EXPLORING EMERGING INFORMATION GOVERNANCE AND LEGISLATIVE CHALLENGES OF CLOUD COMPUTING

Bedour Alboloushi *, Mohammad Alkandari **, Basil Alothman ***, Shaikha AlSanad ****, Anwaar Alkandari *****

* *Corresponding author,* Department of Business Management, Kuwait College of Science and Technology, Kuwait City, Kuwait
Contact details: Kuwait College of Science and Technology, P. O. Box 27235, 13133 Kuwait City, Kuwait
** Kuwait International Law School, Kuwait City, Kuwait
*** Department of Computer Science and Engineering, Kuwait College of Science and Technology, Kuwait City, Kuwait
**** Energy and Building Research Center, Kuwait Institute for Scientific Research, Kuwait City, Kuwait
***** Department of Business Management, Kuwait Technical College, Abu-Halifa, Kuwait

How to cite this paper: Alboloushi, B., Alkandari, M., Alothman, B., AlSanad, S., & Alkandari, A. (2026). Exploring emerging information governance and legislative challenges of cloud computing. *Corporate Law & Governance Review, 8*(2), 38–50. https://doi.org/10.22495/clgrv8i2p4

ISSN Online: 2664-1542
ISSN Print: 2707-1111

Received: 13.08.2025
Revised: 14.02.2026; 05.03.2026
Accepted: 10.03.2026

JEL Classification: K24, M15, O32, O38
DOI: 10.22495/clgrv8i2p4

Abstract

Cloud computing is increasingly integrated into e-government initiatives to improve service efficiency (Wibisana et al., 2026). However, this integration raises unique non-technological challenges for developing countries where regulatory and institutional frameworks are still evolving. This paper examines information governance and legislative challenges that hinder effective cloud computing adoption in developing countries (Younus et al., 2025). By using Kuwait as an exploratory case, the paper employs a qualitative case study approach, incorporating a literature review and document analysis to critically examine the non-technological challenges associated with cloud computing. The analysis identifies key information governance and legislative issues that pose significant obstacles to cloud computing integration, including data security, privacy protection, and policy adequacy. To address these challenges, the cloud security framework model (CSFM) is introduced to offer a comprehensive view of legislative and information governance dimensions that support more secure and accountable cloud adoption. The framework provides a lens for government organizations to evaluate governance readiness and regulatory alignment. The paper offers practical implications for policymakers, government entities, and information technology (IT) professionals seeking to support secure and efficient cloud-based e-government services.

Keywords: Cloud Computing, Governance, E-government, Technology Policy, Cyber Security, Developing Country, Technology Adoption

Authors' individual contribution: Conceptualization — B.Alb., M.A., S.A., and A.A.; Methodology — B.Alb., M.A., and A.A.; Investigation — B.Alb., M.A., and B.Al.; Writing — Original Draft — B.Alb., M.A., B.Al., S.A., and A.A.; Writing — Review & Editing — B.Alb. and M.A.; Visualization — B.Al.; Supervision — A.A.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

1. INTRODUCTION

Following the adoption of e-government, developing countries are racing to innovate to achieve economic, social, and environmental goals. This technological advancement requires governments to create sustainable infrastructure. Hence, infrastructure investment is essential to support ongoing e-government improvement initiatives. However, the high costs associated with development and maintenance, as well as disruptions in infrastructure, push developing countries towards integrating cloud computing.

Cloud computing offers opportunities for developing countries to improve the quality of government services, reduce operating costs, and enhance the integration of government organizations (K. Ali et al., 2018; Ren et al., 2023; Nguyen et al., 2025). Given the rapid increase in both the demand for and implementation of cloud computing by government organizations in developing countries, it is essential to understand the different vulnerabilities and challenges imposed by this emerging technology. The integration of cloud computing into e-government is a complex paradox. It involves various technological and non-technological dimensions that need to be considered to ensure successful integration (Wahsh & Dhillon, 2015). In the context of developing countries, non-technological challenges have a more significant influence (Alkhwaldi et al., 2018; Subramaniam & Teh, 2026; Labkir et al., 2026).

Despite the widespread use of cloud computing applications, information security remains a primary concern, particularly in the context of e-government, where information is considered a significant government asset (AlMindeel & Martins, 2021). With the use of cloud computing, government-sensitive data can be stored in remote servers under the control of a third party and, hence, can be exposed to privacy and security concerns (Al Mudawi et al., 2020). Therefore, it is critically important to focus on the non-technological challenges of information assets.

This paper aims to contribute to the ongoing discussion in the literature by focusing on the privacy and security concerns of cloud computing from a non-technological perspective, considering two domains: information governance and legislative challenges. Information governance ensures the effective utilization and protection of information assets following an established set of procedures and policies. It also ensures that information assets are appropriately regulated and maintained by offering standards and guidelines for cloud computing. Information governance can also encompass legislative practices (MacLennan, 2014). Legislation and government laws influence how cloud computing applications are implemented and utilized, and due to the operational complexities of cloud computing, laws and regulations involving data security and privacy may either encourage or prohibit cloud services (Younus et al., 2025). Therefore, it is essential to analyze legislative challenges in order to address policy gaps and to keep pace with the rapid advancement of cloud computing initiatives (Kushagra & Dhingra, 2022).

To further understand and address these challenges, this research aims to identify and analyze the critical non-technological challenges associated with integrating cloud computing into e-government services. This emphasis aligns with the main research question:

RQ: What are the key information governance and legislative challenges that hinder the integration of cloud computing in e-government services in developing countries, and how can these challenges be addressed?

By addressing this question, this research contributes to the existing literature by exploring the unique challenges and considerations that developing countries face when integrating cloud computing into their e-government initiatives. In addition, this research provides insights and recommendations that can guide policymakers and government organizations in developing countries.

This paper focuses on Kuwait as a critical case study of a developing country navigating the complex transition toward integrating cloud computing into e-government services. In Kuwait, the recent initiative of utilizing cloud-based storage solutions in the context of e-government has raised significant concerns regarding data security, privacy, and regulatory readiness. These concerns reflect existing gaps in information governance and legislative structures that support digital transformation. Therefore, the analysis and evaluation of information governance and legislative challenges related to data protection are crucial to align with the advancement of cloud computing and to support broader government strategies and goals for digital transformation.

The paper provides new insights because cloud adoption in government settings increasingly depends not only on technical capability but also on governance readiness, legal clarity, and data protection compliance, particularly in developing regulatory contexts (Wibisana et al., 2026). The paper applies a qualitative exploratory case approach based on literature review and regulatory and policy document analysis. The paper identifies the key information governance and legislative challenges faced by the country in integrating cloud computing solutions into e-government.

The main contribution of the study is: first, it identifies key governance and legislative gaps affecting cloud computing adoption in e-government; and second, it proposes a structured conceptual framework to support more secure cloud integration.

The remainder of this paper is organized as follows. Section 2 provides a literature review of cloud computing, information governance, and legislative challenges. Section 3 explains the methodology and research approach. Section 4 presents the results of the Kuwait case analysis, including the legislative and information security challenges, and, based on the results, discusses its relevance in relation to existing literature. Section 5 concludes the paper, offering recommendations to aid practitioners and suggesting directions for future work.

2. LITERATURE REVIEW

2.1. Cloud computing in the context of e-governments

E-government refers to the provision of government information and public services to citizens and organizations via the internet (Al Mudawi et al., 2020). It empowers countries to navigate forthcoming disruptions or exigencies with enhanced resilience and preparedness. E-government involves harnessing information and communication technology (ICT) to transform governmental operations, improve the efficiency and effectiveness of service delivery, and enhance citizen engagement (Albous & Alboloushi, 2025).

Extensive research has focused on e-government adoption and implementation in developing countries (Kumar et al., 2018; Mustaf

et al., 2020). Despite the advancement in e-government and the investments made by developing countries, challenges persist (Kushagra & Dhingra, 2022; Wibisana et al., 2026).

Cloud computing holds potential for improving the effectiveness and efficiency of government operations and the delivery of public services (K. Ali et al., 2018; Irion, 2012; Liang, 2012). Therefore, cloud computing is increasingly adopted by governments for data storage and processing (Zhang et al., 2014; Ara et al., 2020).

Cloud computing offers many benefits, such as scalability, which is related to expandable capacity to handle big data and manage increasing user numbers (Mohammed & Ibrahim, 2015). Another major benefit is related to cost savings on infrastructure and technical support, as government organizations can lease ICT resources according to demand. The "pay-as-you-go" model of cloud computing lowers operational expenses for organizations in the public sector (Alshomrani & Qamar, 2013). Other major benefits include availability from any internet-connected device, time savings in data access and processing, remote installation and configuration across multiple devices, disaster recovery capability, and increased capacity to manage large data volumes (Hasimi & Penzel, 2023).

Given the potential of cloud computing as an emerging transformative technology to revolutionize various sectors and drive innovation across industries, research suggests that cloud computing has evolved into a strategic focus for many governments and is already utilized in key components of the government's information technology (IT) infrastructure (Karim, 2022; Albous & Alboloushi, 2025). The literature discusses the technological aspects of cloud computing, including security, data encryption, compatibility, and system architecture (Phaphoom et al., 2015). It also explores the organizational aspects of cloud computing (Al Hadwer et al., 2021; Gangwar et al., 2015), notably organizational adoption decisions (Sallehudin et al., 2015), IT leaders' perceptions of cloud computing (Hailu, 2012), and employees' technical knowledge and competence (Lian et al., 2014; Wahsh & Dhillon, 2015; Isabella et al., 2025).

Although prior research has examined cloud adoption in developing countries (Kushagra & Dhingra, 2022; Gibreel et al., 2024), integration levels remain uneven. Research shows that many governments continue to encounter structural and institutional challenges that limit the effective integration of cloud computing, such as legislative ambiguities and fragmented governance frameworks (Wibisana et al., 2026). This gap is reflected within the Gulf Cooperation Council (GCC), which includes Kuwait, Saudi Arabia, the United Arab Emirates (UAE), Qatar, Oman, and Bahrain. Significant digital transformation investments have been made by GCC countries to diversify their economies and achieve sustainable development in the public sector (Fadlelmula & Qadhi, 2024). These countries are actively pursuing "smart city" initiatives to improve the efficiency and effectiveness of public services (Elian & Kisswani, 2024). Cloud computing and artificial intelligence (AI) are critical components of this digital transformation (Al-Hajri et al., 2024). Given that GCC countries have unique technological and regulatory landscapes, the absence of context-specific research poses challenges for governments and policymakers to effectively integrate cloud computing into e-government initiatives.

Most cloud computing research focuses mainly on the UAE and Saudi Arabia, while other GCC countries like Kuwait remain underexplored despite comparable digital transformation ambitions (Al-Hajri et al., 2024). UAE and Saudi Arabia serve as regional models for digital transformation and cloud computing adoption. For example, the UAE developed a National Digital Government Strategy 2025 to promote integrated cloud adoption across sectors (Mohammed et al., 2024). Research shows that the UAE has widely integrated cloud computing in various industries through proactive digital strategies and public–private partnerships (Goher et al., 2021). Similarly, as part of the Saudi Vision 2030, Saudi Arabia has made significant progress in cloud adoption and launched a "Cloud-First Policy" to guide cloud computing integration across different government entities (A. Ali et al., 2021).

In contrast, cloud computing integration in Kuwait remains fragmented as the country is actively pursuing implementing a comparable national framework. Understanding the challenges of cloud computing in Kuwait is essential to developing context-specific strategies that align with its digital transformation goals.

2.2. Information governance in the era of cloud computing

During the transition of government to the cloud, one of the major concerns of cloud computing is information security. Information security is not only a technological issue; it also involves how organizations manage information, use technology, and evaluate the security risks. Therefore, it is necessary to consider information security from the perspective of information governance (George & Gao, 2014). The processes and procedures designed to regulate the use of information, including but not limited to those required by law, are known as information governance (MacLennan, 2014).

The use of cloud computing increases the complexity of information governance. The reason for this is that cloud-based architectures pose a threat to conventional data security measures. Hence, governments must provide specific guidelines for cloud computing to ensure that their information assets are stored safely and securely.

Within the domain of e-government, public sector organizations handle vast amounts of public data, generated, managed, and utilized to provide government services. This increasing reliance on public data emphasizes the need to embrace cloud computing. The core aspect of cloud computing is data migration to a third party. Governments form agreements or alliances with service providers concerning data migration and obtaining cloud services.

The data migration process entails transferring data, applications, or other essential items from the client system to a cloud computing system (Shakya, 2019). The data is transferred across the network and stored on the service provider's servers.

The transmitted data can include personal details, health records, financial transactions, and sensitive government information and records. It is believed that when clients transmit data to the cloud for processing, their control over the information asset is significantly diminished (Irion, 2012). Service providers' servers may be situated anywhere globally, including Europe and Asia. Clients do not own or control these remote servers, used for storing and processing sensitive data. Data encryption and blockchain solutions are primarily employed during data transfer to protect data and combat unauthorized access (Sehgal et al., 2020; Zhang et al., 2024).

2.3. Information governance challenges in cloud computing

Despite the associated benefits of cloud computing, some significant challenges and concerns are debated by various researchers (Irion, 2012). These encompass not only technical challenges associated with adopting and using cloud computing (Phaphoom et al., 2015), but also concerns related to data and information security (Sehgal et al., 2020). This is related to safeguarding and ensuring that data stored in the cloud is protected from a variety of dangers and threats.

Data security challenges can be classified into four aspects:

1) *Integrity*: Ensuring data remains unaltered and protected from unauthorized deletion, modification, or fabrication is vital (Mahmood et al., 2019). Data manipulation or loss might occur as a result of unintentional behavior, such as a data crash, or malicious behavior, such as cyberattacks (Mahmood et al., 2019). In cloud computing, this raises some concerns due to the limited understanding of how data accuracy is maintained. As a result, a significant trust concern arises because of the lack of transparency and security assurances (Abied et al., 2022). Research indicates that trust has a significant impact on individuals' long-term usage of IT, such as e-government services (Zhang et al., 2018; Zhang et al., 2022). The lack of trust in the government's ability to safeguard government information and citizens' data may have broader effects on governance and societal stability (Zaman & Kamshad, 2023).

2) *Accountability*: Accountability is related to having unified bylaws and legal guidelines of data protection (Liang, 2012). Integrating cloud computing with e-government leads to cross-border data movement. As a result, in the event of a security breach, it would be difficult to determine when the breach occurred, in which nation it occurred, and under what legal authority. This complexity is exacerbated by the fact that many countries still lack or have insufficient cloud computing rules (Irion, 2012). The lack of evidence of accountability is one of the major concerns related to data security in cloud computing (Al-Rashdi et al., 2021).

3) *Confidentiality*: Protecting data from unauthorized access is a vital facet of data security (Zissis & Lekkas, 2012). As mentioned earlier, cloud computing involves allowing a cloud service provider (a third party) to store and process information. The usage of a cloud service provider to store data exposes data to unauthorized users who may be able to access citizens' personally identifiable information (PII) (Al Mudawi et al., 2020), which could lead to both financial and reputational damage (Shakya, 2019).

4) *Privacy*: Data privacy refers to the ability of users to limit the disclosure, use, and storage of personal information (Zissis & Lekkas, 2012). Privacy policy is one of the fundamental aspects of information governance (Zhou et al., 2020). Cloud computing involves transferring and processing government information and personal data (PD) within blurred boundaries. As a result, people's rights to retain the ownership and the privacy of their sensitive information used in e-government systems are compromised by the vulnerability of cloud computing (Al Mudawi et al., 2020; Tripathy et al., 2023).

The absence of comprehensive governance frameworks can reduce the effectiveness of integrating cloud computing into e-government services (Wibisana et al., 2026). Therefore, implementing robust information governance practices is crucial in order to fulfil the requirements for data protection. Information governance practices aid in safeguarding data, preventing unauthorized access, and ensuring proper use of data and information, thereby enhancing the quality of data and information. Therefore, establishing transparent data governance frameworks is a crucial imperative to promote efficiency, accountability, and user security. This necessitates the implementation of rigorous measures to safeguard PD and ensure its ethical and transparent utilization.

2.4. Legislative challenges in cloud computing

Legislatures worldwide are currently facing challenges related to the need to keep pace with the rapid production of data due to the use of cloud computing and the transfer of data beyond borders. The following subsection discusses the issues that arise in relation to data protection frameworks and PD privacy regulations.

2.4.1. Data protection frameworks

The primary purpose of any data protection regime is to protect sensitive government data and to ensure the privacy of individuals. This is achieved through both regulating the processes associated with collecting, storing, and transferring information while preventing its misapplication, mishandling, or misuse. In response to these concerns and the increasing demands of data protection, various countries around the world are enforcing regulations to address these issues stemming from the use of new technologies. For example, the European Union (EU) considers privacy and data protection to be fundamental rights that should be enshrined within EU legislation, whereas the US protects data on a sectoral basis. The main challenge of data protection within cloud computing relates to cross-border data transfer to a third country. For example, the EU recognizes the paramount importance of transferring data as an essential element of the intercontinental relationship that fosters economic growth amongst countries. However,

the presence of different and sometimes conflicting data protection legislation and rules makes it challenging to ensure the protection of transferred data (Ahmed, 2011).

For example, despite the US offering assurances to the EU about providing an adequate data protection framework, many intelligence and surveillance agencies (e.g., the Federal Bureau of Investigation [FBI]) have been granted access to the PD of EU citizens that are stored on US servers. As a result, a number of legal challenges threaten bilateral trade between the US and EU member states. This case highlights the critical need for countries utilizing cloud computing services to examine the laws of the third country and determine whether it secures the transferred data from any surveillance or intelligence activities. The EU mandates that all countries comply with its regulations when transferring data in cloud computing. Data controllers working within the EU and European Economic Area (EEA) must comply with Chapter 5 of the General Data Protection Regulation 2016/679 (GDPR), which prohibits entities from transferring PD to countries that do not provide an adequate level of protection (European Union, 2016). As a result, numerous multinational institutions located both inside and outside the EU and EEA countries face difficulties when it comes to ensuring their compliance with all of the applicable data protection requirements when transferring data into and out of the EU. Therefore, as cloud computing is borderless, paying close attention to both the country's own laws and regulations and those of other countries is critically important (Irion, 2012).

2.4.2. Personal data privacy regulations

Privacy, as defined by Warren and Brandeis (1890), is the right of individuals to be left alone. This right has traditionally been afforded a high degree of importance, which has led to it being included in many legal frameworks. This is reflected in frameworks like the GDPR, which sets strict standards to guarantee a high level of data protection across the EU.

When addressing the concept of PD, it is important to first recognize that the data subject is the individual to whom particular examples of PD are concerned (Singh & Cobbe, 2019). The GDPR defines PD in Article 4 as information that can directly or indirectly identify an individual through specific identifiers (European Union, 2016).

PD has an essential role in the digital economy because digital services and transactions rely heavily on information relating to identifiable individuals (Salbu, 2002). For example, PD can include a person's name, age, contact details, and medical condition. The collection of PD has increased significantly in recent decades due to the use of the Internet. This supports the growth of both public and private sectors and drives advancements in areas such as commerce and healthcare (MacDonald & Streatfeild, 2014; Yakovleva, 2020).

It is essential to consider the challenges associated with PD in cloud computing. Given the value of PD, an outright ban on transferring PD to a country lacking robust data protection regulations could have a negative economic impact on those operating within the EU/EEA. Therefore, Chapter 5 of the GDPR regulates the transfer of PD to any country located outside the EU/EEA (i.e., a third country). The primary concern when transferring data to a third country is the possibility that such countries do not provide an adequate level of data protection when compared with the GDPR. Therefore, Articles 44, 45, and 46 of the GDPR detail different transfer tools that can be used to legitimize the transfer of PD outside the EU/EEA. It should be noted here that further discussion of these transfer tools falls outside the scope of the present article.

Another key challenge is related to obtaining valid and informed consent. The failure to obtain individuals' explicit consent prior to the use of their data may lead to unfair practices and pose a threat to individuals' privacy. A key concern is that individuals may be identified, in a direct or indirect way, through related information. Thus, the definition of PD within the GDPR Article 4 includes the phrase "any information", which reflects the broad scope of data protection provisions applied to any information relating to individuals that may enable their identification by others (van Bekkum & Borgesius, 2023). Some PD might be considered more sensitive than other data due to its nature and so require a higher level of protection. As a consequence, the GDPR aims to protect such information under a new category termed a "special category of PD", including information related to ethnic background, religious beliefs, political opinions, genetics, biometrics (where used for identification purposes), health, or criminal convictions and offences. The use of certain special categories of data is prohibited, and stricter rules apply for those who obtain an individual's information (van Bekkum & Borgesius, 2023).

Therefore, ensuring valid and informed consent is considered a central requirement. It is particularly essential in cloud environments where data processing purposes and locations may not always be transparent.

3. RESEARCH METHODOLOGY

This paper employs an exploratory qualitative research approach, incorporating a case study approach and an extensive literature review. The qualitative case study approach is widely used in exploratory research as it allows an in-depth investigation of complex phenomena within a specific context (Yin, 2014). Hence, it enables a comprehensive understanding of the complexities involved in the integration of cloud computing.

Document analysis represents the primary data collection method for this research. Document analysis involves thorough examination and extraction of meaningful information from a variety of documentary sources (Kutsyuruba, 2023). This method is well-suited for qualitative case studies that focus on providing a comprehensive exploration and generating detailed insights into a specific phenomenon (Bowen, 2009). According to Dalglish et al. (2020), document analysis can be used independently as a stand-alone method for data collection. This is because document analysis not only provides a rich and detailed understanding of a specific phenomenon, but it is also as efficient as

other qualitative data collection methods, such as interviews or participant observation (Mogalakwe, 2006).

Document analysis has been widely used in prior research on information systems, governance, and public policy to examine regulatory environments, compliance structures, and institutional frameworks (Nwagboso et al., 2024). Documents are often recognized as effective advocacy tools, especially when document analysis is used to highlight critical issues and engage policymakers (Kayesa & Shung-King, 2021). Given that this paper examines information governance and legislative challenges related to cloud computing in e-government, which are primarily reflected in regulatory documents, policy frameworks, and institutional reports, document analysis is considered well-suited. It is particularly suitable for exploratory and framework-building research where legal texts, policy documents, and formal guidelines constitute the main units of analysis because it allows for the synthesis of information from multiple documentary sources to build a comprehensive understanding of the information governance and legislative challenges in cloud computing (Kayesa & Shung-King, 2021).

In this research, the authors investigated government IT policies and relevant literature to identify challenges related to information governance and legislation. The documents used in the analysis were collected through various sources such as peer-reviewed journals, government reports, IT/cloud policy documents, regulatory guidelines, and publicly available e-government strategies. Newspaper articles were considered only when they reported officially issued policies or government initiatives and were used for contextual support.

Document selection followed a structured and transparent screening process to ensure relevance and credibility. Included documents met the following criteria: 1) issued by official government bodies, regulatory authorities, or recognized institutional sources; 2) directly related to cloud computing, data governance, digital services, cybersecurity, or e-government regulation; 3) publicly accessible documents. The authors prioritized materials that explicitly addressed key relevant themes such as data privacy, protection, information classification, and cloud infrastructure deployment. By closely examining these sources, the authors extracted recurring concepts, information governance challenges, and policy gaps. This in-depth exploratory analysis of government IT policies and the literature serves as the foundation for understanding the broader context of cloud computing within e-government initiatives, particularly in developing countries such as Kuwait.

The rationale for selecting Kuwait as a case study is to gain insights into the unique challenges of integrating cloud computing into e-government services within a developing country in the Middle East region. Although the challenges related to e-government in developing countries may share similarities, but Kuwait requires a distinctive perspective to understand and address these challenges due to its unique socio-economic, technological, and institutional context (Mrhaouarh et al., 2018). As highlighted in prior comparisons with other GCC countries, in particular the UAE and Saudi Arabia, Kuwait has made slower progress and remains comparatively behind in formalizing cloud computing strategies and lacks a unified national policy framework. This gap highlights the importance of a thorough and focused investigation of cloud computing in Kuwait.

By understanding the challenges affecting cloud services integration, such as compliance with data protection laws and ensuring data security and privacy, researchers can provide valuable insights and recommendations for government agencies in developing countries looking to adopt cloud computing solutions in their e-government initiatives.

The comprehensive analysis of the findings from both the literature review and the case study analysis informs the development of a conceptual framework depicted in Figure 1. This framework is designed to highlight the key aspects to consider when migrating government services to the cloud. It provides valuable insights regarding compliance with key data protection laws and information governance principles to ensure the security and privacy of sensitive government information and citizens' data.

4. RESULTS AND DISCUSSION

4.1. The case of cloud computing in Kuwait

The following subsection analyzes the issues that arise in relation to information governance and legislation in Kuwait to propose directions for reforming the current data protection framework to enhance the effective utilization of cloud computing services.

As a developing country, Kuwait is actively working towards improving the efficiency of e-government and supporting public sector organizations (ALMutairi & Thuwaini, 2015). However, in the context of e-government development, Kuwait lags behind most GCC countries. According to the United Nations' 2022 global e-government report, Kuwait ranks as one of the lowest countries within the GCC region, as cited in the United Nations' survey on E-Government Development Index [EGDI] (United Nations, 2022).

Countries such as the UAE, Saudi Arabia, and Qatar have introduced data protection and digital governance regulations, although their scope and provisions vary. Kuwait has also made recent regulatory advances.

The Kuwaiti government launched the 2035 Vision initiative, which incorporates cloud computing into the national e-government strategy. Consequently, the Kuwaiti government announced a strategic partnership with Google to enhance this digital transformation. The utilization of Google's cutting-edge technology and experience in data analytics, cybersecurity, and AI allows Kuwait to accomplish its digitalization objectives in terms of healthcare, education, disaster recovery, and smart living, while also creating job opportunities for young Kuwaitis (Kuwait Times, 2023). Recently, Kuwait's 2035 Vision has been extended to Kuwait's 2040 Vision in response to national and international changes (Kuwait News Agency [KUNA], 2023), though no official announcement has been made regarding this extension to date.

The announcement of this strategic partnership to integrate cloud computing raises significant concerns regarding data and information management, particularly in terms of data breaches and issues related to a lack of ownership and control over data (Al-Roomi, 2023). Cyberthreats are a major concern for cloud computing and e-government. According to The National Cyber Security Index (NCSI)[1], Kuwait currently ranks 98th globally, whereas other GCC countries boast higher rankings. For example, Saudi Arabia is ranked 14th on the list. This index assesses the degree of preventive cybersecurity in terms of implementing information security requirements and dealing with cyber incidents, considering factors such as existing data protection legislation and established authorities. According to Al-Mekaimi (2025), a significant data breaches recently occurred in Kuwait, impacting 887 Kuwaiti websites and exposing over 4,360 data files. The affected websites included multiple sectors, such as education, communications, e-commerce, and certain public sector entities. The incident was reported following prior warnings from IT security specialists regarding vulnerabilities in security controls. This breach is not an isolated case, as Kuwait has previously experienced cyber incidents, including the "Anthrax" attack, targeting both governmental and private websites and resulting in financial losses for banking and financial institutions. A recent report by Rackspace Technology (2023) indicates that only 48% of organizations in the Middle East are confident in their ability to understand cybersecurity threats. With the increasing frequency of significant data breaches and the growing complexity of cybercriminal tactics, it is imperative for Kuwait to urgently adopt international cybersecurity standards to mitigate such incidents. In Kuwait, the Communication and Information Technology Regulatory Authority (CITRA) is a recently established institution concerned with dealing with e-government and cloud computing services (Ghloum, 2023).

Månsson (2023) argues that security concerns and the legislative and regulatory frameworks exert influence on the adoption and use of cloud computing in Kuwait. Public sector employees grapple with several challenges in the digital transfer to cloud computing, such as a lack of expertise, data availability, data integration, and transfer. In addition, they have cloud security considerations like data breaches, data encryption, Identity and Access Management (IAM policies), compliance with local data protection policies, data loss, and cloud incident response strategies (Månsson, 2023). The integration of data between government agencies can increase the vulnerability of e-government systems. In alignment with previous research, a recent study conducted by Zaman and Kamshad (2023) indicates that a majority of people in Kuwait, more than 60%, are worried about how their PD is managed by both government and private organizations. This concern is likely driven by the lack of clear information governance policies and legal frameworks for cloud computing in the country. The challenges of information governance and legal implications need to be carefully addressed to ensure data security and privacy in e-government applications using cloud computing.

Compliance with data protection laws and ensuring the security and privacy of sensitive government data are essential factors to be considered when integrating cloud computing into e-government services in developing countries (Alkaraan et al., 2022). In Kuwait, it is essential to consider government cloud compliance frameworks such as Federal Risk and Authorization Management Program (FedRAMP), Federal Information Security Management Act (FISMA), Defense Information Systems Agency (DISA), Security Technical Implementation Guides (STIGs), and International Organization for Standardization (ISO 27018). The adoption of these frameworks may pose challenges for the government related to security, privacy, and regulatory requirements.

Given the complexity of cloud computing, it is essential to investigate the potential effects of such an initiative on all levels of information governance. Hence, a comprehensive framework linking governance and legal requirements is needed to strengthen security, risk management, data protection, privacy, accountability, data ownership, responsibilities, Service-Level Agreements (SLAs), and data handling clauses (Nugraha & Martin, 2022).

4.2. Legislation of cloud computing in Kuwait

The situation with regard to the protection of PD in Kuwait differs from other countries. In Kuwait, specific legal challenges emerge in the context of e-government. The lack of specific, comprehensive data protection laws and regulations pose a significant challenge to the implementation of cloud computing (Zaman & Kamshad, 2023).

Kuwait, being an Arab-Muslim country, delivers its legislation from an Islamic perspective (Al-Mutairi, 2022). The relevant laws classify data based on the sensitivity of its content, aligning with the accepted norms of Kuwaiti society. Specifically, CITRA's data classification policy classifies the secrecy of PD according to the following four tiers (CITRA, 2021a).

- Tier one (public data) refers to unclassified data openly accessible and available to the public, including openly accessible policies, published laws and regulations, newspapers, and general website content. This data does not require any encryption because it does not identify the individual or protected government or private sector information.
- Tier two (private insensitive data) refers to data that is owned by public and private organizations or by an individual. This data has a low degree of sensitivity, and its unauthorized disclosure causes minimal or no harm. Examples include name, email, job details, e-mail address, age, civil identification number, academic qualifications, and contact information.
- Tier three (private sensitive data) refers to data that is owned by public and private organizations or by an individual at the personal level. The unauthorized release of such data may harm individual privacy or negatively affect organizational interests. It includes internal reports, files concerning lawsuits, and medical reports.
- Tier four (highly sensitive data) represents highly confidential private data. The exposure of this data causes severe damage to the privacy of individuals or organizations. Therefore, this data requires a high level of encryption that ensures

[1] https://ncsi.ega.ee/country/kw/

the highest possible levels of protection and security, such as political documents, international negotiations records, and similarly critical records.

The four tiers described above demonstrate CITRA's relatively narrow approach to data protection. Therefore, Kuwait's legislature needs to consider revising the current classification system to ensure complete compliance with international regulations such as the GDPR and to reduce potential future legislative challenges.

In contrast to Europe, electronic PD represents an integral part of the Kuwaiti Constitution of 1962[2]. While the right to privacy is not explicitly stated within the Constitution, it acknowledges data protection rights are considered in Article 30, specifying that "Personal liberty is guaranteed", and Article 39, which states that "The freedom of postal, telegraphic and telephonic communications is safeguarded and their secrecy is guaranteed". Moreover, in Case No 3 of 1982, the Constitutional Court of Kuwait clarified the core meaning of Article 30 by stating that "The individual's right to freedom requires the preservation of their dignity and personal information, as well as the prevention of unauthorized access to their secrets, pursuant to the individual's right to enjoy their private life". Thus, an individual's private life forms part of their personal entity, which must be protected and not disclosed under any circumstances, except in cases where prior consent has been provided.

The Kuwaiti legislature has also passed Law No. 20 of 2014 on Electronic Transactions (ETL), which addresses the protection of PD and the privacy of ETL in Chapter 7. However, its data protection coverage is considered relatively limited as it does not provide specific principles governing the transfer of data outside Kuwait. The lack of a clear, structured framework for lawful cross-border data transfers creates practical regulatory gaps and uncertainty for government cloud systems regarding whether foreign storage or remote administration qualifies as a regulated transfer. In addition, transferred data is not explicitly protected against foreign surveillance.

Soon after the promulgation of the ETL, Law No. 37 of 2014 on the Establishment of Communication and Information Technology Regulatory Authority (CITRA) was introduced, aimed at regulating the Kuwaiti telecommunications sector pursuant to general constitutional principles in order to ensure individuals' privacy. Chapter 3 of the law explicitly stipulates this goal and guarantees CITRA the power to issue data protection regulations in Kuwait. In 2021, CITRA issued the Data Privacy Protection Regulation (DPPR) No. 21 of 2021 (CITRA, 2021b), which guarantees the basic rights and freedoms in respect of the collection, processing, and transferring of PD. The introduction of the DPPR represented a significant milestone in the development of Kuwait's legal sector, as previously, there was no inclusive data protection law, and the concept of privacy relied on relevant legal provisions found in other pieces of legislation, such as the duty of confidentiality or binding terms between private individuals.

Shortly after the promulgation of the DPPR, CITRA issued the Cloud Computing Regulatory Framework (CCRF) No. 112 of 2021 (CITRA, 2021c) in an effort to regulate the cloud activities offered by computing service providers registered with CITRA. The CCRF is intended to regulate the implementation of cloud services in Kuwait. As such, its provisions bind the following entities:

1) Cloud service providers licensed by CITRA with operating data centers in Kuwait that host third- and fourth-level data.

2) Providers approved by CITRA that host first- and second-level data for public sector entities.

3) All public sector cloud service subscribers.

4) Private sector entities that host government data.

Unlike the GDPR, the DPPR has limited application to telecommunication service providers and related industry sectors regarding data collection, storage, processing, and transfer by private and public sectors. Interestingly, the DPPR considers the process of data transfer in a broad context when it defines data collection and processing as "any process or set of processes applied to PD, whether inside or outside Kuwait" (CITRA, 2021b, p. 2). This definition fails to provide an exact meaning for the term "outside Kuwait" and, therefore, may include the storage of data on outside servers or the provision of remote access to PD from a different country. Moreover, the DPPR also lacks clarity on the concept of transferring data outside the jurisdiction of Kuwait.

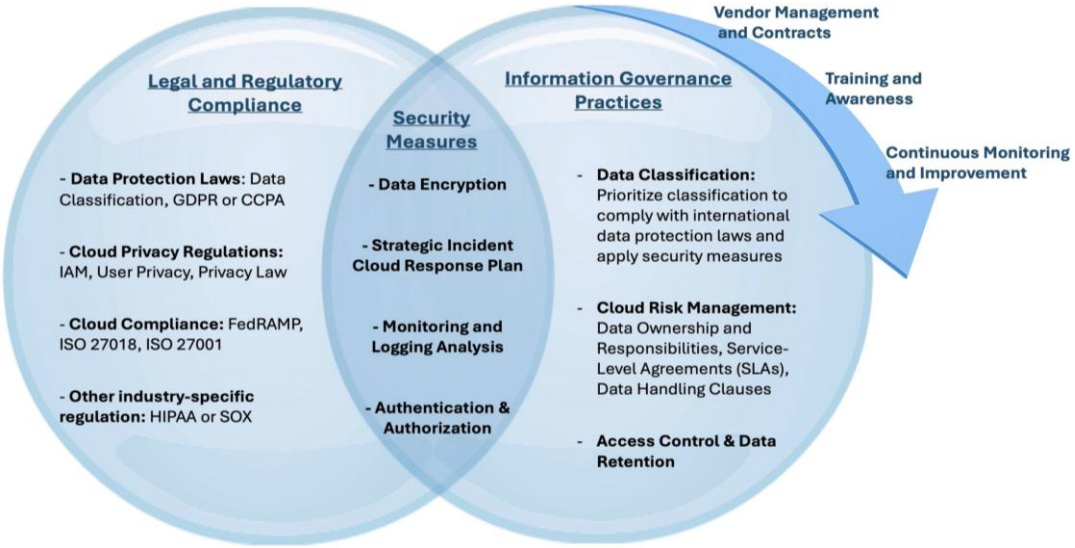
Compared with Kuwait, the EU regulatory framework provides more structured data transfer conditions, as the European Data Protection Board (EDPB) has established essential criteria governing the transfer of data outside of the EU/EEA territories. The primary goal in restricting the transfer of data to a third country is not undermine the EU's data protection regime; rather, it is to prevent PD from being accessed by the third country's authorities. In this context, the ETL and DPPR both fall short in providing clear guidelines for the qualified transfer of data outside Kuwait. However, although DPPR may not fully achieve its intended final goal without clear regulations and guidelines and real monitoring of data processing, the DPPR represents a constructive step forward for the Government of Kuwait. This emphasizes the need for the development of a robust information governance and legislative framework in cloud computing. The following proposed framework aims to address these issues and enhance the integration of cloud computing into e-government services in Kuwait.

4.3. Cloud security framework model

Ensuring the security of government information in the cloud represents a complex and evolving challenge (Kandukuri et al., 2009). Therefore, when considering the migration of government services to the cloud, it is important to think beyond technical controls. Effective cloud computing adoption requires alignment with governance structures and legislative requirements. To address this, this study proposes an integrated conceptual framework (Figure 1), the cloud security framework model (CSFM), that combines information governance and legal-regulatory considerations with security measures to support secure and effective cloud computing adoption.

[2] https://www.lexismiddleeast.com/law/Kuwait/Law_0_1962/en/Title_2_-_Fundamental_Constituents_of_Kuwaiti_Society.html

Figure 1. Cloud security framework model (CSFM)



Source: Authors' elaboration.

In Figure 1, the CSFM illustrates the multi-dimensional approach required for the establishment and operation of a comprehensive cloud security framework. This framework integrates the needs of legal compliance, information governance, and security measures to safeguard cloud database security. The proposed framework model complies with the local data protection laws, cloud privacy regulations, and cloud compliance, as demonstrated in Table 1.

Table 1. Algorithm based on the CSFM

Algorithm	***CSFM***
Require:	Cloud Service Provider (CSP), Cloud Legal and Regulatory (CLR), Cloud Industry Standards (CIS).
Ensure:	Cloud policies, implementation guidelines, adaptation, and refinement suggestions.
Step 1:	Initialize cloud security framework.
Step 2:	Define legal and regulatory compliance.
Step 3:	Integrate Industry Standards and cybersecurity best practices.
Step 4:	Develop a cloud security framework model.
Step 5:	Create documentation and policies.
Step 6:	Provide implementation instruction guidelines.
Step 7:	Adaptation and refinement strategies.
Step 8:	End

Source: Authors' elaboration.

The proposed algorithm (Table 1) provides a structured eight-step approach for the effective integration of cloud computing based on the proposed CSFM. The proposed algorithm is grounded in the three core pillars of CSFM: legal and regulatory compliance, security measures, and information governance. It includes eight sequential steps essential to ensure that cloud integration into e-government is secure, compliant, and aligned with regulatory standards.

Step 1 involves establishing the initial groundwork for cloud security, for example, by defining objectives, identifying key stakeholders, and outlining the scope of the cloud integration. In Step 2, relevant legal and regulatory requirements (such as GDPR) are identified and interpreted. Step 3 involves incorporating information governance and cybersecurity measures to enhance data protection. Step 4 involves designing a comprehensive security model that outlines scope, processes, and control mechanisms by integrating legal, technical, and operational aspects. Step 5 involves drafting the formal documentation required to institutionalize the framework, including security policies, compliance protocols, access control policies, data classification schemes, and incident response procedures. Step 6 focuses on creating practical and step-by-step guidelines to assist implementation teams as well as the decision-makers in applying the cloud integration model. Documents can include architectural diagrams, deployment protocols, and training materials to support effective cloud integration. Step 7 involves reviewing and updating the integration model as the organizational and regulatory landscapes evolve to address new risks or gaps. The algorithm concludes with Step 8, which reflects that cloud integration should be secured and institutionalized across the organization, and that cloud computing is supported by policy, training, and continuous monitoring mechanisms. This algorithm offers a practical approach for government organizations in developing countries like Kuwait to adopt cloud computing effectively.

4.4. Discussion

The results of this study highlight that cloud computing adoption in e-government environments is significantly shaped by governance and legislative readiness rather than technical capability alone. In the Kuwait context, lack of standard data governance structures, gaps in regulatory clarity, and lack of unified policy frameworks emerge as central constraints. This supports and extends prior literature that identifies institutional and regulatory factors as primary barriers to public sector cloud transformation (Tripathy et al., 2023; Wibisana et al., 2026).

The results of this study informed the development of the CSFM, which highlights the fundamental requirements and challenges associated with information governance and legislative compliance in cloud e-government

environments. This framework provides conceptual insights by illustrating the combined roles of regulatory compliance obligations, information governance mechanisms, and security measures. By integrating these dimensions, the model helps explain how legal, policy, and governance factors interact with technical safeguards in shaping secure cloud adoption. In this way, the CSFM serves as an interpretive lens for understanding governance and legislative readiness in cloud computing initiatives. These results add to the rapidly expanding fields of cloud computing and e-government.

5. CONCLUSION

The Kuwaiti legislature must enact a comprehensive data protection framework that is able to keep pace with developments concerning data transfer and cloud computing. This could be achieved through the following means:

1) Establish information governance procedures and policies to increase transparency and accountability, thereby increasing the level of confidence and trust in information security and privacy, in alignment with ISO 27018.

2) Periodically review and assess the country's data protection laws and regulations to accommodate technology advancements.

3) Mandate a protection adequacy assessment, involving a thorough review and endorsement of the data transfer destination's legislation, similar to the provisions of the GDPR.

4) Establish an authority or department tasked with monitoring illegal access to data by authorities in third countries, including surveillance activities.

5) Document any remote access by individuals who operate local data storage servers and pursue legal action based on the principle of confidentiality.

6) Create a strategic cloud compliance framework aligned with the stipulations of the proposed CSFM.

The fundamental objective of this paper is to explore the integration of cloud computing into e-government services in developing countries. The paper explores the challenges that developing countries face when considering migrating government information and services to the cloud. The CSFM has been proposed to identify the key requirements and challenges arising from information governance and legislative considerations. The CSFM integrates compliance requirements, governance structures, and technical security controls to support cloud computing adoption. Consequently, the CSFM offers a conceptual roadmap for addressing governance and legislative requirements in the effective integration of cloud computing into e-government services. However, the proposed framework warrants further validation with empirical data collected through different methods, such as surveys or interviews with government entities and cloud governance stakeholders. Future research is therefore essential to provide deeper insight into its practical effectiveness and broader applicability.

In addition, this paper uses Kuwait's e-government as a case study and an exemplar for developing countries. Accordingly, while the framework provides conceptual insights that may be adaptable to other countries with similar regulatory and governance characteristics, it remains grounded in the Kuwait context and has not yet been empirically validated across multiple settings. Hence, further cross-context validation is required before broader generalization can be established.

Based on this focus on Kuwait, the study provides practical recommendations specifically directed at the Kuwaiti legislative and regulatory environment to contribute to the advancement of e-government initiatives. In addition, the findings offer practical guidance for policymakers in navigating information governance and legislative compliance challenges in cloud computing. This can facilitate the successful implementation of cloud computing in e-government.

There are other essential opportunities for future research that hold potential to enhance our understanding and drive forward the development of cloud computing and e-government. One prospective area for future exploration in subsequent studies is the role of international collaboration in confronting legislative challenges associated with the implementation of e-government. This could involve investigating how various countries cooperate and negotiate regulatory frameworks to provide valuable insights into efficacious strategies for standardizing policies and addressing shared challenges. Moreover, the integration of other emerging technologies into e-government, such as AI and blockchain present a promising avenue for future investigation. By delving into these specific avenues for future research, researchers can contribute to the continual evolution of e-government practices and policies.

REFERENCES

Abied, O., Ibrahim, O., & Kamal, S. N.-I. M. (2022). Adoption of cloud computing in e-government: A systematic literature review. *Pertanika Journal of Science & Technology, 30*(1). https://doi.org/10.47836/pjst.30.1.36

Ahmed, S. (2011). *A discussion of practical steps to harmonize data protection rules globally*. https://doi.org/10.2139/ssrn.1966281

Al Hadwer, A., Tavana, M., Gillis, D., & Rezania, D. (2021). A systematic review of organizational factors impacting cloud-based technology adoption using technology-organization-environment framework. *Internet of Things, 15*, Article 100407. https://doi.org/10.1016/j.iot.2021.100407

Al Mudawi, N., Beloff, N., & White, M. (2020). Issues and challenges: Cloud computing e-government in developing countries. *International Journal of Advanced Computer Science and Applications, 11*(4), 7–11. https://doi.org/10.14569/IJACSA.2020.0110402

Albous, M. R., & Alboloushi, B. (2025). AI-driven innovations in e-government: How is AI reshaping the public sector? In M. Lytras, A. Alkhaldi, & P. Ordóñez de Pablos (Eds.), *Harnessing AI, blockchain, and cloud computing for enhanced e-government services* (pp. 93–118). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-7678-2.ch004

Al-Hajri, A., Abdella, G. M., Al-Yafei, H., Aseel, S., & Hamouda, A. M. (2024). A systematic literature review of the digital transformation in the Arabian Gulf's oil and gas sector. *Sustainability, 16*(15), Article 6601. https://doi.org/10.3390/su16156601

Ali, A., Manzoor, D., & Alouraini, A. (2021). The implementation of government cloud for the services under e-governance in the KSA. *Science International Journal, 3*(3), 249–257. https://www.researchgate.net/publication/352642789_THE_IMPLEMENTATION_OF_GOVERNMENT_CLOUD_FOR_THE_SERVICES_UNDER_E-GOVERNANCE_IN_THE_KSA

Ali, K. E., Mazen, S. A., & Hassanein, E. E. (2018). Assessment of cloud computing adoption models in e-government environment. *International Journal of Computational Intelligence Studies, 7*(1), 67–92. https://doi.org/10.1504/IJCISTUDIES.2018.090168

Alkaraan, F., Albitar, K., Hussainey, K., & Venkatesh, V. G. (2022). Corporate transformation toward Industry 4.0 and financial performance: The influence of environmental, social, and governance (ESG). *Technological Forecasting and Social Change, 175*, Article 121423. https://doi.org/10.1016/j.techfore.2021.121423

Alkhwaldi, A. F. A., Kamala, M. A., & Qahwaji, R. S. R. (2018). Analysis of cloud-based e-government services acceptance in Jordan: Challenges and barriers. *Journal of Internet Technology and Secured Transactions, 6*(2), 556–568. https://doi.org/10.20533/jitst.2046.3723.2018.0069

Al-Mekaimi, H. (2025). Digital diplomacy in Kuwait's new foreign policy (2020–2024): Opportunities and challenges. In M. Zreik (Ed.), *Innovations and tactics for 21st century diplomacy* (pp. 225–252). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-6074-3.ch010

AlMindeel, R., & Martins, J. T. (2021). Information security awareness in a developing country context: Insights from the government sector in Saudi Arabia. *Information Technology and People, 34*(2), 770–788. https://doi.org/10.1108/ITP-06-2019-0269

Al-Mutairi, N. H. (2022). The right to privacy in the digital age as expressed in a Muslim country: A case study of Kuwait. *Arab Law Quarterly, 38*(1–2), 110–137. https://doi.org/10.1163/15730255-bja10108

ALMutairi, N. N., & Thuwaini, S. F. (2015). Cloud computing uses for e-government in the Middle East region opportunities and challenges. *International Journal of Business and Management, 10*(4), 60–69. https://doi.org/10.5539/ijbm.v10n4p60

Al-Rashdi, Z. A., Dick, M., Al-Rashdi, R. A., & Al-Husaini, Y. (2021). Information security accountability in the cloud computing context — A comprehensive review. In R. Montasari, H. Jahankhani, & H. Al-Khateeb (Eds.), *Challenges in the IoT and smart environments: A practitioners' guide to security, ethics and criminal threats* (pp. 189–210). Springer International Publishing. https://doi.org/10.1007/978-3-030-87166-6_8

Al-Roomi, M. (2023, January 10). Kuwait's Google partnership: What's behind the headlines? *Kuwait Times*. https://kuwaittimes.com/kuwaits-google-partnership-whats-behind-the-headlines/

Alshomrani, S., & Qamar, S. (2013). Cloud based e-government: Benefits and challenges. *International Journal of Multidisciplinary Sciences and Engineering, 4*(6), 1–7. https://www.ijmse.org/Volume4/Issue6/paper4.pdf

Ara, R., Rahim, M. A., Roy, S., & Prodhan, U. K. (2020). Cloud computing: Architecture, services, deployment models, storage, benefits and challenges. *International Journal of Trend in Scientific Research and Development, 4*(4), 837–842. https://www.researchgate.net/publication/341788106_Cloud_Computing_Architecture_Services_Deployment_Models_Storage_Benefits_and_Challenges

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Case No. 3 of 1982. (1982). Court of Cassation. https://www.eastlaws.com/judgments-full-text/ar/kuwait/cassation-constitutional/judicial-year-1982/08-11-1982/no-3?type=1&id=367993

Communication and Information Technology Authority (CITRA). (2021a, June 13). *Data classification policy V2.3*. https://www.citra.gov.kw/sites/ar/LegalReferences/Data%20Classification%20Policy.pdf

Communication and Information Technology Authority (CITRA). (2021b, June 28). *Data privacy protection regulation V1.8*. https://www.citra.gov.kw/sites/en/LegalReferences/Data_Privacy_Protection_Regulation.pdf

Communication and Information Technology Authority (CITRA). (2021c, September 21). *Cloud computing regulatory framework V2.4*. https://www.citra.gov.kw/sites/en/LegalReferences/Cloud_computing_regulatory_framework.pdf

Dalglish, S. L., Khalid, H., & McMahon, S. A. (2020). Document analysis in health policy research: The READ approach. *Health Policy and Planning, 35*(10), 1424–1431. https://doi.org/10.1093/heapol/czaa064

Elian, M. I., & Kisswani, K. M. (2024). Smart cities: GCC and Kuwait experience. In F. Belaïd & A. Arora (Eds.), *Smart cities: Social and environmental challenges and opportunities for local authorities* (pp. 339–358). Springer, Cham. https://doi.org/10.1007/978-3-031-35664-3_18

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of European Union, L 119*, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Fadlelmula, F. K., & Qadhi, S. M. (2024). A systematic review of research on artificial intelligence in higher education: Practice, gaps, and future directions in the GCC. *Journal of University Teaching and Learning Practice, 21*(6), 146–173. https://doi.org/10.53761/pswgbw82

Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management, 28*(1), 107–130. https://doi.org/10.1108/JEIM-08-2013-0065

George, E., & Gao, J. (2014). A qualitative study of information challenges in the cloud. In *Proceedings of the 25th Australasian Conference on Information Systems (ACIS 2014)*. https://openrepository.aut.ac.nz/server/api/core/bitstreams/49cb63ea-c4fa-48b8-b006-8b6f0da6bebc/content

Ghloum, G. (2023, May 30). Google Cloud key for Kuwait's digital transformation: Official. *Kuwait Times*. https://kuwaittimes.com/google-cloud-key-for-kuwaits-digital-transformation-official/

Gibreel, O., Alsaber, A. R., Mahenthiran, S., & Tahat, L. (2024). Factors and barriers to cloud computing adoption for small and medium-sized enterprises in Kuwait. *World Journal of Science, Technology and Sustainable Development, 19*(3–4), 233–246. https://doi.org/10.47556/J.WJSTSD.19.3-4.2024.9

Goher, G., Masrom, M., Amrin, A., & Abd Rahim, N. (2021). Disruptive technologies for labor market information system implementation enhancement in the UAE: A conceptual perspective. *International Journal of Advanced Computer Science and Applications, 12*(2), 370–378. https://doi.org/10.14569/IJACSA.2021.0120247

Hailu, A. (2012). *Factors influencing cloud-computing technology adoption in developing countries* [Ph.D. Dissertation, Capella University]. ERIC. https://eric.ed.gov/?id=ED551853

Hasimi, L., & Penzel, D. (2023). A case study on cloud computing: Challenges, opportunities, and potentials. In N. Kryvinska, M. Greguš, & S. Fedushko (Eds.), *Developments in information and knowledge management systems for business applications* (pp. 1–25). Springer, Cham. https://doi.org/10.1007/978-3-031-27506-7_1

Irion, K. (2012). Government cloud computing and national data sovereignty. *Policy & Internet, 4*(3–4), 40–71. https://doi.org/10.1002/poi3.10

Isabella, Agustian, E., Baharuddin, T., & Ibrahim, A. H. H. (2025). Bridging e-government with digital literacy: A literature review [Special issue]. *Journal of Governance & Regulation, 14*(1), 361–371. https://doi.org/10.22495/jgrv14i1siart12

Kandukuri, B. R., Paturi, R. V., & Rakshit, A. (2009). Cloud security issues. In *2009 IEEE International Conference on Services Computing* (pp. 517–520). IEEE. https://doi.org/10.1109/SCC.2009.84

Karim, F. (2022). Cloud computing-based M-Government. *Informatica, 46*(5), 69–73. https://doi.org/10.31449/inf.v46i5.3879

Kayesa, N. K., & Shung-King, M. (2021). The role of document analysis in health policy analysis studies in low and middle-income countries: Lessons for HPA researchers from a qualitative systematic review. *Health Policy OPEN, 2*, Article 100024. https://doi.org/10.1016/j.hpopen.2020.100024

Kumar, R., Sachan, A., & Mukherjee, A. (2018). Direct vs indirect e-government adoption: An exploratory study. *Digital Policy, Regulation and Governance, 20*(2), 149–162. https://doi.org/10.1108/DPRG-07-2017-0040

Kushagra, K., & Dhingra, S. (2022). Cloud doctrine: impact on cloud adoption in the government organizations of India. *Journal of Science and Technology Policy Management, 13*(4), 925–951. https://doi.org/10.1108/JSTPM-06-2019-0058

Kutsyuruba, B. (2023). Document analysis. In J. M. Okoko, S. Tunison, & K. D. Walker (Eds.), *Varieties of qualitative research methods: Selected contextual perspectives* (pp. 139–146). Springer, Cham. https://doi.org/10.1007/978-3-031-04394-9_23

Kuwait Law No. 20/2014 on Electronic Transactions. (2014). LexisNexis. https://www.lexismiddleeast.com/law/Kuwait/Law_20_2014/en

Kuwait News Agency (KUNA). (2023, September 25). *Minister: 4th Kuwait Master Plan 2040 to boost development, strategic vision*. Kuwait News Agency. https://www.kuna.net.kw/ArticleDetails.aspx?id=3110618

Kuwait Times. (2023, January 10). *Google Cloud will boost Kuwait's digital infrastructure: Al-Nahedh*. https://www.kuwaittimes.com/google-cloud-will-boost-kuwaits-digital-infrastructure-al-nahedh/

Labkir, S.-E., El Loumani, L., & El Harmouzi, N. (2026). E-government, institutional quality and economic growth in the MENA region: Theoretical analysis and empirical evidence. *Journal of Governance and Regulation, 15*(1), 117–125. https://doi.org/10.22495/jgrv15i1art11

Law No. 37 of 2014 on the Establishment of Communication and Information Technology Regulatory Authority. (2014). Communication and Information Technology Regulatory Authority (CITRA). https://www.citra.gov.kw/sites/en/LawofCITRA/Law%20No.%2037-%202014.pdf

Lian, J.-W., Yen, D. C., & Wang, Y.-T. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. *International Journal of Information Management, 34*(1), 28–36. https://doi.org/10.1016/j.ijinfomgt.2013.09.004

Liang, J. (2012). Government cloud: enhancing efficiency of e-government and providing better public services. In *Proceedings of the 2012 International Joint Conference on Service Sciences* (pp. 261–265). IEEE. https://doi.org/10.1109/IJCSS.2012.20

MacDonald, D. A., & Streatfeild, C. M. (2014). Personal data privacy and the WTO. *Houston Journal of International Law, 36*(3), 625–653. https://international.vlex.com/vid/personal-data-privacy-and-636230525

MacLennan, A. (2014). *Information governance and assurance: Reducing risk, promoting policy*. Facet Publishing.

Mahmood, G. S., Huang, D. J., & Jaleel, B. A. (2019). Achieving an effective, confidentiality and integrity of data in cloud computing. *International Journal of Network Security, 21*(2), 326–332. https://www.researchgate.net/publication/332819858_Achieving_an_Effective_Confidentiality_and_Integrity_of_Data_in_Cloud_Computing

Månsson, H. (2023). Adoption and implementation of cloud computing in public organizations in Kuwait: A qualitative study. *Kuwait Journal of Information Technology and Decision Sciences, 1*(1). https://kuwaitjournals.com/index.php/kjitds/article/view/12

Mogalakwe, M. (2006). The use of documentary research methods in social research. *African Sociological Review, 10*(1), 221–230. https://www.researchgate.net/publication/267994948_The_Use_of_Documentary_Research_Methods_in_Social_Research

Mohammed, F., & Ibrahim, O. B. (2015). Drivers of cloud computing adoption for E-government services implementation. *International Journal of Distributed Systems and Technologies, 6*(1), 1–14. https://doi.org/10.4018/ijdst.2015010101

Mohammed, G., Ines, S., & Hayet, K. (2024). The digital transformation experience in the United Arab Emirates. *International Journal of Economic Perspectives, 18*(11), 1963–1980. https://ijeponline.org/index.php/journal/article/view/696

Mrhaouarh, I., Okar, C., Namir, A., & Chafiq, N. (2018). Cloud computing adoption in developing countries: A systematic literature review. In *the 2018 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)* (pp. 73–79). IEEE. https://doi.org/10.1109/ITMC.2018.8691295

Mustaf, A., Ibrahim, O., & Mohammed, F. (2020). E-government adoption: A systematic review in the context of developing nations. *International Journal of Innovation, 8*(1), 59–76. https://doi.org/10.5585/iji.v8i1.16479

Nguyen, T. B. T., Doan, T. N., Ta, T. T., Tran, H. Y., Nguyen, D. A., Pham, M. A., Nguyen, T. H., & Nguyen, P. T. (2025). Factors affecting the intention of adopting cloud-based accounting strategy: The case of micro, small, and medium-sized enterprises. *Corporate and Business Strategy Review, 6*(4), 194–208. https://doi.org/10.22495/cbsrv6i4art18

Nugraha, Y., & Martin, A. (2022). Cybersecurity service level agreements: Understanding government data confidentiality requirements. *Journal of Cybersecurity, 8*(1), Article tyac004. https://doi.org/10.1093/cybsec/tyac004

Nwagboso, C. I., Ezikeudu, C. C., Nwagboso, N. S., Agbor, U. I., Ebegbulem, J. C., Okorie, C., Adams, J. A., Akah, A. U., Bassey, U. S., Obi, N. N., Ekpo, S.-O., Onyema, O. A., & Egba, V. J. (2024). Public policy and internal security sector governance challenges: A situational study of some economic development indicators [Special issue]. *Journal of Governance & Regulation, 13*(2), 317–326. https://doi.org/10.22495/jgrv13i2siart8

Phaphoom, N., Wang, X., Samuel, S., Helmer, S., & Abrahamsson, P. (2015). A survey study on major technical barriers affecting the decision to adopt cloud services. *Journal of Systems and Software, 103*, 167–181. https://doi.org/10.1016/j.jss.2015.02.002

Rackspace Technology. (2023). *The 2023 Cybersecurity Research Report: Despite security concerns, C-suite and IT leaders raise budgets, explore AI.* https://www.rackspace.com/sites/default/files/white-papers/Solve-The-2023-Cybersecurity-Research-Report-Q32023_EMEA_White-Paper.pdf

Ren, S., Hao, Y., & Wu, H. (2023). Digitalization and environment governance: Does internet development reduce environmental pollution? *Journal of Environmental Planning and Management, 66*(7), 1533–1562. https://doi.org/10.1080/09640568.2022.2033959

Salbu, S. R. (2002). The European Union data privacy directive and international relations. *Vanderbilt Journal of Transnational Law, 35*(2), 655–695. https://scholarship.law.vanderbilt.edu/vjtl/vol35/iss2/7/

Sallehudin, H., Razak, R. C., & Ismail, M. (2015). Factors influencing cloud computing adoption in the public sector: An empirical analysis. *Journal of Entrepreneurship & Business, 3*(1), 30–45. https://doi.org/10.17687/JEB.0301.03

Sehgal, N. K., Bhatt, P. C. P., & Acken, J. M. (Eds.). (2020). Cloud computing and information security. In *Cloud Computing with Security: Concepts and Practices* (pp. 111–141). Springer, Cham. https://doi.org/10.1007/978-3-030-24612-9_7

Shakya, S. (2019). An efficient security framework for data migration in a cloud computing environment. *Journal of Artificial Intelligence, 1*(1), 45–53. https://doi.org/10.36548/jaicn.2019.1.006

Singh, J., & Cobbe, J. (2019). The security implications of data subject rights. *IEEE Security & Privacy, 17*(6), 21–30. https://doi.org/10.1109/MSEC.2019.2914614

Subramaniam, A., & Teh, R. (2026). Accelerating digital transformation: Key drivers of cloud computing adoption and firm performance outcomes in Malaysian SMEs. *Future Business Journal, 12*(1), Article 28. https://doi.org/10.1186/s43093-025-00711-7

Tripathy, S., Sengupta, A., & Jyotishi, A. (2023). Looming market failure in cloud computing: A new institutional economics perspective. *Digital Policy, Regulation and Governance, 25*(5), 490–504. https://doi.org/10.1108/DPRG-09-2022-0111

United Nations. (2022). *E-government survey 2022: The future of digital government.* https://desapublications.un.org/sites/default/files/publications/2022-09/Report%20without%20annexes.pdf

Van Bekkum, M., & Borgesius, F. Z. (2023). Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception? *Computer Law & Security Review, 48*, Article 105770. https://doi.org/10.1016/j.clsr.2022.105770

Wahsh, M. A., & Dhillon, J. S. (2015). An investigation of factors affecting the adoption of cloud computing for e-government implementation. In the *2015 IEEE Student Conference on Research and Development (SCOReD)* (pp. 323–328). IEEE. https://doi.org/10.1109/SCORED.2015.7449349

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220. https://doi.org/10.2307/1321160

Wibisana, P. A., Wijoyo, S., Nadia, F. N. D., Amiati, M., & Putri, S. A. (2026). Cloud-powered knowledge management: A systematic literature review of public sector innovation through cloud computing. *Cogent Business & Management, 13*(1), Article 2616543. https://doi.org/10.1080/23311975.2026.2616543

Yakovleva, S. (2020). Personal data transfers in international trade and EU law: A tale of two 'necessities'. *The Journal of World Investment & Trade, 21*(6), 881–919. https://doi.org/10.1163/22119000-12340189

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). SAGE Publications Ltd.

Younus, M., Purnomo, E. P., Nurmandi, A., Mutiarin, D., Manaf, H. A., Mumtaz, F., & Khairunnisa, T. (2025). Analyzing the trend of government support for cloud computing usage in e-government architecture. *Journal of Cloud Computing, 14*(1), Article 14. https://doi.org/10.1186/s13677-025-00735-y

Zaman, S., & Kamshad, H. (2023). Data leakage in Kuwait: Reasons and solution. In *the 2023 Computer Applications & Technological Solutions (CATS)* (pp. 1–12). IEEE. https://doi.org/10.1109/CATS58046.2023.10424323

Zhang, X., Chang, R., Gu, M., & Huo, B. (2024). Blockchain implementation and shareholder value: A complex adaptive systems perspective. *International Journal of Operations & Production Management, 44*(3), 666–698. https://doi.org/10.1108/IJOPM-11-2022-0711

Zhang, X., Ma, H., Wu, Y., De Pablos, P. O., & Wang, W. (2014). Applying cloud computing technologies to upgrade the resource configuration of laboratory course: The case of quality engineering education platform. *The International Journal of Engineering Education, 30*(3), 596–602. https://dialnet.unirioja.es/servlet/articulo?codigo=7372819

Zhang, X., Wei, X., Ou, C. X. J., Caron, E., Zhu, H., & Xiong, H. (2022). From human-AI confrontation to human-AI symbiosis in society 5.0: Transformation challenges and mechanisms. *IT Professional, 24*(3), 43–51. https://doi.org/10.1109/MITP.2022.3175512

Zhang, X., Yan, X., Cao, X., Sun, Y., Chen, H., & She, J. (2018). The role of perceived e-health literacy in users' continuance intention to use mobile healthcare applications: An exploratory empirical study in China. *Information Technology for Development, 24*(2), 198–223. https://doi.org/10.1080/02681102.2017.1283286

Zhou, S., Zhang, X., Liu, J., Zhang, K., & Zhao, Y. (2020). Exploring development of smart city research through perspectives of governance and information systems: A scientometric analysis using CiteSpace. *Journal of Science and Technology Policy Management, 11*(4), 431–454. https://doi.org/10.1108/JSTPM-05-2019-0051

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006