. Additionally, Qatar's Personal Data Protection Law, inspired by the GDPR, reflects the nation's commitment to high data protection standards. However, balancing local laws with international regulations presents challenges, particularly in ensuring compliance while navigating global data protection complexities. The importance of geolocating cloud data is emphasized by Peterson et al.⁽⁴³⁾, who highlight the legal and policy challenges when data is virtualized and distributed globally. Qatar's proactive approach to cloud computing and data security, especially in government services, underscores its commitment to maintaining data sovereignty while engaging with the global digital economy⁽⁴⁴⁾.

Period	Regulatory Framework	Key Features	Impact on Cloud Computing
The early 2000s	Data Protection Directive (EU)	Protection of personal data and privacy.	Increased awareness of data privacy and sovereignty.
2008-2010	Health Information Technology for Economic and Clinical Health (HITECH) Act (USA)	Enhanced data protection for health information.	Heightened focus on securing health-related data in the cloud.
2012	General Data Protection Regulation (GDPR) Proposal (EU)	Comprehensive data protection regulation, including data sovereignty.	A significant shift in cloud data management and compliance requirements.
2016	GDPR Enforcement (EU)	Strict data protection and privacy standards; heavy fines for non-compliance.	Significant impact on cloud service providers; focus on data localisation and sovereignty.
2018	California Consumer Privacy Act (CCPA) (USA)	Similar to GDPR, it focuses on consumer privacy rights.	Influencing cloud computing policies and practices in the USA.
2020s	Emergence of National Data Protection Laws (Global)	Countries worldwide enacting data protection laws, influencing cloud computing practices.	Global cloud services adapting to diverse national regulations.

Table 2. Regulatory Framework

(40) C. Banse, "Data Sovereignty in the Cloud—Wishful Thinking or Reality?" in Proceedings of the 2021 on Cloud Computing Security Workshop (2021): 153–154.

(41) N. J. King and V. T. Raja, "Protecting the Privacy and Security of Sensitive Customer Data in the Cloud," Computer Law & Security Review 28, no. 3 (2012): 308–319.

(42) A. Kronabeter and S. Fenz, "Cloud Security and Privacy in the Light of the 2012 EU Data Protection Regulation," in Cloud Computing: Third International Conference, CloudComp 2012, Vienna, Austria, September 24–26, 2012, Revised Selected Papers, 3 (Springer International Publishing, 2013): 114–123.

(43) Z. N. J. Peterson, M. Gondree, and R. Beverly, "A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud," in Proceedings of the 3rd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud '11) (2011).

(44) T. Giese and R. Anderl, "Maintaining Control over Distributed Data through a Data Sovereignty Model," in 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA) (2022): 1–7.

Regulation/Law	Description and Objective	Governing Body or Authority
Qatar Personal Data Protection Law (Law No. 13 of 2016)	It focuses on protecting personal data, regulates data processing activities, and ensures individuals' rights regarding their data.	National Cyber Security Agency (NCSA)
Qatar Cybercrime Prevention Law (Law No. 14 of 2014)	Addresses offences committed through information networks or computers, including unauthorised access, data breaches, and cyberattacks.	Ministry of Interior
Law No. (34) of 2006 on Electronic Commerce and Transactions	Establishes the legal framework for electronic transactions and e-commerce, including data authenticity and security measures.	Ministry of Commerce and Industry
Qatar Central Bank's Circulars on Electronic Payments	Regulates electronic payments, emphasises data security standards, and governs financial transactions through digital platforms.	Qatar Central Bank
National Information Assurance Policy (Data Classification)	Sets out policies and standards for information security in public and private sectors, aiming to protect against cyber threats and data breaches.	National Cyber Security Agency (NCSA)
Qatar Cloud Policy Framework	Provides guidelines and principles for cloud adoption in government and semi-government entities, focusing on data sovereignty and security.	Ministry of Transport and Communications

Table 3. Laws and Regulations Governing Data Sovereignty in Qatar

2.4. Technological Perspectives

Cloud computing makes data sovereignty difficult and requires new technologies and strategies. Many solutions in the literature address different data sovereignty issues. These solutions include best practices for encryption, data localisation, and cloud data sharing. One of the best ways to protect cloud data is encryption. Attribute-based encryption (ABE) is a significant advancement in this sector since it lets you restrict data access based on user characteristics. Complex cloud access rules are best enforced using this strategy⁽⁴⁵⁾. Homomorphic encryption allows the handling of encrypted data without revealing its contents, thereby protecting data privacy⁽⁴⁶⁾. Data privacy is increasingly protected via localisation. Businesses that keep data

(45) S. Yu et al., "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," in 2010 Proceedings IEEE INFOCOM (2010): 1–9.

(46) K. Shatilov et al., "Solution for Secure Private Data Storage in a Cloud," in 2014 Federated Conference on Computer Science and Information Systems (2014): 885–889.

locally can follow local data protection laws. The inherent nature of cloud computing, distributing data across multiple servers, introduces complex security challenges. For instance, the traditional approach of securing data in a localised data centre may lead to inefficiencies in a cloud environment, as it necessitates additional layers of security for data stored across various locations. This often results in increased costs and management complexity. A notable example is the need for advanced encryption methods during data transmission and at rest. Furthermore, it's essential to develop robust protocols for updating, deleting, and appending data in the cloud to mitigate risks of unauthorised access or data breaches⁽⁴⁷⁾. These measures are critical for maintaining data integrity and security in the cloud⁽⁴⁸⁾. Data storage security remains crucial with cloud computers. Plans are needed to protect distributed cloud data. To solve these issues, safer update, delete, and append methods are required⁽⁴⁹⁾.

Secure multi-party computation is crucial in collaborative cloud settings. It involves creating rules that allow many persons to compute a function over their inputs while keeping them hidden. This strategy is ideal for cloud environments where numerous parties exchange data and computing tools⁽⁵⁰⁾. Privacy and security of cloud data are crucial. For confidentiality, searchable encryption lets users seek encrypted cloud data without knowing what's inside⁽⁵¹⁾. Cloud trust management systems are growing in popularity. These technologies evaluate cloud service reliability so users may make sensible data-sharing and storage decisions. Cloud environments are safer when data management is trusted⁽⁵²⁾. Effective cloud cryptographic key management is another interest. Key distribution, storage, and revocation must be secure to prevent theft⁽⁵³⁾.

Proxy re-encryption is a new, complex technology gaining popularity. It permits protected data to be switched encryption keys without revealing its content. This strategy is ideal for secure data sharing⁽⁵⁴⁾. In addition to these specialist technologies,

(47) C. Wang et al., "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems* 22, no. 5 (2010): 847–859.

(48) Z. N. J. Peterson, M. Gondree, and R. Beverly, "A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud," in *Proceedings of the 3rd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud '11)* (2011).

(49) C. Wang et al., "Ensuring Data Storage Security in Cloud Computing," in *2009 17th International Workshop on Quality of Service* (2009): 1–9.

(50) Y. Li et al., "Intelligent Cryptography Approach for Secure Distributed Big Data Storage in Cloud Computing," *Information Sciences* 387 (2017): 103–115.

(51) R. Li et al., "Efficient Multi-Keyword Ranked Query over Encrypted Data in Cloud Computing," *Future Generation Computer Systems* 30 (2014): 179–190.

(52) Z. Yan et al., "Flexible Data Access Control Based on Trust and Reputation in Cloud Computing," *IEEE Transactions on Cloud Computing* 5, no. 3 (2015): 485–498.

(53) S. K. Sood, "A Combined Approach to Ensure Data Security in Cloud Computing," *Journal of Network and Computer Applications* 35, no. 6 (2012): 1831–1838.

(54) C. Esposito, A. Castiglione, and K. K. R. Choo, "Encryption-Based Solution for Data Sovereignty in Federated

the cloud security architecture is crucial. Safe cloud architectures require systems that handle data breaches, unauthorised access, and other cyber threats⁽⁵⁵⁾. Due to foreign data protection laws, cloud data management is more complex. Like the GDPR, these laws restrict data handling, processing, and storage. To comply with these laws, cloud providers must adapt their operations⁽⁵⁶⁾. Many things can go wrong when trying to secure cloud data. This includes addressing data leaks, unauthorised access, and user privacy violations. Several investigations into these threats have led to ways to protect data and privacy in untrustworthy cloud settings⁽⁵⁷⁾.

New technologies like flexible multi-keyword query techniques may solve current issues. These methods consider keyword weights and user access records when querying. This improves encrypted cloud data searching⁽⁵⁸⁾. Cloud computing security involves legal and moral issues. Building cloud service trust requires considering these concerns. Secure and private cloud data is crucial for cloud computing and associated technologies⁽⁵⁹⁾. Virtual product development could benefit from a new data ownership model that makes sharing and storage safer. This paradigm displays where distributed and preserved design data is and allows data owners to regulate access⁽⁶⁰⁾. Data safety in cloud computing depends on numerous factors, including where data is held and enterprises' and service providers' legal requirements. Research⁽⁶¹⁾ recommend explicit policy and governance frameworks for good cloud security. To conclude, cloud computing data privacy technologies are numerous. Encryption, data localisation, safe data storage, trust management, key management, and legal compliance is complex. Each aspect is crucial for cloud data security, privacy, and control.

2.5. Best Practices and Solutions

Global best practices ensure cloud data security and compliance with local laws. For Qatar, prioritizing digital transformation and data governance, adopting these

Clouds,” IEEE Cloud Computing 3, no. 1 (2016): 12–17.

(55) Y. Sun et al., “Data Security and Privacy in Cloud Computing,” International Journal of Distributed Sensor Networks 10, no. 7 (2014): 190903.

(56) C. Banse, “Data Sovereignty in the Cloud—Wishful Thinking or Reality?” in Proceedings of the 2021 on Cloud Computing Security Workshop (2021): 153–154.

(57) J. Tang et al., “Ensuring Security and Privacy Preservation for Cloud Data Services,” ACM Computing Surveys (CSUR) 49, no. 1 (2016): 1–39.

(58) K. Singi et al., “Data Sovereignty Governance Framework,” in Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops (2020): 303–306.

(59) D. Zissis and D. Lekkas, “Addressing Cloud Computing Security Issues,” Future Generation Computer Systems 28, no. 3 (2012): 583–592.

(60) T. Giese and R. Anderl, “Maintaining Control over Distributed Data through a Data Sovereignty Model,” in 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA) (2022): 1–7.

(61) S. Medawar, “Information Retrieval in Systematic Reviews: Challenges and Opportunities,” Information Processing & Management 58, no. 1 (2021): 102389.

practices, including clear geolocation rules, is crucial. Peterson et al.⁽⁶²⁾ emphasize knowing data storage locations to meet legal obligations, which is particularly important in Qatar.

Best Practice/Solution	Description	Reference
Data Localization	Storing data within the physical borders of a country to comply with local data protection laws.	Peterson et al., 2011
Encryption Technologies	Using encryption methods to secure data in transit and at rest, including techniques like homomorphic encryption.	Yu, Wang, Ren, & Lou, 2010
Access Control Mechanisms	Implementing strong access control policies, including attribute-based access control (ABAC) and role-based access control (RBAC).	Banse, 2021
Cloud Service Agreements	Ensuring cloud service agreements outline data handling, privacy, and compliance measures.	Wei et al., 2014
Auditing and Compliance Monitoring	Regular audits and monitoring for compliance with data protection laws and standards.	Hashem et al., 2015
Data Masking and Tokenization	Using data masking and tokenisation techniques to anonymise sensitive data.	Giese & Anderl, 2022
Federated Identity Management	Managing user identities and access across different cloud services and platforms.	Harauz et al., 2009
Cloud Data Management Interface (CDMI)	Standardising cloud storage and data management operations through CDMI protocols.	Sookhak et al., 2017
Hybrid Cloud Models	Combining private and public cloud models to optimise control and scalability.	Zissis & Lekkas, 2012
Trust and Reputation Management Systems	It establishes trust and reputation systems for evaluating the reliability of cloud services.	Yan et al., 2017

Table 4. Best Practices & Solutions

Implementing data governance, access, and usage management in shared data networks is complex, particularly in ensuring data sovereignty. Hellmeier et al.⁽⁶³⁾ highlight the need for clear data ownership and control, essential for Qatar's expanding digital projects. The impact of the EU's GDPR and EUCS on data

(62) Z. N. J. Peterson, M. Gondree, and R. Beverly, "A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud," in Proceedings of the 3rd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud '11) (2011).

(63) M. Hellmeier et al., "Implementing Data Sovereignty: Requirements and Challenges from Practice," in Proceedings of the 18th International Conference on Availability, Reliability and Security (2023): 1–9.

autonomy underscores the importance of integrating robust cloud data control strategies in Qatar⁽⁶⁴⁾. Flexible access controls based on trust and reputation, as suggested by Yan et al.⁽⁶⁵⁾, could enhance data privacy in Qatar's cloud services. Additionally, encryption-based solutions, as discussed by Esposito et al.⁽⁶⁶⁾, are crucial for secure data migration across federated clouds—a key consideration for Qatar's collaboration with international cloud providers.

2.6. Gaps in Current Literature

Despite the wealth of literature on cloud computing and data sovereignty, existing research tends to emphasize technical advancements without fully addressing the socio-political and legal complexities of data management across jurisdictions. Studies like Zissis and Lekkas⁽⁶⁷⁾ and Marston et al.⁽⁶⁸⁾ provide foundational insights into the evolution of cloud computing, but they lack critical engagement with emerging challenges such as data localization and compliance in rapidly digitizing economies like Qatar. While Banse⁽⁶⁹⁾ discusses the complexities of open cloud ecosystems under the GDPR, there is limited exploration of how non-EU nations like Qatar adapt these frameworks to fit local legal and cultural contexts. Similarly, Giese and Anderl⁽⁷⁰⁾ offer solutions for secure data sharing but fail to address how these approaches can be scaled to governmental applications where data sovereignty is paramount. Furthermore, many referenced studies, including Rehman and Sakr⁽⁷¹⁾ and Irion⁽⁷²⁾, are outdated and fail to account for recent advancements in cloud security technologies, such as AI-driven encryption systems⁽⁷³⁾. This study aims to

(64) C. Banse, "Data Sovereignty in the Cloud—Wishful Thinking or Reality?" in Proceedings of the 2021 on Cloud Computing Security Workshop (2021): 153–154.

(65) Z. Yan et al., "Flexible Data Access Control Based on Trust and Reputation in Cloud Computing," IEEE Transactions on Cloud Computing 5, no. 3 (2015): 485–498.

(66) C. Esposito, A. Castiglione, and K. K. R. Choo, "Encryption-Based Solution for Data Sovereignty in Federated Clouds," IEEE Cloud Computing 3, no. 1 (2016): 12–17.

(67) D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Generation Computer Systems 28, no. 3 (2012): 583–592.

(68) S. Marston et al., "Cloud Computing—The Business Perspective," Decision Support Systems 51, no. 1 (2011): 176–189.

(69) C. Banse, "Data Sovereignty in the Cloud—Wishful Thinking or Reality?" in Proceedings of the 2021 on Cloud Computing Security Workshop (2021): 153–154.

(70) T. Giese and R. Anderl, "Maintaining Control over Distributed Data through a Data Sovereignty Model," in 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA) (2022): 1–7.

(71) M. S. Rehman and M. F. Sakr, "Teaching the Cloud: Experiences in Designing and Teaching an Undergraduate-Level Course in Cloud Computing at Carnegie Mellon University in Qatar," in 2011 IEEE Global Engineering Education Conference (EDUCON) (2011): 875–879.

(72) K. Irion, "Government Cloud Computing and National Data Sovereignty," Policy & Internet 4, no. 3-4 (2012): 40–71.

(73) C. Esposito, A. Castiglione, and K. K. R. Choo, "Encryption-Based Solution for Data Sovereignty in Federated Clouds," IEEE Cloud Computing 3, no. 1 (2016): 12–17.

fill these gaps by providing a nuanced understanding of cloud computing in the Qatari public sector, focusing on leadership's role in ensuring both technological innovation and regulatory compliance.

3. Methodology

Information security is crucial in Qatar's ever-changing digital environment⁽⁷⁴⁾. This paper examines Qatar's legislative and technological criteria for moving from public to autonomous cloud infrastructure. As indicated by earlier research, it places data sovereignty in its proper place in Qatar and stresses its importance during a broad digitisation period.

3.1. Theoretical Framework

This study applies the Data Governance Framework and Technological Determinism to explore Qatar's cloud data sovereignty. Smith and Marx's (1994, 12) concept of Technological Determinism explains how technological advancements drive societal change, impacting government operations and data security in Qatar's IT sector.

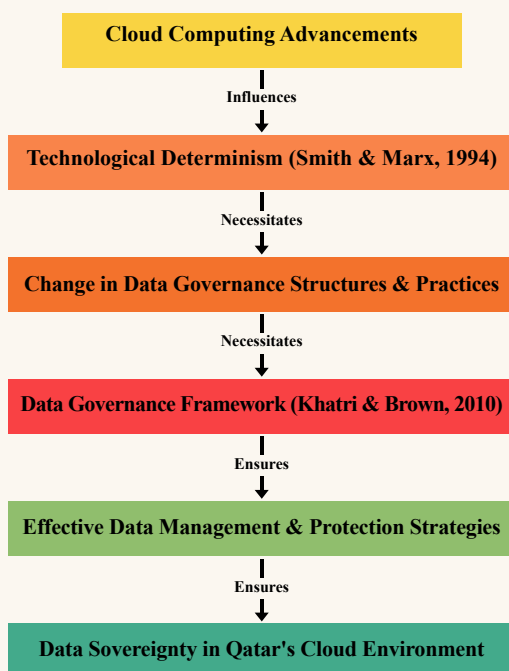


Figure 1: Theoretical Framework (Self-Created)

(74) K. Scarfone and P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS) (National Institute of Standards and Technology, 2007).

The Khatri and Brown (2010, 23) Data Governance Framework provides a practical view of data management tools and procedures. Data security, usability, and correctness require robust rules, norms, and processes in the cloud's dynamic and growing environment. Qataris must grasp these governance regimes to establish, contest, or reinterpret data sovereignty as more people use cloud platforms. This paper uses these theoretical approaches to analyse how technology and governance affect Qatar's cloud data privacy. Technological Determinism explains how cloud advancements change and the Data Governance Framework evaluates data sovereignty. This paper examines how Qatar might use and govern cloud computing. Data governance, new technology, and legal frameworks are analysed from two angles. Qatar and the world need multidimensional research on cloud computing⁽⁷⁵⁾. This article addresses government, nationalism, and safety challenges many countries have with cloud computers. Independent state conflicts complicate problems. Abraham et al. (2019, 45) state that the research's findings and implications globally affect business and academic personnel. Looking at data governance and technology change together shows their cross-border connections.

3.2. Interviews

This paper explores how legislation and technology impact cloud computing in Qatar through structured interviews with key government, corporate, and academic figures. Insights from these interviews were analysed using Braun and Clarke's⁽⁷⁶⁾ thematic analysis, revealing critical data patterns and scholarly concepts. The research adhered strictly to Institutional Review Board (IRB) guidelines, ensuring ethical integrity. Informed consent, confidentiality, and participant protection were prioritized throughout the study, ensuring that the research was conducted with the highest ethical standards at Hamad Bin Khalifa University (HBKU).

3.2.1. Participant Selection

This paper used purposeful sampling to gather diverse perspectives on Qatari cloud computing, focusing on the complexities of data governance and policy. Participants were selected based on their senior positions, expertise in IT, data governance, and policy-making, ensuring informed insights into data sovereignty. The sample included professionals with extensive experience in cloud data governance, recognized thought leaders contributing to the field, and individuals from government, academia, tech, and cybersecurity sectors. This approach aimed

(75) P. Albrecht, "How the General Data Protection Regulation Will Change Our World," *Journal of Privacy and Data Protection* 2, no. 2 (2016): 84–90.

(76) V. Braun and V. Clarke, "Using Thematic Analysis in Psychology," *Qualitative Research in Psychology* 3, no. 2 (2006): 77–101.

to provide a comprehensive and balanced understanding of the technological, regulatory, and governance challenges impacting data sovereignty in Qatar.

3.2.2. Data Collection

This paper involved semi-structured interviews with six experts in cloud computing, law, and data management in Qatar. Participants included two cloud professionals, two academic experts, one cloud service provider expert, and one security specialist. Ethical considerations ensured privacy, fostering open discussions crucial for obtaining valuable qualitative data.

Interviewee ID	Role/Position
Interviewee 1	Director in a security Agency and responsible for privacy
Interviewee 2	Assistant Undersecretary in the government, responsible for bringing the cloud to Qatar
Interviewee 3	Director of Cloud Computing in Qatar
Interviewee 4	Associate Professor and Associate Dean for Academic Affairs
Interviewee 5	Associate Professor and Head of Information and Computing Technology
Interviewee 6	Advisor for Microsoft and Google cloud service providers in Qatar

Table 5. Participants' Information

3.3. Literature Search Strategy

For the literature search, Scopus and Google Scholar were utilized due to their comprehensive coverage of cloud computing and data sovereignty research. Scopus provided peer-reviewed academic papers with a focus on abstracts, titles, and keywords, while Google Scholar included broader sources such as government reports and think tank publications. Search terms like "Data Sovereignty," "Cloud Computing," "Qatar," and "Legislation" targeted the study's focus on Qatar's cloud infrastructure. The review spanned publications from 2010 to 2023, ensuring a thorough examination of both historical and recent developments in the field.

Criteria Type	Criteria	Description
Inclusion	Peer-Reviewed Sources	Focus on peer-reviewed sources to ensure reliability and accuracy
Inclusion	Relevant Case Studies and National Legislation	Case studies and relevant national legislation should be included for a comprehensive examination
Inclusion	Publication Date Range ((2010-2023	It is limited to publications from 2010 to 2023 to capture recent advancements
Exclusion	Non-Peer-Reviewed and Biased Sources	Exclusion of sources lacking peer review or exhibiting potential bias
Exclusion	Irrelevant or Redundant Entries	Remove duplicates and entries unrelated to the research questions

Table 6: Inclusion & Exclusion Criteria

The literature review began with 950 sources, narrowed to 341 after removing duplicates and irrelevant entries. After further screening, 129 papers required closer examination, with only 15 meeting the critical criteria for the systematic review. This meticulous selection process ensured the inclusion of high-quality, relevant studies focused on Qatar's cloud computing data privacy.

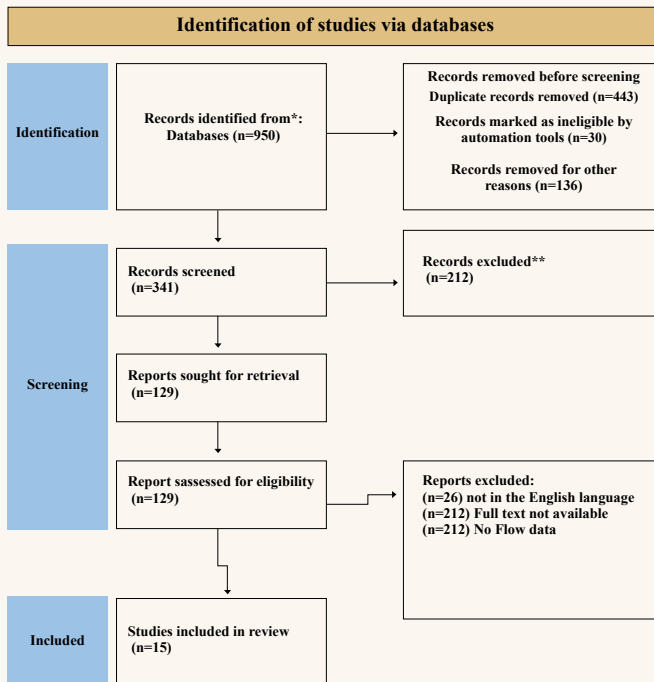


Figure 2: PRISMA Flow Chart

This paper selected 15 diverse pieces of literature to explore Qatari data sovereignty, addressing legal, scientific, and business challenges and opportunities⁽⁷⁷⁾. The careful selection ensured a comprehensive analysis, focusing on Qatar's regulatory challenges and using Qatar-specific data for relevant insights into the nation's cloud infrastructure upgrades⁽⁷⁸⁾. In this paper, a comprehensive examination of Qatar's legal landscape, technical challenges, and benefits of adopting a sovereign cloud model was conducted. The study focused on understanding Qatar's data sovereignty legislative frameworks, particularly the Qatar Financial Centre Data Security Regulations 2021 and the Qatar Personal Data Protection Law (PDPPL). Additionally, it assessed the technical aspects of implementing a sovereign cloud model in Qatar, analyzing technological limitations and advantages. This paper acknowledges its limitations, primarily the exclusive use of Google Scholar and Scopus, potentially limiting source diversity on data sovereignty in Qatar⁽⁷⁹⁾. The focus on peer-reviewed articles from 2010-2023 may introduce publication bias⁽⁸⁰⁾, and the small selection of 15 studies could affect comprehensiveness⁽⁸¹⁾. The emphasis on Qatari issues may limit broader applicability⁽⁸²⁾. Addressing these limitations would enhance the study's robustness and provide a more comprehensive analysis of data sovereignty in Qatar's evolving digital landscape.

4. Results and Findings

4.1. Findings from Existing Review

Integration of Cloud Computing with National Vision and Sustainability Initiatives

Elidrisy⁽⁸³⁾ noted that cloud computing in Qatar's national strategies and environmental programs supports QNV2030. This plan promotes a knowledge-based economy with cloud computing for Msheireb Downtown Doha and the Qatar Free

(77) A. Kasiwi, M. Ikeda, and D. Anderson, "Rethinking Data Sovereignty in Cloud Computing," *Journal of Data Sovereignty* 15, no. 1 (2022): 142–155.

(78) I. Calzada, *Data Sovereignty in the Age of Big Tech: Political Geographies of Data and Challenges of Decentralized Alternatives* (Oxford University Press, 2021).

(79) S. Medawar, "Information Retrieval in Systematic Reviews: Challenges and Opportunities," *Information Processing & Management* 58, no. 1 (2021): 102389.

(80) J. Harris et al., "How Stakeholder Participation Can Contribute to Systematic Reviews of Complex Interventions," *Journal of Epidemiology and Community Health* 70, no. 2 (2014): 207–214.

(81) A. Kasiwi, M. Ikeda, and D. Anderson, "Rethinking Data Sovereignty in Cloud Computing," *Journal of Data Sovereignty* 15, no. 1 (2022): 142–155.

(82) C. Okoli, "A Guide to Conducting a Standalone Systematic Literature Review," *Communications of the Association for Information Systems* 37, no. 1 (2015): 879–910.

(83) A. Elidrisy, "Leveraging Cloud Services & Digital Transformation for Sustainability: Insights from Cases of Qatar," *Journal of Innovative Research* 2, no. 1 (2024): 20–28.

Zone. The QFZ, a crucial project, shows how cloud technology and economic growth may work together by encouraging corporate growth and innovation. This initiative supports sustainable development goals such as Decent Work and Economic Growth (SDG 8), Industry, Innovation, and Infrastructure (SDG 9), and Sustainable Cities and Communities (SDG 11). Since it uses the cloud, this alignment represents a paradigm change toward an eco-friendlier and more sustainable city lifestyle, which aligns with SDG 13: Climate Action and other global environmental challenges.

Legal Frameworks and Privacy Concerns in Cloud Computing

Al-Sharim's 2021 analysis details Qatar's complex cloud computing rules, focusing on privacy and data security rules. The analysis reveals how difficult it is for Qatar to keep cloud data private because cloud services are utilised worldwide, and the USA PATRIOT Act applies to numerous countries. This issue is crucial to data sovereignty since international rules may trump local ones. People in other countries can access cloud data. Data sovereignty in Qatar requires robust, clear, and enforceable regulations to protect cloud data from unauthorized access and ensure compliance with international standards. While Qatar has made strides in developing its digital data laws, gaps remain, particularly regarding international legal challenges. These jurisdictional issues complicate Qatar's data sovereignty goals, potentially undermining national laws. The paper highlights Qatar's proactive adoption of cloud technology to support its national vision and environmental goals, while also addressing the legal complexities of data privacy and authority. This analysis underscores the intricate balance between technological advancement and legal challenges in achieving Qatar's ambitions.

Impact of Cloud Computing on the Financial Sector and Data Security in Qatar:

Najafi et al.⁽⁸⁴⁾ found FinTech growing in Qatar. Cloud computing is crucial to changing the finance industry. Qatar's FinTech activities heavily rely on banking services, so this development is vital. Cloud computing simplifies and improves financial services, improving banking and payment services. It's not simple with this shift. The report raises concerns about financial transaction data laws and security hazards. With the government's financial and legal support, this fast growth illustrates that leveraging cloud technology for financial improvement is a plan.

(84) B. Najafi, M. Amra, and A. Najafi, "Exploring Global Fintech Advancement and Application: Case of Saudi Arabia, Turkey, and Qatar," in Exploring Global FinTech Advancement and Applications (IGI Global, 2024): 158–211.

Healthcare Sector's Adoption of Cloud Computing in Qatar:

Al-Qahtani and Abu-Shanab⁽⁸⁵⁾ research on cloud computing in Qatar's health business illustrates how it has revolutionised care. According to the report, cloud computing saves resources; thus, more healthcare organisations are using it. The study found that trust, compliance concerns, economic and operational benefits, and functional benefits most affect user happiness. The study also recommends fixing private cloud management and risk issues. Data sovereignty issues arise when healthcare uses the cloud, especially when protecting sensitive health data. Cloud technology in healthcare must be fast, safe, and compliant. A comprehensive examination of cloud healthcare demonstrates that cloud technology can enhance Qatari healthcare but potentially threaten data privacy and sovereignty.

Legal and Regulatory Challenges in Cloud Computing:

Qatar requires cloud computing regulations because they are new. Al-Sharim's 2021 assessment of Qatar's cloud privacy challenges found that cloud data standards are failing. The report dislikes Qatar's cloud computing and privacy laws. It demands more vital cloud data ownership and use rules. This topic impacts cloud software safety and international use. Qatar must amend its cloud computer legislation like many others. This adjustment is needed to maximise cloud computing without compromising data security and privacy. Data privacy and laws governing cloud data storage, processing, and sending are the focus of this theme. Qatar should implement Al-Sharim's advice to fix cloud computer issues immediately. There are privacy, data security, and international law rules. How law and technology interact is crucial to this issue. Qatar needs rigorous data protection standards for industry and society to adopt cloud computing. Qatar must demonstrate safe and honest cloud computing to create trust in cloud technology.

Cloud Computing's Role in Enhancing National Economies and Sustainable Development

The impact of cloud computing on national economies and sustainable development is profound and multifaceted. In their study, Hashem et al.⁽⁸⁶⁾ delve into the exponential growth of big data driven by cloud computing. They underscore the crucial need for substantial computational infrastructure to manage this burgeoning volume

(85) F. Al-Qahtani and E. A. Abu-Shanab, "End User Satisfaction with Cloud Computing: The Case of Hamad Medical Corporation in Qatar," *International Journal of Healthcare Information Systems and Informatics* 16, no. 4 (2021): 1–23

(86) I. A. T. Hashem et al., "The Rise of 'Big Data' on Cloud Computing: Review and Open Research Issues," *Information Systems* 47 (2015): 98–115.

of data effectively. This aspect is particularly pertinent for economies like Qatar, which are in the process of diversifying and digitalizing. The robust computational capabilities offered by cloud computing can significantly bolster Qatar's initiatives in sectors such as healthcare, education, and smart city development, aligning with the country's National Vision 2030. Giese and Anderl⁽⁸⁷⁾ highlight the challenge of controlling distributed data in global collaborations, a key concern for Qatar's international partnerships in technology and education. Ensuring data sovereignty is crucial for protecting Qatar's economic development and sustainability.

The Interplay between Cloud Computing, Data Sovereignty, and Regulatory Compliance

The equilibrium between cloud computing, data sovereignty, and regulatory compliance is critical for countries like Qatar. Blancato (2023, 251) investigates the European Union's strategy in managing cloud data migration and reducing reliance on non-EU cloud service providers. This analysis is relevant to Qatar, offering insights into how a region can maintain data sovereignty while leveraging global cloud computing services. The study implies that for Qatar, aligning cloud strategies with national interests and security concerns is as vital as ensuring technical efficiency. Banse⁽⁸⁸⁾ addresses the intricate concept of data sovereignty in the cloud, unravelling the technical and regulatory complexities entwined in this sphere. This research is particularly pertinent to Qatar, as it navigates its cloud computing strategy amidst an evolving international legal landscape.

Technological Innovations and Challenges in Ensuring Data Sovereignty in the Cloud

Technological innovations and challenges play a significant role in ensuring data sovereignty in the cloud, a topic critical for Qatar's digital strategy. Yang et al.⁽⁸⁹⁾ focus on the key issues of data security and privacy protection within the cloud environment. This area is of paramount importance for Qatar as it advances its cloud computing capabilities. The study provides insights into various security measures and privacy protection strategies, essential for Qatar to maintain data integrity and sovereignty. Research⁽⁹⁰⁾ contribute to this discussion by examining big data processing techniques in cloud computing environments. Their research offers Qatar perspectives on managing the challenges associated with big data in the cloud. This is particularly relevant as Qatar continues to grow its digital infrastructure and services, generating and processing large volumes of data.

(87) T. Giese and R. Anderl, "Maintaining Control over Distributed Data through a Data Sovereignty Model," in 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA) (2022): 1–7.

(88) C. Banse, "Data Sovereignty in the Cloud—Wishful Thinking or Reality?" in Proceedings of the 2021 on Cloud Computing Security Workshop (2021): 153–154.

(89) H. Yang and M. Tate, "A Descriptive Literature Review and Classification of Cloud Computing Research," Communications of the Association for Information Systems 31, no. 1 (2012): 2–57.

(90) C. Kuner, "An International Legal Framework for Data Protection: Issues and Prospects," Computer Law & Security Review 25, no. 4 (2009): 307–317.

4.2. Analysis of Interviews

For this paper, experts, policymakers, and researchers discussed cloud computing and data sovereignty in Qatar. Interviews were aimed at eliciting deep, deliberate responses, and recordings were examined for central themes. Significant priorities include Data Sovereignty, Geographic Localization, Regulatory Compliance, and Legal Framework.

4.2.1. Data Sovereignty and Geographical Localization

Data sovereignty and regional localization highlight the challenges of data governance in specific regions. Participants emphasized the importance of storing data within Qatar or under an EU regional agreement, ensuring compliance with local laws. Geographic localization is crucial for data security and aligning with legal requirements, especially where national laws strictly govern privacy and security. "Keeping data within national borders is essential for sovereignty," an interviewee noted. This underscores the legal and regulatory power over data location. Geographical localization offers control but faces limitations in a global digital environment where data crosses borders, complicating efforts to maintain control over cloud software. The interviews revealed the complexities of cloud computing laws, particularly how Qatar's evolving policies intersect with foreign legislation like the USA PATRIOT Act and CLOUD Act. Balancing local and international laws is critical for Qatar's secure data management amid its digital transformation.

4.2.2. Public vs. Private Cloud Considerations

This theme examines the impact of private versus public cloud infrastructures on Qatari data ownership, security, and control. People indicated that cloud options meet different data security and ownership concerns. "Private clouds offer greater control and security, which fits well with the needs of sensitive government data," said a tech. They cost more and grow slower than public clouds. Private clouds give more control and safety but may be less scalable and cost-effective than public clouds. However, public clouds, hosted by outside companies, are flexible and cheap but create privacy and security concerns. "Public clouds are shared environments where data is stored off-premises," a government expert stated. "This brings up questions about jurisdictional control and access." This raises concerns that public cloud data may be subject to the cloud provider's country laws. The theme compares public and private clouds under Qatar's unique security and regulation framework. It suggests we need a balanced, possibly hybrid, approach to optimise sovereignty and operational efficiency.

4.2.3. Cloud Security and Privacy Concerns

Cybersecurity issues, including data protection and encryption, were discussed. The goal was to strike a balance between security and cloud vulnerability. "Cloud computing has many benefits but complex security issues," said a scholar. Increased encryption and monitoring are needed to prevent data leaks. This comment shows how hard it is to manage cloud security with evolving threats. Participants explored the delicate privacy-accessibility balance. A privacy expert said, "Encryption and strict access controls are necessary, but they shouldn't get in the way of the user experience or make cloud services less useful." Users and providers struggle to balance security and usability in the cloud.

4.2.4. Vendor Lock-in and Flexibility in Cloud Services

According to interviews, Qatar's cloud service alternatives and flexibility are hampered by vendor lock-in. Managing hazards and having various cloud providers were discussed. Expert said: "It's hard to avoid vendor lock-in." Comparing services and ensuring compatibility is necessary for cloud migration. You must carefully select providers so you can switch, and no seller has too much power or authority. An expert noted as well, "Having multiple cloud providers in Qatar prevents vendor lock-in and encourages competition, which leads to better services and new ideas." This principle suggests multiple providers create a healthy, competitive market that rewards customers with better service and new ideas. Interviews revealed that cost is the primary barrier to cloud adoption in Qatar. Participants discussed cost reduction, scalability, and resource management, emphasizing that the potential savings and efficient resource use drive cloud service adoption. An academic noted, "Scalability is a key economic factor," allowing businesses to adjust resources without heavy infrastructure investment. However, concerns about provider lock-in and economic factors impact strategic cloud decisions. Qatar's decision-makers must balance efficiency, scalability, cost, and vendor relationships to ensure successful cloud computing implementation, reflecting the nuanced challenges of cloud utilization in the region. Interviews also highlighted the importance of disaster recovery and business continuity in Qatari cloud operations. Companies moving to the cloud are concerned about data security and redundancy. One expert emphasized, "Strong disaster recovery solutions drove our cloud adoption." Cloud services enable business continuity during crises, with redundancy ensuring smooth operations. This underscores the need for comprehensive disaster recovery plans beyond data backup. The interviews stressed the importance of collaboration and communication with cloud providers. Experts noted that strong provider relationships enhance service delivery, problem-solving, and goal alignment, which are crucial for successful cloud adoption in Qatar.

4.3. Integration of Interview and Literature Review Findings

The paper's literature review and interviews offer diverse perspectives on Qatari data sovereignty and cloud computing, highlighting key areas of agreement and divergence. The focus on data control and legal compliance reflects significant progress. Both Elidrisy⁽⁹¹⁾ and Al-Sharim⁽⁹²⁾ align with interviewees on stringent data governance practices, emphasizing the importance of adhering to local and international laws. Concerns about compliance with foreign legislation like the USA PATRIOT Act and the CLOUD Act underscore the complexities of data sovereignty in a global context. Security perceptions varied, with Alsalemi et al.⁽⁹³⁾ providing a strong data classification framework, though interviewees expressed differing levels of trust in cloud security. This suggests a disconnection between academic research and real-world cloud security concerns. There is growing consensus on the benefits of private cloud systems, with Najafi et al.⁽⁹⁴⁾ and interviewees agreeing on enhanced security and control. However, vendor lock-in concerns, raised in interviews, are underexplored in literature, indicating a research gap. Interviewees provided deeper insights into disaster management and cloud operations, suggesting the need for more targeted research. The interviews contribute valuable, unique data, enhancing the understanding of cloud computing challenges in Qatar. Qatar's cloud computing landscape ties data sovereignty to advanced technologies. Robust encryption, like Attribute-Based Encryption (ABE), offers refined access control but faces practical challenges due to its complexity. Homomorphic encryption enhances privacy, especially in sensitive sectors, but its computational demands are a hurdle. Data localization aligns with national laws but may limit global interoperability. Balancing these technologies with practical cloud realities is crucial for Qatar's digital ambitions.

4.4. Discussion of Key Findings

Al-Thani et al. (2020) explore the intricate interplay between Qatar's rapid technological advancements in cloud computing and its evolving social norms and group demands. Their study highlights the delicate balance between embracing cloud technology and preserving societal values, crucial in addressing Qatar's cloud

(91) A. Elidrisy, "Leveraging Cloud Services & Digital Transformation for Sustainability: Insights from Cases of Qatar," *Journal of Innovative Research* 2, no. 1 (2024): 20–28.

(92) H. A. Al-Sharim, "The Privacy in the Cloud: An Examination of the Law in Qatar" (PhD diss., Hamad Bin Khalifa University, 2021).

(93) A. Alsalemi et al., "Cloud Energy Micro-Moment Data Classification: A Platform Study," in 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC) (2020): 420–425.

(94) B. Najafi, M. Amra, and A. Najafi, "Exploring Global Fintech Advancement and Application: Case of Saudi Arabia, Turkey, and Qatar," in *Exploring Global FinTech Advancement and Applications* (IGI Global, 2024): 158–211.

data protection challenges. A key finding emphasizes the importance of aligning cloud strategies with national and international laws, as compliance is vital for data security. Interviewees, including Elidrisy⁽⁹⁵⁾ and Interviewee 4, stress the need to understand extraterritorial laws like the USA PATRIOT Act and CLOUD Act, which may threaten data sovereignty. Balancing cloud security with user privacy is another critical issue, with scholars like Alsalemi et al.⁽⁹⁶⁾ and Zubair et al.⁽⁹⁷⁾ noting the complexities of implementing robust encryption while safeguarding privacy. The choice between public and private cloud systems also impacts data security, particularly in Qatar's context, where privacy and control are paramount. Finally, the issue of vendor lock-in raises concerns for Qatari businesses, highlighting the need for strategies that ensure flexibility and competitive cloud service options. Understanding these dynamics is essential for Qatar's cloud computing strategies, which aim to foster economic growth and innovation while maintaining security and privacy.

5. Discussion and Recommendations

5.1. Discussion

This section addresses cloud environment issues in Qatar and globally, focusing on key findings and their relevance to cloud data security. It explores Qatar's complex data privacy policy, shaped by evolving legislation, technologies, and political factors, and highlights the challenges of balancing local and international laws, such as the USA PATRIOT Act and CLOUD Act. Public clouds offer cost savings but raise security concerns, while private clouds align with Qatar's sovereignty standards, offering greater control. Qatar's approach to cloud data management, emphasizing flexibility and multiple providers, mirrors global trends, underscoring the need for ongoing research in this evolving field.

5.2. Recommendations

This paper enhances cloud computing and data security theories, focusing on Qatar's unique context. It highlights the complex interplay between technology, law, and geopolitics, revealing gaps in existing models. The study integrates international laws, like the CLOUD Act, with local regulations, recommending adaptable legal

(95) A. Elidrisy, "Leveraging Cloud Services & Digital Transformation for Sustainability: Insights from Cases of Qatar," *Journal of Innovative Research* 2, no. 1 (2024): 20–28.

(96) A. Alsalemi et al., "Cloud Energy Micro-Moment Data Classification: A Platform Study," in 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC) (2020): 420–425.

(97) M. Zubair et al., "Cybersecurity for Next-Generation Healthcare in Qatar," *Journal of Emergency Medicine, Trauma & Acute Care, Qatar Health 2020 Conference* 2021, no. 2 (2021): 41.

frameworks and urging cloud providers to comply with local laws. This paper recommends data accessibility rules to protect national security and privacy, ensuring cloud data meets standards. It suggests bilateral agreements with cloud server countries to give Qatar legal authority over foreign data and urges cloud providers to invest in security while adhering to Qatari laws. The paper advises creating Qatar-specific cloud options for greater control and emphasizes the importance of regular audits to ensure compliance with evolving data security laws. It also calls for more research on international cloud data sovereignty regulations, especially for small countries like Qatar, highlighting the challenges of balancing innovation with strict data management.

5.3. Theoretical Implications

To strengthen the discussion of theoretical and practical implications, this study's findings can be linked explicitly to leadership and data sovereignty theories. Theoretically, this research contributes to transformational leadership theory by demonstrating how leadership styles significantly influence the successful adoption of cloud computing in the public sector. It highlights how leaders with strategic foresight, risk management skills, and collaborative approaches can drive digital transformation, particularly in complex environments like Qatar. Additionally, the study extends data sovereignty theory by exploring how local legal frameworks interact with global cloud computing standards, offering new insights into the balance between national security concerns and international data-sharing requirements.

For practical implications, the study provides actionable recommendations for policymakers and public sector leaders. Specifically, it suggests the need for leadership training focused on managing ICT integration and cloud computing adoption. Additionally, it recommends that policymakers develop clear guidelines on data sovereignty and compliance with international regulations to ensure secure cloud usage. Public sector organizations should also focus on fostering partnerships with global cloud service providers while maintaining compliance with national legal frameworks. By addressing these recommendations, practitioners can better navigate the complex landscape of cloud adoption, data security, and regulatory compliance in the digital age.

6. Conclusion

This paper comprehensively explores cloud data sovereignty in Qatar, offering insights into the complexities of cloud computing within a national context. By integrating literature reviews and interviews, it reveals key themes like data

sovereignty, regulatory compliance, and cloud security. The paper highlights the significance of geographical localization for maintaining data sovereignty and examines the impact of international laws such as the USA PATRIOT Act and the CLOUD Act. It contrasts public and private cloud infrastructures, emphasizing the trade-offs between control, security, cost, and scalability. The study also underscores the importance of disaster recovery, business continuity, and effective collaboration between cloud providers and clients. The paper's findings challenge existing models and theories, providing new perspectives on the interaction between local and international legal frameworks. It offers practical recommendations for policymakers, cloud service providers, and businesses, emphasizing tailored strategies, robust cybersecurity measures, and best practices in data management. Future research directions include exploring emerging technologies and evolving legal landscapes in cloud computing. Overall, this paper contributes valuable insights to the academic field, offers practical guidance for stakeholders, and lays the groundwork for further research in cloud data sovereignty. The findings are relevant not only to Qatar but also to other nations facing similar challenges in cloud computing.

Bibliography

- Abulhussain, F. M. "A Study Evaluating the Readiness Level for Qatar Companies to Adopt Industry 4.0." Master's thesis, 2021.
- Abu-Taieh, E., A. Alfaries, S. Al-Otaibi, and G. Aldehim. "Cybersecurity Crime and Punishment: A Comparative Study of the Laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia." *International Journal of Cyber Warfare and Terrorism* 8, no. 3 (2018): 46-59. <https://doi.org/10.4018/IJCWT.2018070104>.
- Ahmed, R., and J. Campbell. "The Role of Leadership and Governance in Transforming Public Sector Organizations: A Review and Future Research Agenda." *Public Administration Quarterly* 45, no. 3 (2021): 345-375.
- Albrecht, J. P. "How the General Data Protection Regulation Will Change Our World." *Journal of Privacy and Data Protection* 2, no. 2 (2016): 84-90.
- Aldossary, S., and A. Saad. "Cloud Computing Approaches, Characteristics and Cloud Computing Status in the Arab World." *Multi-Knowledge Electronic Comprehensive Journal for Education & Science Publications*, no. 25 (2019): 1-18.
- Ali, H. B. Y., L. M. Abdullah, M. Kartiwi, A. Nordin, N. Salleh, and N. S. A. A. Bakar. "A Systematic Literature Mapping of Extensive Data Risk Analysis in a Cloud Computing Environment." In *Journal of Physics: Conference Series*, vol. 1018, no. 1, p. 012017. IOP Publishing, 2018.

- Almorsy, M., J. Grundy, and I. Müller. "An Analysis of the Cloud Computing Security Problem." *Communications of the ACM* 59, no. 1 (2016): 38-46.
- Al-Naama, M. "Data Sovereignty in the GCC: Legal and Regulatory Perspectives." *Gulf Affairs*, 2022.
- Alnaemi, S. R. "The Gulf Crisis and Rise of Digital Nationalism in Qatar: A Case Study of Tweets." Master's thesis, 2021.
- Al-Qahtani, F., and E. A. Abu-Shanab. "End User Satisfaction with Cloud Computing: The Case of Hamad Medical Corporation in Qatar." *International Journal of Healthcare Information Systems and Informatics* 16, no. 4 (2021): 1-23. <https://doi.org/10.4018/IJHISI.2021100101>.
- Alsalemi, A., A. Al-Kababji, Y. Himeur, F. Bensaali, and A. Amira. "Cloud Energy Micro-Moment Data Classification: A Platform Study." In *2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC)*, 420-425. IEEE, 2020.
- Alshamaila, Y., S. Papagiannidis, and F. Li. "Cloud Computing Adoption by SMEs in the North East of England: A Multi-Perspective Framework." *Journal of Enterprise Information Management* 26, no. 3 (2013): 250-275. <https://doi.org/10.1108/JEIM-09-2012-0054>.
- Al-Sharim, H. A. "The Privacy in the Cloud: An Examination of the Law in Qatar." PhD diss., Hamad Bin Khalifa University, 2021.
- Alshomrani, S., and S. Qamar. "Cloud-Based E-Government: Benefits and Challenges." *International Journal of Multidisciplinary Sciences and Engineering* 4, no. 6 (2013): 1-9.
- Alzadjali, K., and A. Elbanna. "Smart Institutional Intervention in Adopting Digital Infrastructure: The Case of Government Cloud Computing in Oman." *Information Systems Frontiers* 22, no. 2 (2020): 365-380. <https://doi.org/10.1007/s10796-019-09915-7>.
- Baker McKenzie. "Qatar: Data Protection Overview." Baker McKenzie, 2021.
- Banerjee, P. "Governing the Cloud: Policy Strategies for Data Sovereignty and Digital Infrastructure." *Digital Policy, Regulation and Governance* 24, no. 2 (2022): 125-137.
- Bannister, F., and R. Connolly. "ICT, Public Values and Transformative Government: A Framework and Programme for Research." *Government Information Quarterly* 31, no. 1 (2014): 119-128.

- Banse, C. "Data Sovereignty in the Cloud—Wishful Thinking or Reality?" In Proceedings of the 2021 on Cloud Computing Security Workshop, 153-154, November 2021.
- Bass, B. M., and R. E. Riggio. Transformational Leadership. Mahwah, NJ: Lawrence Erlbaum Associates, 2006.
- Bertot, J. C., P. T. Jaeger, and J. M. Grimes. "Using ICTs to Create a Culture of Transparency: E-Government and Social Media as Openness and Anti-Corruption Tools for Societies." Government Information Quarterly 27, no. 3 (2010): 264-271.
- Biočić, B., D. Tomić, and D. Ogrizović. "Economics of Cloud Computing." In 2011 Proceedings of the 34th International Convention MIPRO, 1438-1442. IEEE, May 2011.
- Braun, V., and V. Clarke. "Using Thematic Analysis in Psychology." Qualitative Research in Psychology 3, no. 2 (2006): 77-101. <https://doi.org/10.1191/1478088706qp063oa>.
- ———. "Thematic Analysis." In APA Handbook of Research Methods in Psychology, Vol. 2: Research Designs, edited by H. Cooper, 57-71. APA, 2012.
- Buyya, R., J. Broberg, and A. Goscinski, eds. Cloud Computing: Principles and Paradigms. Wiley, 2018.
- Calzada, I. Data Sovereignty in the Age of Big Tech: Political Geographies of Data and Challenges of Decentralized Alternatives. Oxford University Press, 2021.
- Castleberry, A., and A. Nolen. "Thematic Analysis of Qualitative Research Data: Is It as Easy as It Sounds?" Currents in Pharmacy Teaching and Learning 10, no. 6 (2018): 807-815. <https://doi.org/10.1016/j.cptl.2018.03.019>.
- Celeste, E. "Data Sovereignty and the Cloud: A Board Game with Many Players." Computer Law & Security Review 40 (2021): 105486. <https://doi.org/10.1016/j.clsr.2020.105486>.
- Chakraborty, S., and K. Joseph. ICT and Digital Transformation in the Middle East. Routledge, 2021.
- Chandrasekaran, A., and M. Kapoor. "State of the Public Cloud: The Cloud Adoption Conundrum." Infosys Labs Briefings 9, no. 1 (2011): 3-10.
- Chatterjee, S., N. P. Rana, and Y. K. Dwivedi. "Examining the Role of Transformational Leadership in Cloud Security Management: A Quantitative Study." Information Technology & People 32, no. 6 (2019): 1325-1351.
- Choo, K. K. R. "Legal Issues in the Cloud." IEEE Cloud Computing 1, no. 01 (2014): 94-96.

- Clohessy, T., T. Acton, and L. Morgan. "Smart City as a Service (SCaaS): A Future Roadmap for E-Government Smart City Cloud Computing Initiatives." *Digital Policy, Regulation and Governance* 19, no. 1 (2017): 58-69.
- Connett, W., and T. Johnson. "Updating Systematic Reviews: An International Survey." *PLoS ONE* 8, no. 7 (2013): e67145. <https://doi.org/10.1371/journal.pone.0067145>.
- Cordella, A., and N. Tempini. "E-Government and Organizational Change: Reappraising the Role of ICT and Bureaucracy in Public Service Delivery." *Government Information Quarterly* 32, no. 3 (2015): 279-286.
- Cortellazzo, L., E. Bruni, and R. Zampieri. "The Role of Leadership in a Digitalized World: A Review." *Frontiers in Psychology* 10 (2019): 1938. <https://doi.org/10.3389/fpsyg.2019.01938>.
- Creswell, J. W., and J. D. Creswell. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5th ed. SAGE Publications, 2017.
- Creswell, J. W., and C. N. Poth. *Qualitative Inquiry and Research Design: Choosing among Five Approaches*. 4th ed. SAGE Publications, 2017.
- De Hert, P., and V. Papakonstantinou. "Three Scenarios for International Data Privacy Governance: Towards a Global Data Privacy Organization, Preferably a UN Agency." *ISJLP* 9 (2013): 271-300.
- Eaton, C. "Platform as a Service (PaaS)." *Gartner IT Glossary*, 2010. <https://www.gartner.com/en/information-technology/glossary/platform-as-a-service-paas>.
- Elidrisy, A. "Leveraging Cloud Services & Digital Transformation for Sustainability: Insights from Cases of Qatar." *Journal of Innovative Research* 2, no. 1 (2024): 20-28.
- Esposito, C., A. Castiglione, and K. K. R. Choo. "Encryption-Based Solution for Data Sovereignty in Federated Clouds." *IEEE Cloud Computing* 3, no. 1 (2016): 12-17.
- Finlay, L. "Negotiating the Swamp: The Opportunity and Challenge of Reflexivity in Research Practice." *Qualitative Research* 2, no. 2 (2002): 209-230.
- Garrison, G., R. L. Wakefield, and S. Kim. "The Effects of IT Capabilities and Delivery Model on Cloud Computing Success and Firm Performance for Cloud-Supported Processes and Operations." *International Journal of Information Management* 35, no. 4 (2015): 377-393.
- GCC-STAT. *GCC Statistical Centre: Data Sovereignty and Cloud Computing*. GCC-STAT, 2022.

- Giese, T., and R. Anderl. "Maintaining Control over Distributed Data through a Data Sovereignty Model." In 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA), 1-7, November 2022.
- Gil-Garcia, J. R., N. Helbig, and A. Ojo. "Being Smart: Emerging Technologies and Innovation in the Public Sector." *Government Information Quarterly* 31, no. S1 (2014): S2-S8.
- Gong, Y., X. Hu, and H. Liu. "Leadership Styles, Team Dynamics, and Information Technology Service Innovation: Evidence from the Chinese Public Sector." *Journal of Public Administration Research and Theory* 30, no. 1 (2020): 47-66.
- Hairi, N. A. "World Reaction and the Role of Turkiye, Iran, and Asian Countries in Maintaining Qatar Sovereignty: A Case Study of Gulf Crisis." *Sains Insani* 8, no. 2 (2023): 168-173.
- Harris, J., L. Croot, J. Thompson, and J. Springett. "How Stakeholder Participation Can Contribute to Systematic Reviews of Complex Interventions." *Journal of Epidemiology and Community Health* 70, no. 2 (2014): 207-214.
- Hashem, I. A. T., I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. U. Khan. "The Rise of 'Big Data' on Cloud Computing: Review and Open Research Issues." *Information Systems* 47 (2015): 98-115.
- Hashizume, K., D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez. "An Analysis of Security Issues for Cloud Computing." *Journal of Internet Services and Applications* 4, no. 1 (2013): 1-13.
- Heeks, R., and C. Stanforth. "Technological Change in Developing Countries: Opening the Black Box of Process Using Actor-Network Theory." *Development Studies Research* 2, no. 1 (2015): 33-50.
- Hellmeier, M., J. Pampus, H. Qarawlus, and F. Howar. "Implementing Data Sovereignty: Requirements and Challenges from Practice." In *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 1-9, August 2023.
- Houghton, J. D., A. Carnes, and C. N. Ellison. "A Cross-Sectional Examination of Transformational Leadership and Transformational Leaders in the United States." *Leadership Quarterly* 26, no. 3 (2015): 437-447.
- Huang, Z., and M. Benyoucef. "From E-Commerce to Social Commerce: A Close Look at Design Features." *Electronic Commerce Research and Applications* 12, no. 4 (2015): 246-259.

- Irion, K. "Government Cloud Computing and National Data Sovereignty." *Policy & Internet* 4, no. 3-4 (2012): 40-71.
- Istepanian, R. S. H., S. Hu, N. Y. Philip, and A. Sungoor. "The Potential of Internet of Medical Things (IoMT) for Healthcare Applications." *Journal of Healthcare Engineering* 2, no. 3 (2011): 309-318.
- Janssen, M., E. Estevez, and T. Janowski. "Interoperability in Big, Open, and Linked Data—Organizational Maturity, Capabilities, and Data Portfolios." *Government Information Quarterly* 31, no. 3 (2014): S57-S68.
- Johansson, J., L. Sundberg, and S. Mattsson. "Leadership Styles and Their Influence on Digital Transformation in Public Sector Organizations." *Journal of Public Administration Research and Theory* 31, no. 1 (2021): 125-139.
- Jordan, M. I., and T. M. Mitchell. "Machine Learning: Trends, Perspectives, and Prospects." *Science* 349, no. 6245 (2015): 255-260.
- Kallio, H., A.-M. Pietilä, M. Johnson, and M. Kangasniemi. "Systematic Methodological Review: Developing a Framework for a Qualitative Semi-Structured Interview Guide." *Journal of Advanced Nursing* 72, no. 12 (2016): 2954-2965.
- Kaplan, J., T. Bailey, C. Rezek, and D. O'Halloran. "Cybersecurity: A Necessary Foundation for the Future." McKinsey & Company, 2016. <https://www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-a-necessary-foundation-for-the-future>.
- Kasiwi, A., M. Ikeda, and D. Anderson. "Rethinking Data Sovereignty in Cloud Computing." *Journal of Data Sovereignty* 15, no. 1 (2022): 142-155.
- Kaufman, L. M. "Data Security in the World of Cloud Computing." *IEEE Security & Privacy* 7, no. 4 (2009): 61-64.
- King, N. J., and V. T. Raja. "Protecting the Privacy and Security of Sensitive Customer Data in the Cloud." *Computer Law & Security Review* 28, no. 3 (2012): 308-319.
- KPMG. "Doing Business in Qatar: Investment Opportunities and Challenges." KPMG, 2021.
- Kronabeter, A., and S. Fenz. "Cloud Security and Privacy in the Light of the 2012 EU Data Protection Regulation." In *Cloud Computing: Third International Conference, CloudComp 2012, Vienna, Austria, September 24-26, 2012, Revised Selected Papers* 3, 114-123. Springer International Publishing, 2013.

- Kuner, C., F. H. Cate, C. Millard, and D. J. B. Svantesson. "Data Protection and Privacy Laws in a Nutshell." *Journal of Data Protection & Privacy* 2, no. 1 (2017): 47-61.
- Kuner, C. "An International Legal Framework for Data Protection: Issues and Prospects." *Computer Law & Security Review* 25, no. 4 (2009): 307-317.
- Li, R., Z. Xu, W. Kang, K. C. Yow, and C. Z. Xu. "Efficient Multi-Keyword Ranked Query over Encrypted Data in Cloud Computing." *Future Generation Computer Systems* 30 (2014): 179-190.
- Li, Y., K. Gai, L. Qiu, M. Qiu, and H. Zhao. "Intelligent Cryptography Approach for Secure Distributed Big Data Storage in Cloud Computing." *Information Sciences* 387 (2017): 103-115.
- Marston, S., Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi. "Cloud Computing—The Business Perspective." *Decision Support Systems* 51, no. 1 (2011): 176-189.
- Martin, S., R. Moore, and J. Redshaw. "Public Sector Leadership in the Digital Age: Navigating through Disruption." *Public Administration Review* 79, no. 5 (2019): 687-693.
- Medawar, S. "Information Retrieval in Systematic Reviews: Challenges and Opportunities." *Information Processing & Management* 58, no. 1 (2021): 102389.
- Mell, P., and T. Grance. "The NIST Definition of Cloud Computing." *National Institute of Standards and Technology* 53, no. 6 (2011): 50-51.
- Menezes, A. J., P. C. Van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
- Middleton, A. M. "Data-Intensive Technologies for Cloud Computing." In *Handbook of Cloud Computing*, 83-136. 2010.
- Milford, T., and B. George. "Data Sovereignty and the Cloud: A Board and Executive Officer's Guide." *Journal of Cloud Computing: Advances, Systems and Applications* 8, no. 1 (2020): 1-12.
- Ministry of Transport and Communications. *Qatar Smart Program (TASMU)*. Ministry of Transport and Communications, 2019.
- Mishra, M., I. Arora, P. Singh, and S. Prabhakar. "An Assessment of Cloud Computing: Evolution." *Journal of Cloud Computing: Advances, Systems and Applications*, 2020.

- Najafi, B., M. Amra, and A. Najafi. "Exploring Global Fintech Advancement and Application: Case of Saudi Arabia, Turkey, and Qatar." In *Exploring Global FinTech Advancement and Applications*, 158-211. IGI Global, 2024.
- Nam, T., and T. A. Pardo. "Conceptualizing Smart City with Dimensions of Technology, People, and Institutions." In *Proceedings of the 12th Annual International Conference on Digital Government Research*, 282-291. 2011.
- Nurdiani, I., M. S. Börjesson, and L. Angelis. "A Systematic Mapping Study on the Combination of Agile Software Development and Leadership Styles." *Journal of Systems and Software* 161 (2020): 110459.
- Okoli, C. "A Guide to Conducting a Standalone Systematic Literature Review." *Communications of the Association for Information Systems* 37, no. 1 (2015): 879-910.
- Omran, R. "A Qualitative Analysis of Cloud Computing Adoption Challenges in the Arabian Gulf Region." PhD diss., Colorado Technical University, 2020.
- Pallis, G. "Cloud Computing: The New Frontier of Internet Computing." *IEEE Internet Computing* 14, no. 5 (2010): 70-73.
- Peterson, Z. N. J., M. Gondree, and R. Beverly. "A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud." In *Proceedings of the 3rd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud '11)*. 2011.
- Qatar Cybersecurity Strategy. National Cybersecurity Strategy. Ministry of Transport and Communications, Qatar, 2020.
- Qatar Financial Centre. Personal Data Privacy Protection Law No. 13 of 2016. Qatar Financial Centre, 2020.
- Qatar National Vision 2030. Planning and Statistics Authority. <http://www.psa.gov.qa/en/qnv/Pages/default.aspx>, 2018.
- Qatar National Vision 2030. QNV 2030 Implementation Plan. Ministry of Planning and Statistics, Qatar, 2020.
- Q-CERT. Qatar Computer Emergency Response Team Annual Report. Q-CERT, 2021.
- Rehman, M. S., and M. F. Sakr. "Teaching the Cloud: Experiences in Designing and Teaching an Undergraduate-Level Course in Cloud Computing at Carnegie Mellon University in Qatar." In *2011 IEEE Global Engineering Education Conference (EDUCON)*, 875-879. IEEE, 2011.

- Rouse, M. "Infrastructure as a Service (IaaS)." TechTarget. <https://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS>, 2019.
- Scarfone, K., and P. Mell. "Guide to Intrusion Detection and Prevention Systems (IDPS)." National Institute of Standards and Technology, 2007.
- Shapiro, C., and H. R. Varian. Information Rules: A Strategic Guide to the Network Economy. Harvard Business School Press, 1999.
- Sharim, L. "Challenges of Data Sovereignty in Cloud Computing: A Systematic Review." Journal of Cloud Computing 20, no. 2 (2021): 89-102.
- Shatilov, K., V. Boiko, S. Krendelev, D. Anisutina, and A. Sumaneev. "Solution for Secure Private Data Storage in a Cloud." In 2014 Federated Conference on Computer Science and Information Systems, 885-889. IEEE, September 2014.
- Singi, K., S. G. Choudhury, V. Kaulgud, R. J. C. Bose, S. Podder, and A. P. Burden. "Data Sovereignty Governance Framework." In Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, 303-306, June 2020.
- Sood, S. K. "A Combined Approach to Ensure Data Security in Cloud Computing." Journal of Network and Computer Applications 35, no. 6 (2012): 1831-1838.
- Soofi, A. A., M. I. Khan, and F. E. Amin. "A Review on Data Security in Cloud Computing." International Journal of Computer Applications 96, no. 2 (2017): 95-96.
- Sookhak, M., F. R. Yu, M. K. Khan, Y. Xiang, and R. Buyya. "Attribute-Based Data Access Control in Mobile Cloud Computing: Taxonomy and Open Issues." Future Generation Computer Systems 72 (2017): 273-287.
- Sultan, N. "Cloud Computing: A Democratising Force?" International Journal of Information Management 33, no. 5 (2013): 810-815.
- Sun, Y., J. Zhang, Y. Xiong, and G. Zhu. "Data Security and Privacy in Cloud Computing." International Journal of Distributed Sensor Networks 10, no. 7 (2014): 190903.
- Surbiryala, J., and C. Rong. "Cloud Computing: History and Overview." In 2019 IEEE Cloud Summit, 1-7, August 2019.
- Tang, J., Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya. "Ensuring Security and Privacy Preservation for Cloud Data Services." ACM Computing Surveys (CSUR) 49, no. 1 (2016): 1-39.

- Turner, V., J. Kaplan, S. Thomas, and B. Saunders. "Software as a Service (SaaS): A Market and Financial Model." *Future Generation Computer Systems* 21, no. 3 (2003): 513-522.
- Vial, G. "Understanding Digital Transformation: A Review and a Research Agenda." *The Journal of Strategic Information Systems* 28, no. 2 (2019): 118-144.
- Wallen, J. "Disaster Recovery: IT's Most Important Task." *TechRepublic*. <https://www.techrepublic.com/article/disaster-recovery-its-most-important-task/>, 2018.
- Wang, C., Q. Wang, K. Ren, and W. Lou. "Ensuring Data Storage Security in Cloud Computing." In *2009 17th International Workshop on Quality of Service*, 1-9. IEEE, July 2009.
- Wang, Q., C. Wang, K. Ren, W. Lou, and J. Li. "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing." *IEEE Transactions on Parallel and Distributed Systems* 22, no. 5 (2010): 847-859.
- Weber, A. S. "Can Cloud Computing Overcome Barriers to Education in the Middle East and North Africa (MENA) Region?" In *Conference Proceedings of eLearning and Software for Education (eLSE)*, vol. 7, no. 01, 565-570. Carol I National Defence University Publishing House, 2011.
- Weerakkody, V., M. Janssen, and Y. K. Dwivedi. "Transformational Change and Business Process Reengineering (BPR): Lessons from the British and Dutch Public Sector." *Government Information Quarterly* 28, no. 1 (2016): 27-36.
- Wei, L., H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos. "Security and Privacy for Storage and Computation in Cloud Computing." *Information Sciences* 258 (2014): 371-386.
- Westerman, G., D. Bonnet, and A. McAfee. *Leading Digital: Turning Technology into Business Transformation*. Harvard Business Review Press, 2014.
- World Bank. *Qatar GDP per Capita*. World Bank Data, 2023.
- Yamin, M., and R. Ibrahim. "The Role of Leadership in Digital Transformation: A Review." *Digital Transformation Review* 8, no. 1 (2022): 30-45.
- Yan, Z., X. Li, M. Wang, and A. V. Vasilakos. "Flexible Data Access Control Based on Trust and Reputation in Cloud Computing." *IEEE Transactions on Cloud Computing* 5, no. 3 (2015): 485-498.
- Yang, H., and M. Tate. "A Descriptive Literature Review and Classification of Cloud Computing Research." *Communications of the Association for Information Systems* 31, no. 1 (2012): 2-57.

- Yu, S., C. Wang, K. Ren, and W. Lou. "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing." In 2010 Proceedings IEEE INFOCOM, 1-9. IEEE, March 2010.
- Zainudeen, A., and D. Ratnadiwakara. "Digital Economies and Data Sovereignty in the MENA Region." ICT Policy Review, 2021.
- Zhang, Q., L. Cheng, and R. Boutaba. "Cloud Computing: State-of-the-Art and Research Challenges." Journal of Internet Services and Applications 1 (2010): 7-18.
- Zhang, X., and H. Chen. "Regulatory Frameworks for Data Sovereignty and Cloud Computing: A Comparative Analysis." Journal of Information Technology & Politics 17, no. 3 (2020): 215-231.
- Zhu, X., H. Liu, and S. Wei. "Cloud Computing Adoption in the Public Sector: A Meta-Analysis of Antecedents and Outcomes." Information Systems Frontiers 23, no. 5 (2021): 1229-1248.
- Zissis, D., and D. Lekkas. "Addressing Cloud Computing Security Issues." Future Generation Computer Systems 28, no. 3 (2012): 583-592.
- Zubair, M., D. Unal, A. Al-Ali, T. Reimann, and G. Alinier. "Cybersecurity for Next-Generation Healthcare in Qatar." Journal of Emergency Medicine, Trauma & Acute Care, Qatar Health 2020 Conference 2021, no. 2 (2021): 41.

List of Abbreviations

Abbreviation	Full Form
IRB	Institutional Review Board
HBKU	Hamad Bin Khalifa University
QFZ	Qatar Free Zone
QNV2030	Qatar National Vision 2030
SDG	Sustainable Development Goals
TASMU	Qatar Smart Program
Qnbn	Qatar National Broadband Network
EM	Consumer Engagement Towards Energy Saving Behaviour
ML	Machine Learning
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
M-learning	Mobile Learning
CIA	Confidentiality, Integrity, and Availability
NIA	National Information Assurance
MCIT	Ministry of Communication and Information Technology
GCP	Google Cloud Platform
IoMT	Internet of Medical Things
IDS	Intrusion Detection System
DL	Deep Learning
DNN	Deep Neural Network
SVM	Support Vector Machine
KNN	K-Nearest Neighbours
BYOK	Bring Your Own Key
CRA	Communications Regulatory Authority
GDPR	General Data Protection Regulation
AI	Artificial Intelligence
MENA	Middle East and North Africa
NCSA	National Cybersecurity Agency - Qatar

Appendix 1

Interview Questions

1. What are the main drivers for organisations in Qatar to adopt cloud computing?
2. How do organisations address vulnerabilities concerning data confidentiality in the cloud?
3. How can organisations ensure they retain data ownership when stored in the cloud?
4. What are the key differences between private and public cloud infrastructures?
5. Are there scenarios under existing laws where third parties can access data in the public cloud?
6. How significant is data sovereignty for Qatar from a national perspective?
7. Is Qatar using private clouds for sensitive information, and what are the challenges in developing such infrastructure?
8. What lessons have been learned since cloud service providers began operating in Qatar?
9. How do entities decide to migrate to the cloud, and is it optional?
10. What are the essential steps required before transitioning to the cloud?
11. What types of encryption are used for data stored in the cloud, and can cloud service providers access this data?
12. Are there data classifications that should not be moved to the cloud, and what are the storage strategies for such data?
13. What impacts are anticipated on the cloud computing landscape with new cloud service providers in Qatar?
14. What legal frameworks govern the cloud environment in Qatar, and which body oversees these services?
15. Did cloud service providers comply with specific local laws or regulations upon entering Qatar?
16. How does the USA PATRIOT Act affect Qatar's data sovereignty?
17. Are there ongoing academic research projects focusing on data sovereignty or cloud computing in Qatar?
18. What are the differences between data localisation and data sovereignty?
19. What improvements and regulatory changes are needed in Qatar's cloud computing scenario?
20. Could you share your background and experience in cloud computing?
21. Do you consent to mentioning your name, title, and organisation in this publication?