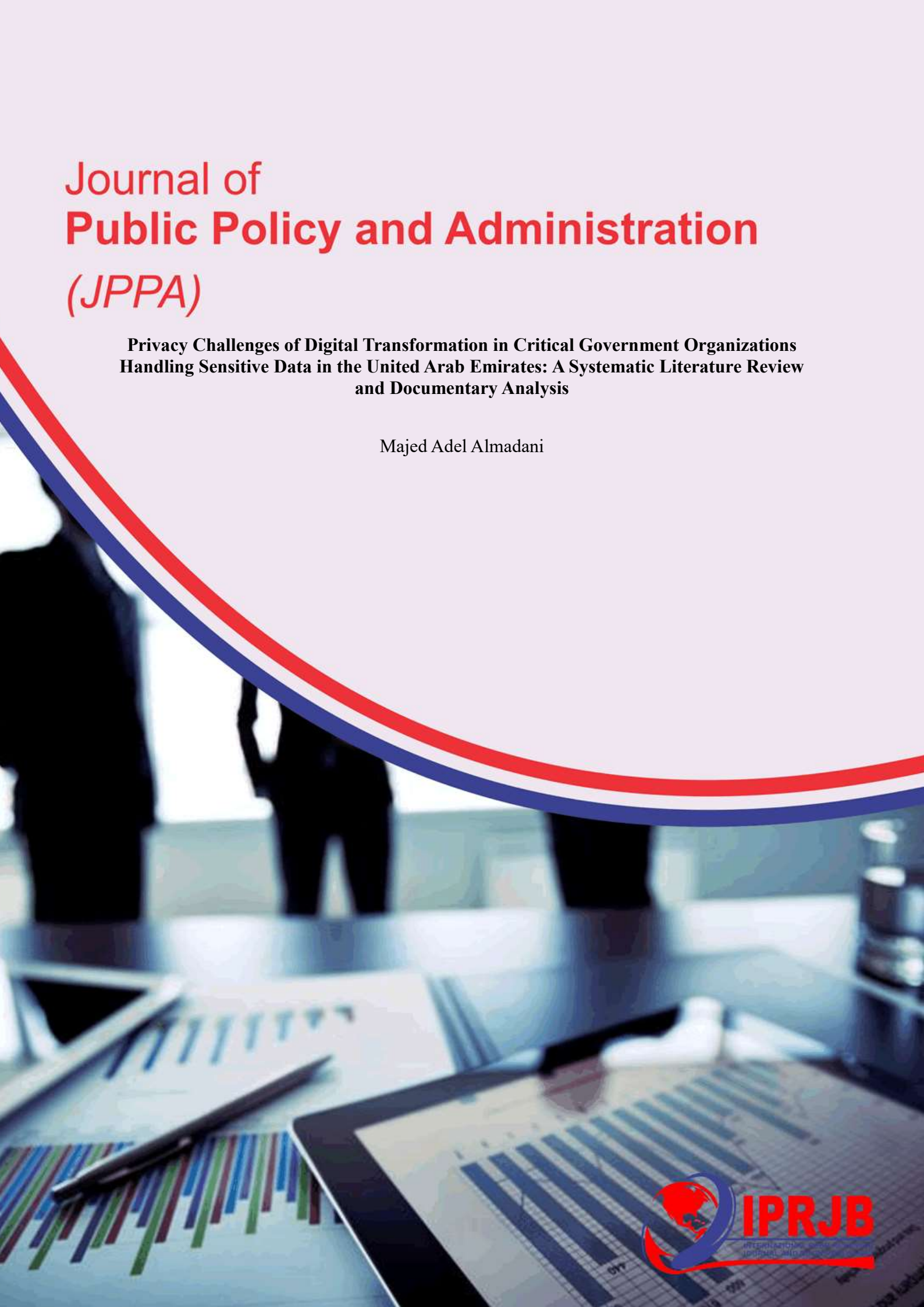
Journal of
Public Policy and Administration
(JPPA)

Privacy Challenges of Digital Transformation in Critical Government Organizations Handling Sensitive Data in the United Arab Emirates: A Systematic Literature Review and Documentary Analysis

Majed Adel Almadani



Journal of Public Policy and Administration
ISSN 2520-5315 (Online)
Vol 11, Issue 2, No.3, pp36 - 65, 2026

www.iprjb.org

Privacy Challenges of Digital Transformation in Critical Government Organizations Handling Sensitive Data in the United Arab Emirates: A Systematic Literature Review and Documentary Analysis

[1*]Majed Adel Almadani
Postgraduate Student, School of Innovation and Change Management, Hamdan Bin Mohammed Smart University

Article History

Received 9th May 2026

Received in Revised Form 11th June 2026

Accepted 8th July 2026

How to cite in APA format:

Almadani, M. (2026). Privacy Challenges of Digital Transformation in Critical Government Organizations Handling Sensitive Data in the United Arab Emirates: A Systematic Literature Review and Documentary Analysis. *Journal of Public Policy and Administration*, *11*(2), 36–65. https://doi.org/10.47604/jppa.3858

Abstract

Purpose: The purpose of this study was to understand the privacy concerns surrounding the digital transformation of critical government organizations handling sensitive data in the United Arab Emirates (UAE). It examined privacy risks arising from technologies, organizational practices, legislation, and third-party involvement during public-sector digital transformation.

Methodology: This study adopted a qualitative systematic literature review and documentary analysis. Scholarly sources were retrieved from Scopus, ScienceDirect and Emerald Insight journals by applying specific search terms for digital transformation, privacy, data protection, security, governance and regulation. The literature search was carried out in English-language sources from 2022 to 2026. Grey literature was collected from official UAE government sources, UAE regulatory and legislative platforms, Digital Dubai sources, and recognized international organizations. A final evidence base of 20 scholarly sources and 12 grey-literature documents was collected.

Findings: The findings demonstrate that privacy risks do not stem from technology alone. They are produced as a result of interactions among digital systems, organizational routines, interpretation of regulations, and external providers. Issues include linkage of data, re-identification, loss of anonymity, opaque artificial intelligence (AI) inferences, excessive access privileges, poor consent models, fragmented governance, cloud vulnerabilities, third-party processing, and reduced public trust. The evidence also reveals that technical measures such as encryption, anonymization, access control, differential privacy, homomorphic encryption, and federated learning are significant but are not enough on their own to ensure privacy.

Unique Contribution to Theory, Practice and Policy: The study demonstrates that risks to privacy are a result of interactions between technologies, people, institutions, rules, and external actors, and thus contributes to Socio-Technical Systems Theory. It also demonstrates the extension of Privacy by Design, highlighting that purely technical measures to store and manage embedded privacy cannot be sufficient without organizational and regulatory support. The four-layer privacy-governance framework it offers is practical and includes technical safeguards, organizational governance, regulatory accountability, and third-party oversight. For policy, it calls for stronger coherence across UAE digital-government, AI, cloud, cybersecurity, and data-protection policies.

Keywords: *Digital Transformation, Privacy Governance, Sensitive Data, Critical Government Organizations, United Arab Emirates*

JEL Classification Codes: *H83, O33, O38, K24, M15*

INTRODUCTION

Digital transformation is much broader than simply transitioning from paper to electronic data processing. It entails the transformation of daily public services, decision-making, the role of institutions, and the accountability of employees using digital technologies and data. Digital government can change the responsiveness of institutions, the continuity of services and access to public services. But as Eom and Lee (2022) explain, while digital transformation can also bring opportunities, it can also reveal vulnerabilities related to organizational capacities, coordination and governance. Haug et al. (2024) also indicate that digitization-induced change impacts organizational structure, jobs and roles, accountability systems, and interactions with people in the service. Therefore, determining the level of digital transformation by simply measuring the availability of a system or its speed is not enough, as the accompanying, though less visible, privacy and governance issues can also be present. This issue is especially urgent now because governments are embedding AI, cloud services, digital identity, and data-sharing platforms into core public services before privacy governance is fully mature.

Cloud computing, artificial intelligence, digital identity and biometric technologies, integrated databases, automated decision-making, and other technologies now allow governments to exchange and process information at an unprecedented level. The Organization for Economic Co-operation and Development (OECD) (2024) identifies risks with these technologies, including the potential for data to be reused, profiled, made through opaque inferences and a fragmented responsibility to regulate. These risks are particularly significant for key governmental entities where the miscommunication or misuse of sensitive information can impact individuals, essential services, the legitimacy of the institution and the public's confidence. Therefore, privacy cannot be a subordinate or secondary issue when it comes to digital transformation projects. The current phase of digital-government expansion therefore creates a narrow policy and implementation window in which privacy safeguards must be embedded before risky practices become routine.

Digitalization does not always conflict with privacy. Integrated platforms can reduce redundant data capturing efforts, enhance and improve data accuracy and boost access monitoring. But getting those benefits does require good governance in regard to technology. Govers and van Amelsvoort (2023) have argued that digital transformation requires technical systems and social arrangements to be considered to be successful. For example, excessive data collection, poorly defined institutional responsibilities, or inappropriate employee privileges cannot be offset by strong encryption. As such, the focus on privacy should consequently be considered as a result of technologies, organization and regulation.

Digital Transformation in the UAE Government Context

The UAE has approached digital government not merely as an information technology project but through a whole-of-government approach. The UAE Government (2024a) states that the UAE Digital Government Strategy 2025 promotes a government that is digital by design, data-driven, proactive, resilient, open, and user-centered. This makes the issue particularly timely because the UAE's digital-by-design direction creates a critical window for embedding privacy safeguards while system architectures, data-sharing practices, and institutional accountability arrangements are still being shaped. The Telecommunications and Digital Government Regulatory Authority (2023) also reports extensive use of UAE Pass, digital-document verification, shared services and application programming interfaces (APIs), and the Government Service Bus. These systems can reduce service fragmentation and administrative

duplication, but they also require high levels of identity verification and system interoperability and involve substantial data movement across organizational boundaries. This makes the UAE an important context for examining privacy because national digital-government ambitions are already linked to identity systems, shared infrastructure, data exchange, and AI-enabled public-service delivery.

The study by Alzarooni et al. (2024) highlights that government support, strategic alignment, and infrastructure investments are key enablers for digital transformation in the public sector of the UAE. They also report, however, that there are some issues related to legacy systems, employee capabilities, cybersecurity and organizational governance. According to their analysis, a high-performance national infrastructure does not automatically address deficiencies in organization implementation. As such, we cannot equate digital maturity at the national level and organizational privacy maturity. A case in point is digital identity. Alhammadi et al. (2024) link the infrastructure for national digital identity with improved access to and integration of Government services. Meanwhile, centralized authentication and identity-linking can lead to increased risks of function expansion, improper data-linking, and improper profiling. Therefore, it is not a question of whether government data should be integrated or not; it is a question of whether this is needed, proportionate, transparent, and accountable throughout the data lifecycle.

Privacy, Sensitive Data, and Critical Government Organizations

Digital transformation was defined in this research as not just the use of software but organizational change with the help of digital technologies. Govers and van Amelsvoort (2023) elaborate that transformation is the establishment of new work structures, new decision-making systems, and new socio-technical relationships. While cybersecurity mainly focuses on safeguarding against unauthorized access, disruption, and attack, information privacy has to do with the collection, processing, sharing, retention, and disposal of information. Although the concepts overlap, OECD (2024) clarifies that they are not synonymous and that a system could be secure yet process too much data or use data for reasons other than those for which it was collected.

Personal, biometric, health, financial, identity, employment, operational, and security-related information were defined as sensitive data because the misuse of such information could cause substantial harm. The definition of critical government organizations was functional and referred to public entities whose disruption or information compromise could have a material impact on essential services, public safety, critical infrastructure, economic stability, and, crucially, government continuity. In this study, the expression critical government organizations was used broadly and was not limited to a single sector, such as healthcare, national security, policing, digital identity, or emergency services. Instead, it referred to any critical public-sector organization whose digital systems process sensitive data and whose disruption or data compromise could produce serious institutional, public-service, or citizen-level consequences. This definition further implied that critical organizations would be subject to a general examination, without having to look at specific ministries or requiring access to classified activities of the organizations. These definitions also informed the research methodology by guiding the inclusion of scholarly and official sources that addressed privacy, sensitive-data processing, digital identity, cloud services, AI governance, data sharing, or privacy risk management in contexts transferable to critical government organizations.

Statement of the Problem

Digital transformation can play a role in increasing government efficiency and making services simpler to use. However, it can also pose privacy risks in addition to hacking and data breaches. This creates a major governance concern for critical government organizations because sensitive data may affect individuals, public trust, service continuity, and institutional legitimacy if it is collected, linked, reused, or shared without adequate safeguards. While data may be originally gathered for proper purposes, such as government administration, government data collection programs expose a potential risk of re-identification, unlawful access, and secondary use, as demonstrated by Barati (2023). Del-Real et al. (2025) also demonstrate how privacy is mostly tackled at the end of a system's design and implementation, yet, for it to work, privacy needs to be integrated into system design and application. A system can therefore be technically secure but privacy-intrusive if it generates excessive data, facilitates opaque data analyses that are typically not expected by the public, or allows data to be used in ways that the public would not generally expect and that may affect individuals' privacy.

The UAE has signed agreements and introduced laws regarding Personal Data Protection, Digital Government, Artificial Intelligence, Cybersecurity, and Cloud Computing. The UAE Government (2025a) defines the national guidelines for protecting the privacy of individuals and the confidentiality of data, and the UAE Government (2024b) states the responsible principles of AI, such as confidentiality and privacy, transparency, accountability, and human oversight. Yet there is no clear evidence in laws or policy statements that they have been consistently understood and implemented in key government bodies. This matters because formal policy commitments may not be enough where digital systems expand faster than institutional capacity, internal accountability, and third-party oversight.

There is also limited and disjointed literature. Most cybersecurity research focuses on threats, most research on digital government is concerned with service performance, and research on the law focuses on formal law. Haug et al. (2024) give an account of the divide between organizational and technological aspects of innovation today, while OECD (2024) illustrates the divide between the governance of the use of AI and data and privacy. This fragmentation complicates the ability to achieve a comprehensive understanding of how technological design, organizational practices and the regulation process lead to issues of privacy. Scholarly publications and government documents were then systematically reviewed and analyzed so as to elicit current evidence and the degree to which the recommended safeguards were simply responses to privacy risks, or whether they were addressing the sources of those risks.

Study Aim and Objectives

The study had the aim of investigating the privacy issues linked to the digital transformation of critical public organizations that handle sensitive data in the UAE. The researcher sought to attain the following objectives:

1. To identify the main privacy challenges associated with digital transformation in UAE critical government organizations.
2. To examine the technological, organizational, and regulatory factors contributing to these challenges.
3. To evaluate privacy-protection measures identified in scholarly and official evidence.

4. To develop an integrated framework for strengthening privacy governance during digital transformation.

Research Questions

The study addressed the following research questions:

1. What privacy challenges are associated with digital transformation in UAE critical government organizations?
2. What technological, organizational, and regulatory factors contribute to these challenges?
3. What privacy-protection measures are identified in scholarly and official evidence?
4. How can privacy governance be strengthened during government digital transformation?

Significance and Contribution of the Study

The study combined research from the literature on digital government, cybersecurity, privacy law and organizational change. There is a need to think beyond implementation and consider organizational change with the new technologies, as well as privacy needs that have to be a core part of the system's design instead of a compliance issue once the technology is implemented, as mentioned by Haug et al. (2024) and Del-Real et al. (2025). These perspectives, along with documents from the UAE government, helped to investigate the disconnect between the policy-level statement of intentions and particular issues raised from the body of evidence. The study also gave a contextually relevant grasp of privacy while at the same time not accessing any confidential organizational practices. It relied on public evidence, academic or official, that was available. This facilitated policy and practice recommendations without the ethical, security and access barriers engendered by investigations on restricted government systems and classified information.

LITERATURE REVIEW

Conceptual Review

It is inaccurate to equate digital transformation with digitization, digitalization, or general organizational transformation. Haug et al. (2024) differentiate the transfer of information into digital form from the wider changes that digitalization creates in organizational structures, roles, and service relationships. Similarly, Govers and van Amelsvoort (2023) explain that transformation occurs when technology changes the design of work, coordination, and decision-making. This study therefore understood digitization as the conversion of information, digitalization as the optimization of processes through digital tools, and digital transformation as the redesign of the overall organization. This distinction is important because privacy exposure does not arise only when records become digital. It also increases when datasets, organizations, and decision systems become increasingly interconnected.

While confidentiality and cybersecurity issues are part of information privacy, these are not the only concerns. Quach et al. (2022) generally describe privacy tensions as what happens when institutional data practices, legal demands, and administrative goals come into conflict with individuals' privacy expectations. Threats of re-identification, poor data anonymization and re-use may even arise from lawful government data projects, as Barati (2023) shows. Data protection is the legal landscape and organizational setting in which personal data processing takes place, and privacy governance also includes systems design, impact assessment,

accountability, decision rights and oversight. OECD (2024) suggests that the use of AI and analytics can reveal sensitive attributes from data that are not sensitive themselves. The risk for privacy can thus be dependent on the nature of the combination, processing and usage of the data.

Digital Transformation in Critical Government Organizations

Key technologies, including cloud computing, artificial intelligence, biometric technologies, interoperable databases, shared platforms, digital identity and analytical tools drive public-sector transformation. Eom and Lee (2022) argue that while these technologies offer both the promise of increasing the adaptiveness of government and responsiveness, they can also run faster than institutional learning and governance capacity. Legacy systems hinder transformation, as data structures, procurement processes, and organizational arrangements are hard to standardize, as pointed out by Irani et al. (2023). Migration can lessen some legacy risks but may cause additional risks to appear, such as double entries, temporary access mechanisms, and vendor relationships, until legacy risks are eliminated.

Ambiguity can be seen in the case of cloud computing. It can provide scalable infrastructure and standardize and centralize government control and security, but it can also cause responsibilities to be shifted among government organizations, cloud providers, subcontractors, and other partners. Cloud security is a national priority for the UAE Government (2025b); however, security alone does not address the privacy issues surrounding location, purpose, vendor access, retention, or secondary use of data. There are comparable dynamics in relation to the use of AI. According to OECD (2024), AI can use information in training and generate sensitive and hard-to-explain inferences. While AI can help public-sector institutions improve prediction and management, it can also widen the information gap between institutions and citizens.

Digital identity poses similar risks. Positive adoption outcomes do not constitute evidence that downstream sharing, retention, or profiling is controlled, as Alhammadi et al. (2024) link UAE digital identity with gains in accessing services. User acceptance could be because of convenience or lack of alternatives, and not because of trust in data governance. Thus, the question is not just whether the digital identity, cloud, or AI systems render better services, but whether they are still necessary and proportionate, transparent and accountable.

Privacy Challenges in Digital Government

The meaning and sensitivity of information may change through integration. Seemingly innocuous datasets can be aggregated to form much richer profiles of an individual, which include ID, geolocation, health, financial or service-use data. As Barati (2023) demonstrates, even when data is supposedly provided as anonymous or non-personal or de-identified, re-identification is possible. Similarly, Verma and Gurtoo (2024) state that policy frameworks for non-personal data are incoherent and that data that appears non-personal may be linked with other data and thus become personal. Therefore, privacy risk is not only present in the original data but can also be generated in the processing, linkage and reuse.

Expansion of purpose and prolonged retention further exacerbate this issue. Long-term retention is facilitated through digital storage, and administrative reuse is more convenient through integrated platforms. According to Quach et al. (2022), there is a conflict between organizational interests and individual control in value creation through data. In governmental service settings, this imbalance is stronger as citizens may rely on required services or may be

legally required to give information. Relying on consent as the primary privacy mechanism is therefore inadequate. Necessity, proportionality, purpose limitation, retention control, and institutional accountability are more appropriate.

Privacy issues with AI include inference, opacity, and automated categorization. There might be a separation of governance of AI and privacy regulation, as the OECD (2024) suggests. Mišić et al. (2025) contend that public-sector AI needs to include privacy, transparency, accountability, equality, and public value, and not simply prioritize prediction. Even if the system is technically correct, it could be found illegitimate when people cannot recognize how the conclusions were drawn, what datasets were merged, or dispute an erroneous conclusion. Compromised biometric identifiers are hard to replace, making the risk of biometric and digital-identity systems even stronger. There is concern about centralized digital identity systems because they raise ethical and privacy issues, while decentralized systems may introduce interoperability and governance complexities, as stated by Alhammadi et al. (2024).

Practices of the organization itself are also crucial. Looking at the way digital technology functions in social and organizational structures, Govers and van Amelsvoort (2023) provide an example. Excessive access, unclear accountability, inadequate oversight, and weak technical controls can create privacy risks. The OECD (2024) also mentions that third-party processing leads to a diffusion of responsibility for vendors, subcontractors, and across-border infrastructure. When public entities cannot provide expert guidance, are not part of the audit, or the technology is not available, contractual obligations might not be sufficient. Therefore, it is essential to have vendor assessment, auditability, restrictions on secondary processing, and verified deletion.

Theoretical Framework

Socio-Technical Systems Theory

Socio-Technical Systems Theory was employed due to its opposition to analyzing technology without the people, structures, and tasks through which it acts. Govers and van Amelsvoort (2023) observe that for a sustainable digital transformation, technical and social systems need to be optimized in combination. Even the most sophisticated authentication systems, encryption, and automated controls are no substitute for unclear accountability, dysfunctional job design, lack of employee skill, or misaligned employee incentives. Further, Haug et al. (2024) demonstrate that digitally induced change redistributes authority and workload across different levels of both individuals and organizations. The theory was appropriate because it enables the study of privacy issues at both the technological and organizational/regulatory boundaries. In the analysis, this theory was used to classify privacy challenges according to how they arise from systems, people, organizational routines, regulatory arrangements, and third-party relationships. However, the theory may be too general, so the present study constrained its application to observable technological, organizational, and regulatory conditions.

Privacy by Design

Privacy by Design provided the foundation for discussing when and how privacy enters the development of digital systems. Four key principles identified by Del-Real et al. (2025) are proactive protection, privacy-preserving defaults, lifecycle protection, transparency, and organizational integration. These principles call into question practices focused on evaluating privacy post-procurement or post-implementation. However, Privacy by Design is not set-and-

forget. All general commitments should be put into effect through procurement needs, system requirements, testing procedures, accountability mechanisms, and measurable controls. When combined with Socio-Technical Systems Theory, Privacy by Design enabled the study to connect institutional context with practical privacy safeguards. In the results and discussion, it was used to assess whether the identified safeguards were preventive, embedded, and lifecycle-based, rather than reactive responses after privacy risks had already emerged.

Empirical Review

From the empirical literature, interoperability can be seen as an administrative convenience as well as a privacy issue. Irani et al. (2023) show how legacy-system complexity is a limitation on public-sector change. Barati (2023) illustrates the impacts of combining public-sector data in ways that compromise anonymization and context. Together, these studies demonstrate that privacy needs to be considered as part of the integration design and not as an afterthought after integration. However, they also show a tension in the literature: digital-government studies often emphasize integration and service efficiency, while privacy-focused studies warn that integration can intensify data linkage, re-identification, and secondary-use risks. Implementation capacity is an issue with cloud and AI studies. Coordinated governance of data ecosystems is supported by the OECD (2024), which also provides high-level guidance for cloud security, including for the UAE government (UAE government 2025b). However, the quality of the top-level structures does not always reflect the level of competency, contractual negotiation and dashboard access of individual organizations to ensure the provider level. Yet another point of disagreement in the literature on AI is between efficiency and public values. While Mišić et al. (2025) and OECD (2024) emphasize the necessity of explainability, allowing ease of access to information is expected to conflict with operational secrecy for critical government organizations. Excess transparency poses potential security concerns, while it may also decrease accountability if it is not adequate. This means that privacy governance in critical government organizations must balance transparency, operational confidentiality, service efficiency, and public accountability rather than treating any one of these goals as sufficient on its own.

The flip side of digital-identity research is that evidence of convenience and adoption is lacking when it comes to privacy protection in the longer term. According to Alhammadi et al. (2024), UAE digital identity has positive relationships with the uptake of services, although they also indicate that it is based on perception and that it is a cross-sectional study, which does not facilitate drawing clear conclusions in relation to causal effects. The study does not reveal users' awareness of downstream organizations sharing the data, and there was no indication that users were prevented from expanding the function. But this is a factor that is broadly apparent in the field of digital government studies: the convenience of having a few or no options other than availing a service is mistaken for trust. Therefore, the empirical evidence should be read cautiously: adoption may indicate usability or necessity, but it does not by itself prove that users understand, accept, or trust downstream data processing. This reinforces the need to synthesize digital-service evidence together with privacy, governance, and accountability evidence.

UAE Legal and Policy Context

The UAE legal system and strategy set high expectations regarding privacy and digital governance. The UAE Government (2025a) outlines national data-protection policies relating to personal-data processing, correction, and protection. Responsible AI principles, such as

privacy, transparency, accountability, and human oversight, are also described by the UAE Government (2024b). These instruments do not explicitly give priority to technological innovation over information privacy. However, written commitments do not necessarily lead to action. In line with the 2030 target of an integrated government, and with the view that a data-driven, digital approach saves lives and protects resources, the Government of the UAE (2024a) offers support for an integrated government with a data-driven approach, and the Telecommunications and Digital Government Regulatory Authority (2023) has revealed that the share of digital infrastructure has increased. The movement of information to these programs requires and relies on interorganizational movement, which must be authorized, auditable, necessary and proportionate.

Responsibilities are also distributed among data protection, AI, cybersecurity, and digital government tools. Where governance requirements are specialized, this distribution can facilitate implementation but can also cause fragmentation where governance requirements are interpreted separately. The question is not, therefore, whether the UAE has policies that relate to privacy, but whether the UAE has consistent privacy governance in key government institutions.

Research Gaps

Based on the literature reviewed, the study identified five gaps. First, privacy is usually viewed as an issue that is subsumed within cybersecurity, even though it is also about collecting, using, and retaining appropriate data. Second, UAE digital-government studies tend to emphasize service performance over privacy governance. Third, technological, organizational, and regulatory aspects are treated independently. Fourth, there is very little evidence of integration between scholarly research, official documents, and literature, providing little comparison between reported dangers and formal protections. Lastly, Privacy by Design is often praised without consideration of the capacity for the organization to manage its implementation. These gaps are the reasons for doing the integrated systematic literature review and documentary analysis.

Conceptual Framework

The conceptual framework connected digital technologies, including cloud-based services, AI, digital identity, biometrics, integrated databases, and automated services, with technological, organizational, regulatory, and third-party conditions. These conditions shape privacy challenges involving data collection, access, sharing, inference, retention, and secondary use. Privacy-governance responses were analyzed through Socio-Technical Systems Theory and Privacy by Design in relation to lawful processing, institutional accountability, public trust, and sustainable digital transformation. Figure 1 below is a depiction of the conceptual framework.

Journal of Public Policy and Administration
ISSN 2520-5315 (Online)
Vol 11, Issue 2, No.3, pp36 - 65, 2026
www.iprjb.org

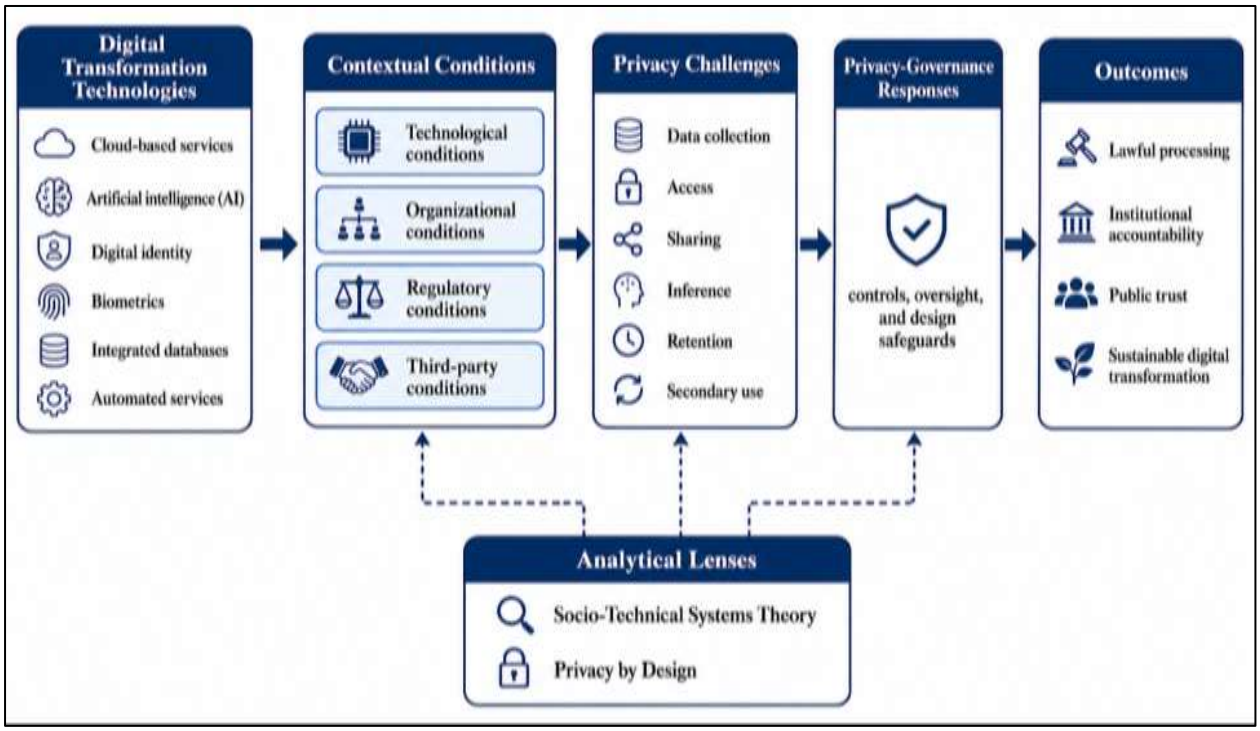


Figure 1: A Depiction of the Conceptual Framework

METHODOLOGY

Research Design

A qualitative systematic literature review and documentary analysis were used in this study. Systematic reviews are reviews using defined research questions with transparent selection and retrieval processes, eligibility criteria, screening, appraisal, review, and synthesis, according to Kolaski et al. (2023). This design was deemed appropriate for the purposes of the study since it was aimed at synthesizing available evidence on privacy issues related to digital transformation and not gathering primary data from government institutions. Documentary analysis was included as there was a need for official documents from the UAE government, UAE regulatory, international institutional, and digital-government sources to understand the policy and governance context. The study was done through secondary sources only. It did not include interviews, surveys, human participants, personal records of any kind, classified materials, or restricted organizational documents.

Sources of Evidence

Two categories of evidence were used. The first category included scholarly evidence collected from Scopus, ScienceDirect and Emerald Insight. Scopus was chosen due to the fact that it covers various fields associated with technology, public administration, information systems, governance and law. ScienceDirect was selected because it is a repository of peer-reviewed research articles in computer science, decision science, information systems, technology and management. Emerald Insight was chosen due to its relevant literature relating to governance, public management, digital transformation, information governance, and organizational change.

The second category was grey literature. The sources used for grey literature included UAE Government official sites, sites with UAE-related regulations and legislation, UAE-related

websites that provided digital-government services and credible international sources. This requirement was necessitated because government policies, data protection guidelines, AI regulations, cloud security policies, and digital-government initiatives are not necessarily found in academic publications. But no official or institutional status was deemed to be a guarantee of effectiveness. Therefore, the grey literature was appraised separately using authority, accuracy, coverage, objectivity, date, and significance (AACODS).

Search Strategy

The aim of the study and the research questions guided the development of the search strategy for the scholarly sources. Digital transformation, privacy, data protection, security, governance and regulation were key themes. The research focused on digital transformation and privacy-related topics to ensure that the majority of the literature retrieved would focus on privacy and privacy governance. Only English-language sources were retrieved from the last seven years (2022-2026). This is the time frame chosen to represent the most recent evidence in the AI, cloud services, digital identity, data governance and digital public-sector transformation fields. Different searches were used for the three databases due to the different syntax and search fields used by the databases. In the Scopus search, the fields chosen were title and abstract. The ScienceDirect search appeared to be the most precise using the title field, as this field is frequently highly descriptive. Since the Emerald Insight search interface was not best equipped to search using the exact syntax used in Scopus, a broader Boolean search structure was devised.

Database Search Queries

The following Scopus query was used:

> *TITLE-ABS(("digital transformation") AND (privacy OR "data privacy" OR "privacy challenge" OR "privacy concern" OR "privacy risk" OR "data protection")) AND PUBYEAR > 2021 AND PUBYEAR < 2027 AND LANGUAGE(English)*

The ScienceDirect query was:

> *Title: ("digital transformation") AND ("data privacy" OR "privacy challenges" OR "data protection") AND (security OR governance OR regulation)*

The Emerald Insight query was entered as:

> *privacy AND (challenges OR problem OR difficulties) AND (digital OR technology)*

Grey Literature Search Strategy

Grey literature searching focused on documents published or updated between 2024 and 2026. The search targeted official UAE government sources, the UAE Legislation Portal, Digital Dubai, UAE digital-government sources, and international institutions such as the OECD, United Nations, and World Bank. Search terms included “digital government privacy,” “data protection laws UAE,” “AI governance UAE,” “cloud security policy UAE,” “digital public infrastructure,” “data governance,” “digital identity,” “AI privacy,” and “government data sharing.” The grey-literature search prioritized UAE-specific sources because the study focused on critical government organizations in the United Arab Emirates. International institutional reports were included only where they provided directly relevant frameworks for digital government, AI governance, data governance, privacy, or digital public infrastructure. Professional and industry sources were not prioritized unless they had direct relevance and could pass stricter appraisal under AACODS.

Eligibility Criteria

Scholarly sources were used based on five criteria.

1. They needed to comply with the following requirements: They needed to be published within the search period between 2022 and 2026.
2. They had to be in English.
3. They had to tackle challenges related to digital transformation or digital technologies, data protection or information privacy, privacy risk or privacy governance.
4. They had to provide sufficient methodological, conceptual, or analytical detail that allows for synthesis.
5. If studies did not explicitly focus on a particular government, then they had to be transferable to critical organizations, sensitive data handling, systems in the public sector, digital identity, cloud services, governance of AI, data sharing, or privacy risk management.

Sources were excluded if they were not within the specified publication period, were written in a language other than English, had no privacy relevance, dealt only with general cybersecurity issues, or were not detailed enough to be assessed and synthesized. Editorials, blogs, magazines, dissertations, theses, abstract-only records, and unverified opinion pieces were excluded.

Grey literature documents were selected where they were publicly available, published or updated between 2024 and 2026, and published by a recognizable government agency, digital-government body, legislative or regulatory platform, or recognized international organization. The eligible documents ranged from strategies, policies, and regulatory guidance to AI-governance frameworks, cloud-security policies, digital-government reports, data-governance initiatives, and digital public infrastructure reports. Documents that were anonymous, promotional, superseded, undated, leaked, or restricted, or those that were only weakly relevant, were excluded.

Screening and Selection Procedure

All retrieved scholarly records were put into a screening spreadsheet. Duplication of records was determined through comparison of titles, authors, publication dates, and digital object identifiers, where available. Records were first screened according to the title and abstract to exclude irrelevant records. The full text of potentially relevant sources was then assessed against the eligibility criteria.

The reasons for exclusion included not addressing privacy aspects, missing methodological details, publication in the wrong source type, no digital-transformation relevance, wrong publication period, or missing full text. AACODS appraisal was not done on grey literature documents until they had been screened first. This screening took into account publication or update year, issuer, public accessibility, type of document, and relevance to the topics of digital transformation, privacy, data protection, AI, cloud services, digital identity, data governance, or public-sector information sharing.

Quality Appraisal

The selected academic papers were examined for clarity of aims, relevance to the research question(s), transparency of methodology, clarity of findings, and contribution to

understanding privacy problems or possible solutions. De Cassai et al. (2025) point out that systematic reviews must have appraisal processes that address the reliability and applicability of the evidence included, not only the gathering of evidence. In this study, sources with stronger methodological or conceptual significance were given more evidential weight in the synthesis process, while weaker sources were used with caution.

AACODS elements were used to appraise grey literature. Landerdahl Stridsberg et al. (2022) support using AACODS for documents with varying authors, institutional purpose, transparency, and review processes. Authority judged the credibility and mandate of the issuing source. Accuracy concerned whether evidence, references, or clear explanations backed up claims. Coverage encompassed the scope and depth of coverage. Objectivity determined the extent of balance and potential institutional bias. Date assessed currency. Significance judged relevance to the research questions. Each AACODS domain was rated as "fully met," "partly met," or "not met," and these ratings determined whether the source was retained as strong evidence, retained with caution, or excluded.

Data Extraction

The data were extracted and organized in matrices. The extraction fields used for scholarly sources were author, year of publication, source type, research focus, privacy issues, security issues, ethical issues, regulatory issues, proposed solutions, key findings, and relevance to the research question. In the case of grey-literature documents, they were recorded using the following fields: issuing body, year, document type, jurisdictional or institutional scope, policy area, relevance to research goals, and AACODS appraisal outcome. These fields made it possible to compare the scholarly and documentary evidence in a consistent way, without assuming that scholarly studies and documentary evidence were equivalent evidence types.

Data Synthesis

Thematic synthesis was carried out on the evidence retrieved. Braun and Clarke (2022) explain that thematic analysis is useful for identifying patterns of meaning across qualitative evidence. The synthesis process in this study started with multiple readings of the extraction matrices, grouping of common privacy issues and technological risks, grouping of organizational issues and regulations, and compilation of proposed safeguards. The coding of evidence was initially done in two categories: officially produced grey-literature evidence and peer-reviewed scholarly evidence. A comparison of the two evidence streams was undertaken to identify converging and diverging aspects and complementary insights. The interpretation was informed by Socio-Technical Systems Theory and Privacy by Design. Socio-Technical Systems Theory was used to analyze privacy risk in technology, people, organization, and regulation. Privacy by Design contributed to the evaluation of safeguards as being preventive, embedded, and lifecycle-based rather than reactive.

Rigor and Transparency

A structured approach of defined search questions, search process by the different databases, documented eligibility criteria, removal of duplicates, title and abstract screening, full text screening, quality appraisal, and structured data extraction added rigor and transparency to the process. A search log and matrix of extraction were maintained to provide transparency. Triangulation was achieved through comparison of what was found in scholarly evidence and what was found in official/institutional documents. Caution was, however, used when trying to propose agreement between the categories of evidence since official documents indicate

outcomes of policy intent and not necessarily independently verified outcomes of policy implementation.

Ethical Considerations

Only secondary evidence, which was publicly available, was used for the study. No human participants were recruited, and no personal, classified, leaked, restricted or illegal information was collected. The study did not report on technical aspects that would reveal vulnerable aspects of government systems. All sources were represented accurately and cited appropriately.

RESULTS AND DISCUSSION

Search and Selection Results

The study selection process followed the PRISMA 2020 guidelines. A total of 2,949 records were identified from three databases: Scopus (n = 1,559), ScienceDirect (n = 776), and Emerald Insight (n = 614). During the identification stage, 633 duplicate records and 26 records removed for other reasons were excluded, resulting in 2,290 records for title and abstract screening. Following the screening process, 1,346 records were excluded based on relevance, leaving 944 records for retrieval. Of these, 16 reports could not be retrieved, and 928 full-text articles were assessed for eligibility. During the eligibility assessment, 850 studies were excluded for various reasons, including not being focused on privacy challenges (n = 156), lack of full-text availability (n = 110), being outside the scope of the review (n = 274), or addressing challenges not aligned with the study objectives (n = 310). Lastly, 20 studies met all inclusion criteria and were included in the final systematic literature review. The PRISMA diagram in Figure 2 below provides a summary of the search and selection process, while Table 1 presents the 20 scholarly sources retained for synthesis, and Table 2 presents the 12 grey-literature sources retained for documentary analysis.

Journal of Public Policy and Administration
ISSN 2520-5315 (Online)
Vol 11, Issue 2, No.3, pp36 - 65, 2026
www.iprjb.org

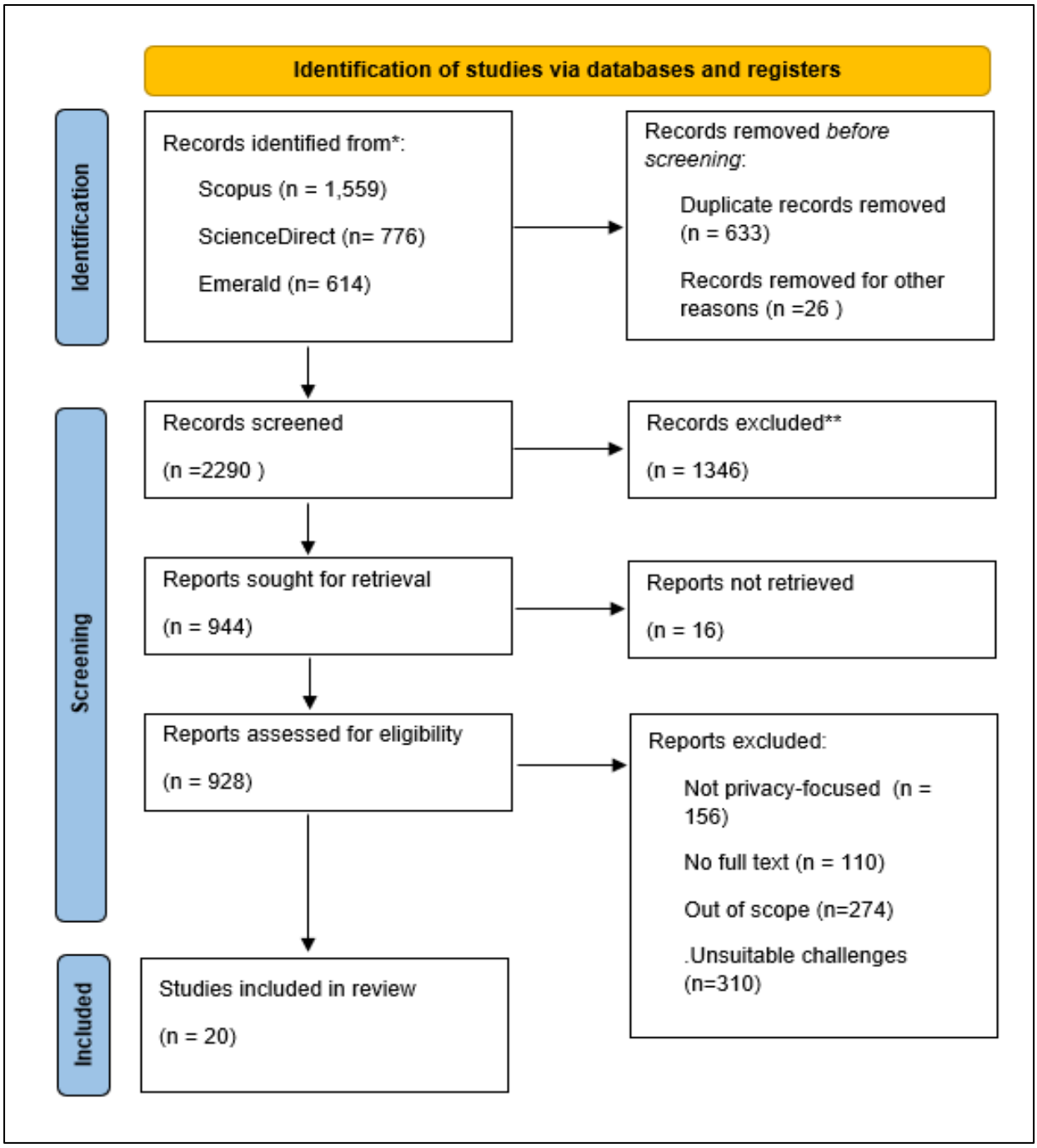


Figure 2: PRISMA Diagram

Journal of Public Policy and Administration
ISSN 2520-5315 (Online)
Vol 11, Issue 2, No.3, pp36 - 65, 2026
www.iprjb.org

Table 1: Summary of Scholarly Sources Included in the Review

No.	Author(s)	Year	Research focus	Main relevance to the study
1	Tukur et al.	2023	Metaverse digital environments	Identifies privacy threats, data-management threats, loss of anonymity, regulatory concerns, and privacy-preserving technologies.
2	Saleha et al.	2026	Online child sexual exploitation prevention	Highlights the privacy-versus-surveillance dilemma, consent issues, cybersecurity threats, reporting weaknesses, and digital literacy.
3	Misra et al.	2025	Digital sovereignty and trust	Links data privacy, AI governance, cross-border trust, fragmented governance, and privacy-enhancing technologies.
4	Kuštelega et al.	2024	Digital twin technologies	Identifies data sensitivity, ownership, access-control vulnerabilities, legal concerns, and data-governance needs.
5	Kolaventi et al.	2024	Cloud-based health informatics	Addresses confidentiality, anonymization, unauthorized access, cloud vulnerabilities, consent, and governance models.
6	Kim	2025	AI digital textbooks and fog computing	Shows cloud privacy concerns and the potential of fog and edge computing for better privacy and efficiency.
7	Ikumapayi et al.	2025	Digital transformation systems	Identifies data breaches, inadequate encryption, IoT vulnerabilities, insider threats, training gaps, and security controls.
8	Chomanski and Lauwaert	2025	Digital privacy regulation	Discusses privacy rights, regulatory capture, democratic accountability, and the responsiveness of privacy regulation.
9	Chomanski	2025	Privacy regulation models	Critiques consent and privacy self-management and proposes alternative regulatory approaches.
10	Banaeian Far and Imani Rad	2022	Digital twins and metaverse	Discusses anonymity, ownership privacy, identity management, government monitoring, blockchain, and zero-knowledge technologies.
11	Alcántara et al.	2024	Digital identity and avatars	Addresses surveillance, data collection, identity theft, deepfakes, avatar cloning, and avatar-specific regulation.
12	Zhou	2025	Cybersecurity and privacy protection	Links data exploitation, privacy violations, malware, phishing, legal frameworks, and privacy-preserving technologies.
13	Vera-Arenas	2025	Human digital twins and blockchain	Examines consent management, data minimization, GDPR compliance, decentralized identifiers, and privacy by design.
14	Song et al.	2025	Privacy attacks and countermeasures	Identifies reconstruction, inference, extraction, and linkage attacks in data and machine-learning systems.
15	Krishna et al.	2025	AI and blockchain in healthcare	Addresses confidentiality, dynamic consent, fairness, transparency, federated learning, homomorphic encryption, and explainable AI.
16	He et al.	2023	Vehicular digital twin networks	Highlights location privacy, behavior inference, cyberattacks, reliability concerns, blockchain, and differential privacy.
17	Brown et al.	2026	Older adults and e-government	Shows privacy concerns, lack of trust, cyber awareness, cybercrime exposure, and digital inclusion issues in e-government.
18	Bansod and Ragha	2022	Blockchain privacy and security	Discusses identity privacy, transaction linkability, blockchain vulnerabilities, GDPR compliance, and cryptographic safeguards.
19	Alhazmi	2025	Smart healthcare during Hajj and Umrah	Addresses data processing, anonymization, unauthorized access, PDPL compliance, privacy audits, and granular controls.
20	Ahmadon et al.	2025	Digital privacy trends and future directions	Supports a holistic technical, legal, and social approach to digital privacy.

Table 2: Summary of Grey-Literature Sources Included in the Documentary Analysis

No.	Grey-literature source	Year	Issuing body	Document type	Main relevance to the study
1	UAE Digital Government Strategy 2025	2024	UAE Government	National digital-government strategy	Establishes the UAE's digital-by-design, data-driven, proactive, resilient, open, and user-centered government direction.
2	Overseeing Digital Transformation in the UAE	2024	UAE Government / TDRA	Official governance guidance	Explains institutional responsibility for digital-transformation strategies, policies, legislation, and projects.
3	Data Protection Laws	2025	UAE Government	Regulatory guidance	Provides official explanation of personal data protection, confidentiality, privacy protection, and data processing obligations.
4	UAE Charter for the Development and Use of Artificial Intelligence	2024	UAE Legislation Portal	AI governance charter	Provides principles for responsible AI development and use, including governance, accountability, and community protection.
5	Artificial Intelligence in Government Policies	2025	UAE Government	AI policy guidance	Explains AI use in government policy and emphasizes data privacy in government AI adoption.
6	Dubai State of AI Report	2025	Digital Dubai / Dubai Future Foundation	Government AI report	Provides evidence of AI adoption trends across the Dubai government.
7	AI Integration Matrix Framework for Government Organizations	2026	Digital Dubai	Government AI framework	Provides a framework for structured AI adoption, maturity, implementation, and technical architecture.
8	Digital Dubai Data Quality Initiative	2024	Digital Dubai	Data-governance initiative	Addresses data quality, accessibility, and governance as foundations for AI and digital-government operations.
9	Dubai Data and Artificial Intelligence Platform	2024	Digital Dubai	Data and AI platform announcement	Describes a unified platform for official data, data hosting, data exchange, and AI-supported analysis.
10	UN E-Government Survey 2024	2024	United Nations DESA	International institutional report	Provides global digital-government benchmarking and comparative context.
11	AI, Data Governance and Privacy	2024	OECD	International policy report	Addresses privacy risks and opportunities arising from AI and links AI principles with privacy principles.
12	Digital Public Infrastructure and Development	2025	World Bank	International institutional report	Provides a framework for digital identity, data sharing, safeguards, and digital public infrastructure.

Characteristics and Appraisal of the Evidence

The 20 scholarly sources covered the period 2022 to 2026, with most sources published between 2024 and 2026. This demonstrates that the review was up to date and included recent advancements in the areas of AI, cloud computing, digital identity, blockchain and digital twins, privacy legislation and e-government. The sources varied in direct relevance to the UAE's critical government organizations. Brown et al. (2026), Chomanski (2025), Chomanski & Lauwaert (2025), Misra et al. (2025), and Ahmadon et al. (2025) were particularly important as they viewed privacy not merely as a technical security problem. Other sources were translatable and not government-specific. Tukur et al. (2023), Banaeian Far and Imani Rad (2022), Kuštelega et al. (2024), Alcántara et al. (2024), and Vera-Arenas (2025) only considered metaverse systems, digital twins, avatars, and human digital twins. These studies

Journal of Public Policy and Administration
ISSN 2520-5315 (Online)
Vol 11, Issue 2, No.3, pp36 - 65, 2026
www.iprjb.org

were retained as they included the issues of identity, ownership, anonymity, surveillance, consent, and data minimization. While their findings were not necessarily considered to be an explicit indication of government risk in the UAE, they provided useful information to direct the identification of privacy mechanisms important to critical organizations that process sensitive information.

The grey literature appraisal showed that the 12 retained documents were generally strong. As shown in Table 3, nine sources were classified as high quality, and three were classified as moderate quality under AACODS. The UN, OECD, and World Bank sources scored highest because they had strong authority, coverage, objectivity, data, and significance. Sources from the UAE government and the UAE Legislation Portal were also very relevant, but these represented evidence of the policy expectations, not necessarily evidence of successful implementation.

Table 3: AACODS Appraisal of Grey-Literature Sources

No.	Source	Authority	Accuracy	Coverage	Objectivity	Date	Significance	Total /12	Classification	Decision
1	UAE Digital Government Strategy 2025	2	2	2	1	2	2	11	High	Include
2	Overseeing Digital Transformation in the UAE	2	1	1	1	2	2	9	Moderate	Include with caution
3	Data Protection Laws	2	2	2	1	2	2	11	High	Include
4	UAE Charter for the Development and Use of Artificial Intelligence	2	2	2	1	2	2	11	High	Include
5	Artificial Intelligence in Government Policies	2	1	2	1	2	2	10	High	Include
6	Dubai State of AI Report	2	1	2	1	2	2	10	High	Include
7	AI Integration Matrix Framework for Government Organizations	2	2	2	1	2	2	11	High	Include
8	Digital Dubai Data Quality Initiative	2	1	1	1	2	2	9	Moderate	Include with caution
9	Dubai Data and Artificial Intelligence Platform	2	1	1	1	2	2	9	Moderate	Include with caution
10	UN E-Government Survey 2024	2	2	2	2	2	2	12	High	Include
11	OECD: AI, Data Governance and Privacy	2	2	2	2	2	2	12	High	Include
12	World Bank: Digital Public Infrastructure and Development	2	2	2	2	2	2	12	High	Include

Technological Privacy Challenges

These findings indicate that digital transformation amplifies another critical issue – privacy risk – by expanding the extent, connectivity, and value of data. The key themes emerging from the evidence in the scholarly and grey literature are summarized in Table 4. Tukur et al. (2023) suggest that privacy threats, data management threats, and loss of anonymity are the primary threats in metaverse digital environments. Data sensitivity, ownership, and data-management challenges in digital twin technologies are also addressed by Kuštelega et al. (2024). The privacy and security issues of user anonymity, authentication, identity management, and decentralized governance are still central in digital twins and metaverse systems, as shown by Banaeian Far and Imani Rad (2022). These findings can be translated to critical government organizations, as such organizations rely on increasingly interconnected systems, where people, assets, services, and behavior can be linked.

A second critical technological challenge was AI and machine-learning systems. Misra et al. (2025) show that privacy and AI governance take center stage in digital sovereignty discussions, particularly in relation to fragmented governance, AI-driven attacks, and cross-border trust. According to Song et al. (2025), attacks on data and machine-learning systems remain a persistent challenge, particularly regarding reconstruction, inference, extraction, and linkage attacks.

Sensitive inference is important, as it is possible that data might not necessarily be sensitive but could turn out to be so once processed or combined with other data. However, in critical government organizations, the risk of privacy is not restricted to prediction, profiling and automated categorisation but can be found in how these systems gain access to data.

Cloud and platform-based systems presented major problems as well. In cloud health informatics, confidentiality, anonymization, unauthorized access, ownership disputes, data breaches, and vulnerabilities in cloud systems have been identified as challenges by Kolaventi et al. (2024). Kim (2025) demonstrates that privacy can be an issue with cloud-only approaches and that the use of fog and edge computing can be helpful in terms of privacy and efficiency. The point is that the adoption of cloud systems is not merely a scalability, cost, or security performance choice. Key areas that should be addressed include location of data, access for vendors, retention, processing of data after its intended use, and auditability.

Table 4: Thematic Summary of Key Findings

Theme	Main finding	Supporting scholarly sources	Supporting grey-literature sources
Technological privacy risks	Digital systems increase privacy exposure through linkage, inference, data sensitivity, access vulnerabilities, and cloud dependence.	Tukur et al.; Kuštelega et al.; Misra et al.; Kolaventi et al.; Kim; Song et al.	UAE Digital Government Strategy 2025; OECD AI, Data Governance and Privacy; World Bank Digital Public Infrastructure and Development
Organizational privacy risks	Weak training, excessive access, unclear accountability, low trust, and weak governance routines increase privacy risk.	Ikumapayi et al.; Brown et al.; Ahmadon et al.	Overseeing Digital Transformation in the UAE; Digital Dubai Data Quality Initiative
Ethical and regulatory risks	Consent, surveillance, fragmented governance, digital sovereignty, and accountability remain major issues.	Chomanski; Chomanski and Lauwaert; Saleha et al.; Misra et al.; Alhazmi	Data Protection Laws; UAE AI Charter; OECD AI, Data Governance and Privacy
Third-party and data-sharing risks	Cloud, AI, blockchain, vendors, and distributed systems disperse responsibility and increase linkage, transfer, and secondary-use risks.	Kolaventi et al.; Zhou; Bansod and Ragha; Vera-Arenas; Song et al.	National/Digital Government sources; Dubai Data and AI Platform; World Bank Digital Public Infrastructure and Development
Privacy-protection measures	Technical safeguards must be combined with governance, privacy audits, training, legal oversight, and lifecycle controls.	Zhou; Song et al.; Krishna et al.; Bansod and Ragha; Alhazmi; Ahmadon et al.	UAE AI Charter; AI Integration Matrix Framework; OECD AI, Data Governance and Privacy

Organizational Privacy Challenges

The evidence suggests that privacy issues are also organizational. Ikumapayi et al. (2025) identify data breaches, inadequate encryption, vulnerabilities in IoT, malware such as ransomware, insider threats, regulatory gaps, and employee training as threats in digital transformation systems. Although this evidence has a cybersecurity focus, it shows that weak training practices, poor access controls, limited internal accountability, and weak governance routines can increase privacy exposure. Therefore, technology and the individual employees are not the only reasons for privacy mistakes to occur, but roles may be poorly designed, access privileges may be excessive, and there may be a lack of responsibility. Brown et al. (2026) indicate that privacy issues and mistrust are still a hindrance to technology uptake towards e-governance, especially for older people. Such a discovery is relevant since the digital transformation in the public sector is dependent on citizens' trust. Even if systems have technically proven viability, if use is perceived as a loss of personal control, as intrusive observation, or as fraud and misuse, they might not be adopted or used as they should be. Therefore, privacy governance is not just on the compliance horizon; it is a key part of public trust and institutional legitimacy.

Organizational weaknesses were also found in consent and privacy self-management. Chomanski (2025) argues that consent-centric approaches to privacy are still underdeveloped, and Chomanski and Lauwaert (2025) argue that digital privacy laws and policies may not be as citizen-centric as they might need to be. The findings are relevant to public organizations, especially because it is not possible to deny a public service or negotiate the terms for using data. In critical governmental institutions, necessity, proportionality, purpose limitation, oversight and institutional accountability are thus required and cannot be replaced by relying on consent alone.

Ethical and Regulatory Challenges

The results reveal a relationship between privacy issues and ethical/regulatory issues. The key issues pointed out by Misra et al. (2025) are GDPR, the AI Act, fragmented governance, and digital sovereignty. Chomanski and Lauwaert (2025) highlight democratic accountability, and Chomanski (2025) casts doubt on notice-and-consent practices. Together, these sources illustrate that regulation is not only a matter of formal legal instruments. The far greater issue is whether legal and policy structures ensure enforceable accountability and are sufficiently robust to curb excessive data use. Saleha et al. (2026) identify the challenge between privacy and surveillance in the prevention of child sexual exploitation online. The context is not exactly that of the UAE Government's transformation, but the ethical tension may be transferable. Even for legitimate protection, administration, or public interest, critical government bodies might use sensitive data, but this can become disproportionate if such use is extended beyond the bounds of what is necessary.

Healthcare-specific sources and stakeholders reinforce context-sensitive regulation. Kolaventi et al. (2024) discuss HIPAA, GDPR, consent, and governance models in cloud-based health informatics. Krishna et al. (2025) highlight that fairness, transparency, confidentiality, dynamic consent, and compliance are key factors in AI and blockchain in healthcare. Alhazmi (2025) emphasizes compliance with PDPL in smart healthcare at the time of Hajj and Umrah, as well as cultural privacy expectations. Based on these sources, it is important to understand that sensitive-data governance can only be legally, technically, and culturally appropriate when contextual factors are considered. These concerns are seen to be relevant for the UAE according to the grey literature. UAE Government sources establish policy expectations regarding digital government, personal-data protection, responsible AI, and cloud security. The instances of digital transformation in Dubai, sourced from Digital Dubai, show how AI is being adopted, data quality efforts, and government data platforms. But many of these sources only provide a formal direction of policy. They do not themselves check that measures are being adopted in a consistent manner in key government institutions.

Third-Party and Data-Sharing Risks

Evidence identified risks of third-party and data sharing. Cloud providers, software suppliers, AI vendors, platform operators, external processors, and anyone else dealing with sensitive data can be part of the sensitive-data environment. For Kolaventi et al. (2024), the challenges encompass unauthorized access and cloud vulnerabilities, alongside the complementary claims of Zhou (2025) that both legal and technical means need to work together when it comes to privacy protection. This means contracts should be effective, along with the technical controls and governance procedures. Distributed systems can also create accountability challenges. According to Bansod and Ragha (2022), some of the challenges involved are compliance, vulnerabilities of blockchains, interoperability and identity privacy, and transaction linkability. The potential application of self-sovereign identities, smart contracts, and decentralized identifiers to improve privacy in human digital twins is not guaranteed to succeed because their effectiveness depends on governance and design, as Vera-Arenas (2025) shows. The results indicate that while shared platforms and distributed technologies hold the power to increase control in certain areas, they can cause new dilemmas in relation to accountability in other areas. There are extra risks of linkage, re-identification, and secondary use with data sharing. Tukur et al. (2023) identify data-management risks and loss of anonymity, while Song et al. (2025) emphasize linkage and inference attacks. This means that for critical government

organizations in the UAE, interagency data sharing and vendor layers of processing will have to, at a minimum, be necessary, proportionate, authorized, auditable, and for a defined purpose.

Privacy-Protection Measures

The reviewed evidence shows several types of technical interventions. Zhou (2025) suggests using differential privacy, homomorphic encryption, and multi-factor authentication. As countermeasures to machine-learning privacy attacks, differential privacy and knowledge distillation are mentioned by Song et al. (2025). In healthcare-related AI and blockchain systems, federated learning, homomorphic encryption, and explainable AI are highlighted by Krishna et al. (2025). Bansod and Ragha (2022) list blockchain privacy measures such as zero-knowledge proofs, secure multiparty computation, ring signatures, and homomorphic encryption. These technologies can play a significant role in minimizing privacy exposure, but they are not a substitute for governance.

This was also the case for safeguards in terms of governance. Good governance is needed for digital health systems, as demonstrated by Kolaventi et al. (2024). Alhazmi (2025) suggests privacy audits and more specific privacy controls. Ahmadon et al. (2025) state that digital privacy should be addressed on technical, legal, and social levels. This helps to validate the use of Socio-Technical Systems Theory and Privacy by Design in the study, as the evidence clearly indicates that privacy needs to be integrated into the design of the system, the practice of the organization, legal aspects, and continuous oversight. Awareness and trust are also important. Saleha et al. (2026) highlight the importance of digital literacy, and Brown et al. (2026) claim that digital literacy, as well as cybersecurity awareness, is pertinent for e-government trust. However, for critical government bodies, awareness should be built upon institutional responsibility and not increase the burden on citizens to protect privacy. Still, organizations have to minimize data collection, limit data access, explain data processing, monitor data use, and be responsible for it.

4.8 Integrated Interpretation

The results indicate a four-level privacy-governance framework – technological safeguards, organizational governance, regulatory accountability, and third-party oversight – that should be integrated. The technology layer refers to secure architecture, audit logs, privacy-preserving analytics, anonymization, authentication, and encryption. The organizational layer includes training and other elements, including role clarity, access governance, data classification, retention control, privacy impact assessment, and internal accountability. The regulatory layer covers aspects like lawful processing, proportionality, transparency, purpose limitation, AI governance, cloud governance, and compliance monitoring. The third-party layer covers vendor due diligence, contractual protections, audit rights, data-transfer controls, and deletion guarantees, among other items.

Overall, technology is not to blame for the privacy challenges in digital transformation. Such risks are generated through the interplay of technologies, organizational practices, legal duties, and external actors. This is in accord with the study's theoretical framework. Socio-Technical Systems Theory can help with the understanding that privacy needs to be addressed at the systems, people, organization, and rules level. Privacy by Design also clarifies the need for preventive, embedded, and lifecycle-based protection, as opposed to reactive protection. It is therefore necessary for successful privacy governance that sensitive data are under ongoing

control for UAE critical government organizations in terms of how they are collected, accessed, shared, inferred, retained, and reused.

SUMMARY, CONCLUSION AND RECOMMENDATIONS

Summary

The focus of this study was to explore privacy issues in the process of digital transformation among critical government organizations in the UAE that handle sensitive data. Results indicate that privacy threats are not created by technology alone. Rather, they result from technological design, organizational practice, regulatory interpretation, and involvement of third parties.

The first objective was to determine the major privacy issues. Weak data consent, re-identification, loss of anonymity, unauthorized data access, inference attacks, and linkage attacks are challenges identified by Tukur et al. (2023), Alcántara et al. (2024), Song et al. (2025), and Brown et al. (2026). These findings were relevant because critical government organizations process ID-rich and sensitive information whose misuse could impact both individuals and the legitimacy and operation of public-service organizations. The second objective was to investigate associated factors. AI-enhanced inference and cloud vulnerabilities increase technological risk, as shown by Kolaventi et al. (2024), Misra et al. (2025), and Song et al. (2025). According to Ikumapayi et al. (2025), Brown et al. (2026), Chomanski (2025), and Chomanski and Lauwaert (2025), the lack of training, lack of controls, excessive access, unclear accountability, low level of trust in e-government, and pockets of governance are also factors increasing exposure.

The third objective was to evaluate privacy-protection measures. Various technical measures can be applied to these contexts, including encryption, anonymization, multi-factor authentication, differential privacy, homomorphic encryption, federated learning, explainable AI, zero-knowledge proofs, and secure multiparty computation as identified by Bansod and Ragha (2022), Zhou (2025), Krishna et al. (2025), and Song et al. (2025). Nevertheless, research by Alhazmi (2025) and Ahmadon et al. (2025) reveals that such measures are not without challenges, as they necessitate privacy audits, fine-grained controls, user awareness, legal clarity, and institutional accountability. Similarly, UAE Government (2024a, 2024b, 2025a), Digital Dubai (2025), and OECD (2024) have pointed to the significance of responsible AI, data protection, cloud security, and digital-government governance. The fourth objective was the development of an integrated framework. The results confirm four layers dependent on each other: technical protections, organizational governance, regulatory accountability, and third-party oversight. This is congruent with Socio-Technical Systems Theory in that privacy outcomes are dependent on systems, people, structures, rules, and external actors. Additionally, it is a reflection of Privacy by Design, which means privacy must be built into systems before the technology is implemented.

Conclusion

The findings of the study are summarized as follows: privacy issues arising in critical government organizations in the context of digital transformation are not only narrow cybersecurity issues but are also socio-technical governance issues. However, the use of security measures like encryption, authentication, firewalls, and access controls is not sufficient to address more general privacy risks relating to collection, necessary use, retention, access, re-use, and understanding and challenging of processing. Strong commitments to digital

transformation at the national and emirate levels support digital transformation in the United Arab Emirates. Data protection and privacy, AI accountability, responsible AI, and digital-by-design government are emphasized in the UAE Government's (2024a, 2024b, 2025a) sources. Digital Dubai (2024a, 2024b, 2025, 2026) also indicates progress on the adoption of AI, data platforms, and data-quality initiatives. Official policy evidence is, however, largely evidence of institutional direction and formal commitment and not independent evidence of consistency of implementation. The bottom line on the research question is that an integrated approach that combines technology, organization, regulation, and third parties is needed to strengthen privacy governance. Focusing only on cybersecurity would be limited, and focusing only on compliance would be too formalistic. Digital transformation needs to be sustainable and underpinned by governance of the collection, access, sharing, inference, holding, and re-use of sensitive data.

Recommendations for Practice

Privacy by Design should be mandated in the design of digital transformation systems within critical government organizations, both during planning and procurement, system design and testing, deployment, and post-implementation review. Song et al. (2025) and Ahmadon et al. (2025) demonstrate that privacy risks are exposed when systems gather more data than necessary, make opaque inferences, or allow secondary uses. Responsible AI, privacy protection, and trustworthy digital government are also supported by the UAE Government (2024b, 2025a) and OECD (2024). There is an urgent need for enhanced approaches to privacy impact assessment for high-impact technologies, particularly AI, biometrics, digital identity, integrated databases, digital twins, and cloud-based services. These checks must look at data minimization, limitation of purposes, proportionality, risk of inference, retention, access rights, vendor participation, and public trust. The notion of "proactive governance" is supported by Alcántara et al. (2024), Song et al. (2025), UAE Government (2024a, 2024b), and Digital Dubai (2026) because identity-related and machine-learning systems can increase the risks of surveillance, extraction, inference, and linkage.

Access governance should be improved through role-based access, least privilege controls, access review, audit trails, and some level of accountability for employees and contractors accessing sensitive information. Ikumapayi et al. (2025) recognize digital transformation risks such as insider threat, lack of encryption, gaps in workforce training, and poor controls. Data minimization and retention controls should also be reinforced since Tukur et al. (2023), Kuštelega et al. (2024), and Vera-Arenas (2025) indicate that the issues of anonymity, ownership, consent, and data-management challenges become more severe in integrated environments. Governance by third parties should be an integral part of the privacy function. Limitations on secondary use, verified deletion, audit rights, contractual privacy controls, data-transfer restrictions, and due diligence of cloud providers, AI vendors, software suppliers, platform operators, and external processors are all important mechanisms for controlling privacy. The risks of cloud computing, distributed computing, and blockchain-based systems are identified as risks for confidentiality, ownership, identity privacy, transaction linkage, and interoperability by Kolaventi et al. (2024) and Bansod and Ragha (2022). Employee training and privacy culture should also be invested in among critical government organizations, as demonstrated by the findings of this study and other studies conducted by Brown et al. (2026) and Saleha et al. (2026), which show that awareness and digital literacy impact trust and digital safety.

Recommendations for Policy

Digital government, AI, cloud, cybersecurity, and data-protection policies and strategies should be aligned in the UAE. Misra et al. (2025) and Chomanski and Lauwaert (2025) both demonstrate how AI systems, cloud services, integrated platforms, as well as third-party agents and providers, can bring about fragmented forms of governance that reduce accountability. A unified privacy-governance framework would help achieve uniformity in how agencies, systems, and technology providers interpret privacy laws. Mandatory Privacy Impact Assessments should be required for high-risk technologies in the public sector, such as AI, biometrics, digital identity, integrated data platforms, digital twins, cloud migration, and automated decision-making. Chomanski (2025), Song et al. (2025), and OECD (2024) demonstrate that technical systems can be secure and still privacy-invasive, and that connections should be made between AI governance, data governance, and privacy. There is a need to have clearer public-sector rules about data-sharing, which should also be strengthened. According to Digital Dubai (2024a, 2024b), the relevance of using government data exchange and analysis with AI is increasing. But with more integration comes a greater need for purpose limitation, access monitoring, and accountability. Data sharing should be necessary, proportionate, authorized, auditable, and limited to defined purposes.

Obligations should be further improved for third parties supporting critical public-sector functions in cloud, AI, and platforms. When involving external providers, the concept of 'privacy responsibility' gets complicated, as seen in the works of Kolaventi et al. (2024), Bansod and Ragha (2022), and Zhou (2025). Key considerations include audit capabilities, certification, breach notifications, limits on secondary uses, controls on data transferred, and data-deletion verifications. However, the role of consent in the processing of government data must also be diminished through policy. According to Chomanski (2025) and Chomanski and Lauwaert (2025), in situations where individuals rely on public services, privacy, self-management and notice-and-consent are inadequate. It is therefore recommended that necessity, proportionality, transparency, accountability, and independent oversight of critical government organizations are given greater importance in the UAE.

Proposed Integrated Privacy-Governance Framework

The proposed framework consists of four levels. The technological layer includes encryption, authentication, access controls, anonymization, audit logs, differential privacy, homomorphic encryption, federated learning, secure architecture, and privacy-preserving analytics. These measures decrease technical exposure and should be governed, as demonstrated by Zhou (2025), Song et al. (2025), and Krishna et al. (2025). The organizational layer refers to aspects such as privacy impact assessments, staff training, access governance, data classification, retention control, measures for internal accountability, and privacy culture. Awareness, trust, and governance play a major role in privacy protection, as reflected in the studies of Ikumapayi et al. (2025), Brown et al. (2026), and Ahmadon et al. (2025). The regulatory aspects include lawful processing, transparency, purpose limitation, proportionality, AI governance, cloud governance, and compliance monitoring. Formal rules need to be coupled with meaningful accountability, as revealed by Chomanski (2025), Chomanski and Lauwaert (2025), and the OECD (2024). The third-party layer includes vendor due diligence, contractual controls, audit rights, data-transfer safeguards, deletion verifications, and monitoring. According to Kolaventi et al. (2024), Bansod and Ragha (2022), and Digital Dubai (2024b), cloud, AI, blockchain, and

Journal of Public Policy and Administration
ISSN 2520-5315 (Online)
Vol 11, Issue 2, No.3, pp36 - 65, 2026
www.iprjb.org

platform-based systems distribute responsibility for data handling. Figure 3 below provides a summary of the proposed integrated privacy-governance framework.

Figure 3: Proposed Integrated Privacy-Governance Framework

Contribution to Theory

The study contributes to Socio-Technical Systems Theory by showing that privacy risks emerge from interactions among technological systems, organizational structures, regulatory frameworks, and third-party ecosystems. It also contributes to Privacy by Design by showing that design principles require organizational and regulatory support. Ahmadon et al. (2025), Zhou (2025), and OECD (2024) show that technical privacy measures require legal, social, and organizational support.

Limitations and Future Research

The study relied on secondary evidence drawn from scholarly sources and grey literature. It did not involve interviews, surveys, internal UAE government records, classified documents, or direct observation of UAE critical government organizations. Therefore, it is not able to ensure implementation within specific organizations. Some of the literature was not UAE-specific, and there was no UAE-specific grey literature as an independent source of information about the effectiveness of implementation. Future study is needed on privacy governance in specific public-sector domains of the UAE, including health, identity management, transport, emergency services, smart-city infrastructure, and digital public infrastructure. Comparative Gulf research would also be helpful. Further research is needed to look into the functioning of privacy impact assessments, AI governance measures, vendor review, and data-sharing regulations.

REFERENCES

Ahmadon, M. A., Napp, N., Rao, S., Silva, C., Lizar, M., Gorog, C., Lu, G., Hawkins, S.-K., & Zanero, S. (2025). Digital privacy: Trends, challenges, and the future. *IT Professional, 27*(3), 69–77. https://doi.org/10.1109/MITP.2025.3546433

Alcántara, J. C., Tasic, I., & Cano, M. (2024). Enhancing digital identity: Evaluating avatar creation tools and privacy challenges for the metaverse. *Information, 15*(10), 624. https://doi.org/10.3390/info15100624

Alhammadi, A. A., Alhashmi, S. M., Lataifeh, M., & Rice, J. L. (2024). The influence of national digital identities and national profiling systems on accelerating the processes of digital transformation: A mixed study report. *Computers, 13*(9), 243. https://doi.org/10.3390/computers13090243

Alhazmi, A. (2025). Privacy in smart digital healthcare during Hajj and Umrah: Challenges and recommendations. In *2025 2nd International Conference on Advanced Innovations in Smart Cities (ICAISC)* (pp. 1–7). https://doi.org/10.1109/ICAISC64594.2025.10959406

Alzarooni, A. I., Alhashmi, S. M., Lataifeh, M., & Rice, J. (2024). Navigating digital transformation in the UAE: Benefits, challenges, and future directions in the public sector. *Computers, 13*(11), 281. https://doi.org/10.3390/computers13110281

Banaeian Far, S., & Imani Rad, A. (2022). Applying digital twins in the metaverse: User interface, security and privacy challenges. *Journal of Metaverse, 2*(1), 8–15. https://dergipark.org.tr/en/pub/jmv/issue/67967/1072189

Bansod, S., & Ragha, L. (2022). Challenges in making blockchain privacy compliant for the digital world: Some measures. *Sādhanā, 47*, 184. https://doi.org/10.1007/s12046-022-01931-1

Barati, M. (2023). Open government data programs and information privacy concerns: A literature review. *JeDEM - eJournal of eDemocracy and Open Government, 15*(1), 73–123. https://doi.org/10.29379/jedem.v15i1.759

Braun, V., & Clarke, V. (2022). *Thematic analysis: A practical guide*. SAGE Publications.

Brown, D., Butt, U., Naqvi, B., & Farag, S. (2026). Bridging the digital gap: Security, privacy and challenges for older adults in governmental digital services. *Information & Computer Security*. Advance online publication. https://doi.org/10.1108/ICS-09-2025-0352

Chomanski, B. (2025). The challenge of regulating digital privacy. *Critical Review of International Social and Political Philosophy*. https://doi.org/10.1080/13698230.2025.2478725

Chomanski, B., & Lauwaert, L. (2025). Digital privacy and the law: The challenge of regulatory capture. *AI & Society, 40*(4), 2777–2787. https://doi.org/10.1007/s00146-024-02041-8

De Cassai, A., Dost, B., Tulgar, S., & Boscolo, A. (2025). Methodological standards for conducting high-quality systematic reviews. *Biology, 14*(8), 973. https://doi.org/10.3390/biology14080973

Del-Real, C., De Busser, E., & van den Berg, B. (2025). A systematic literature review of security and privacy by design principles, norms, and strategies for digital technologies. *International Review of Law, Computers & Technology, 39*(3), 374–405. https://doi.org/10.1080/13600869.2025.2457227

Digital Dubai. (2024a, July 17). *Digital Dubai launches initiative to enhance data quality, aligning with highest international standards*. https://www.digitaldubai.ae/newsroom/news/digital-dubai-launches-initiative-to-enhance-data-quality-aligning-with-highest-international-standards

Digital Dubai. (2024b, September 26). *Digital Dubai launches Dubai Data and AI Platform, ushering in a new phase of digital transformation*. https://www.digitaldubai.ae/newsroom/news/digital-dubai-launches-dubai-data-and-ai-platform-ushering-in-a-new-phase-of-digital-transformation

Digital Dubai. (2025, April 23). *Digital Dubai and Dubai Future Foundation launch inaugural Dubai State of AI Report, showcasing government adoption trends*. https://www.digitaldubai.ae/newsroom/news/digital-dubai-and-dubai-future-foundation-launch-inaugural-dubai-state-of-ai-report-showcasing-government-adoption-trends

Digital Dubai. (2026, April 28). *AI Integration Matrix Framework for Government Organizations*. https://www.digitaldubai.ae/knowledge-hub/publications

Eom, S., & Lee, J. (2022). Digital government transformation in turbulent times: Responses, challenges, and future direction. *Government Information Quarterly, 39*(2), 101690. https://doi.org/10.1016/j.giq.2022.101690

Govers, M., & van Amelsvoort, P. (2023). A theoretical essay on socio-technical systems design thinking in the era of digital transformation. *Gruppe. Interaktion. Organization. Zeitschrift für Angewandte Organisationspsychologie (GIO), 54*(1), 27–40. https://doi.org/10.1007/s11612-023-00675-8

Haug, N., Dan, S., & Mergel, I. (2024). Digitally-induced change in the public sector: A systematic review and research agenda. *Public Management Review, 26*(7), 1963–1987. https://doi.org/10.1080/14719037.2023.2234917

He, C., Luan, T. H., Lu, R., Su, Z., & Dong, M. (2023). Security and privacy in vehicular digital twin networks: Challenges and solutions. *IEEE Wireless Communications, 30*(4), 154–160. https://doi.org/10.1109/MWC.002.2200015

Ikumapayi, O. M., Bayode, A., Jaiyesimi, B. G., Egwuche, O. S., Bello, K. A., Azeez, T. M., Ogunnigbo, C. O., & Onu, P. (2025). Security and privacy challenges in the digital transformation system. *NIPES Journal of Science and Technology Research, 7*(2), 3674–3680. https://doi.org/10.37933/nipes/7.4.2025.SI452

Irani, Z., Abril, R. M., Weerakkody, V., Omar, A., & Sivarajah, U. (2023). The impact of legacy systems on digital transformation in European public administration: Lessons learned from a multi-case analysis. *Government Information Quarterly, 40*(1), 101784. https://doi.org/10.1016/j.giq.2022.101784

Kim, P. W. (2025). Fog computing for artificial intelligence digital textbooks: Educational scaffolding and security and privacy challenges. *Expert Systems, 42*(2), e13801. https://doi.org/10.1111/exsy.13801

Kolaski, K., Romeiser Logan, L., & Ioannidis, J. P. A. (2023). Guidance to best tools and practices for systematic reviews. *Paediatric Rehabilitation Medicine, 16*(2), 171–193. https://doi.org/10.3233/PRM-230019

Kolaventi, S. S., Dash, S., Raju, D., Gupta, M., Setia, N., Niranjan, A., & Jamuna, K. V. (2024). Ethical and privacy challenges in cloud-based health informatics for digital health records. *Seminars in Medical Writing and Education, 3*, 511. https://doi.org/10.56294/mw2024511

Krishna, V. R., Maad, A. H., Alanssari, A. I., Nimah, N. R., Jabbar, K. A., & Thuniki, P. (2025). Ethics, privacy, and security challenges in AI and blockchain-driven digital health ecosystems. In *2025 4th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0* (pp. 1272–1277). IEEE. https://doi.org/10.1109/OTCON65728.2025.11070382

Kuštelega, M., Mekovec, R., & Shareef, A. (2024). Privacy and security challenges of the digital twin: Systematic literature review. *Journal of Universal Computer Science, 30*(13), 1782–1806. https://doi.org/10.3897/jucs.114607

Landerdahl Stridsberg, S., Richardson, M. X., Redekop, K., Ehn, M., & Wamala Andersson, S. (2022). Gray literature in evaluating effectiveness in digital health and health and welfare technology: A source worth considering. *Journal of Medical Internet Research, 24*(3), e29307. https://doi.org/10.2196/29307

Mišić, J., van Est, R., & Kool, L. (2025). Good governance of public sector AI: A combined value framework for good order and a good society. *AI and Ethics, 5*, 4875–4889. https://doi.org/10.1007/s43681-025-00751-3

Misra, S., Barik, K., & Kvalvik, P. (2025). Trust in digital sovereignty: A review of security, privacy, and governance challenges. *Public Organization Review*. Advance online publication. https://doi.org/10.1007/s11115-025-00968-0

OECD. (2024). *AI, data governance and privacy: Synergies and areas of international co-operation* (OECD Artificial Intelligence Papers No. 22). OECD Publishing. https://doi.org/10.1787/2476b1a4-en

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science, 50*(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Saleha, N., Widiasih, R., Pramukti, I., Dhamayanti, M., & Aprilatutini, T. (2026). Privacy rights versus surveillance, challenges of sex education in the digital age: An exploratory qualitative study in Indonesia. *BMC Public Health, 26*, 837. https://doi.org/10.1186/s12889-026-26281-z

Song, B., Pokhrel, S. R., Deng, M., Lan, Q., Doss, R., Zhu, T., & Li, G. (2025). Digital privacy under attack: Challenges and enablers. *ACM Computing Surveys, 58*(4), 107, 1–35. https://doi.org/10.1145/3770853

Telecommunications and Digital Government Regulatory Authority. (2023, December 18). *TDRA releases the Digital Enablers Report 2023*. https://tdra.gov.ae/en/media/press-release/2023/tdra-releases-the-digital-enablers-report-2023

Tukur, M., Schneider, J., Househ, M., Dokoro, A. H., Ismail, U. I., Dawaki, M., & Agus, M. (2023). The metaverse digital environments: A scoping review of the challenges, privacy and security issues. *Frontiers in Big Data, 6*, 1301812. https://doi.org/10.3389/fdata.2023.1301812

UAE Government. (2024a, December 30). *The UAE Digital Government Strategy 2025*. The Official Portal of the UAE Government. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/uae-national-digital-government-strategy

UAE Government. (2024b, June 10). *UAE Charter for the Development and Use of Artificial Intelligence*. UAE Legislation. https://uaelegislation.gov.ae/en/policy/details/the-uae-charter-for-the-development-and-use-of-artificial-intelligence

UAE Government. (2024c, December 30). *Overseeing digital transformation in the UAE*. The Official Portal of the UAE Government. https://u.ae/en/about-the-uae/digital-uae/digital-transformation/cooperation-and-collaboration/overseeing-digital-transformation-in-the-uae

UAE Government. (2025a, November 27). *Data protection laws*. The Official Portal of the UAE Government. https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws

UAE Government. (2025b, October 23). *National Cloud Security Policy*. The Official Portal of the UAE Government. https://u.ae/en/about-the-uae/digital-uae/digital-transformation/strategies-policies-and-initiatives/National-Cloud-Security-Policy

UAE Government. (2025c). *Artificial intelligence in government policies*. The Official Portal of the UAE Government. https://u.ae/en/about-the-uae/digital-uae/artificial-intelligence/artificial-intelligence-in-government-policies

United Nations Department of Economic and Social Affairs. (2024). *United Nations E-Government Survey 2024: Accelerating digital transformation for sustainable development*. United Nations. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024

Vera-Arenas, C. J. (2025). 'Human digital twins' and blockchain: Some challenges and solutions for digital identity and privacy. In C. Pastor Sempere (Ed.), *Governance and control of data and digital economy in the European Single Market* (pp. 473–488). Springer. https://doi.org/10.1007/978-3-031-74889-9_21

Verma, A., & Gurtoo, A. (2024). Evaluating global data policies around non-personal data on social and public goods. *Digital Policy, Regulation and Governance, 26*(1), 72–94. https://doi.org/10.1108/DPRG-03-2023-0044

World Bank. (2025). *Digital public infrastructure and development: A World Bank Group approach*. World Bank. https://documents1.worldbank.org/curated/en/099031025172027713/pdf/P505739-84c5073b-9d40-4b83-a211-98b2263e87dd.pdf

Zhou, Y. (2025). Cybersecurity and privacy protection in the digital age: Challenges and countermeasures. In *2025 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)* (pp. 1–6). IEEE. https://doi.org/10.1109/BMSB65076.2025.11165675