information

MDPI

Article

Quantitative Analysis of Information Security and Privacy Challenges in Government Cloud Service Adoption

Ndukwe Ukeje, Jairo A. Gutierrez and Krassie Petrova *

School of Engineering, Computer and Mathematical Sciences, Auckland University of Technology, Auckland 1010, New Zealand; ndyukeje@yahoo.co.uk (N.U.); jairo.gutierrez@aut.ac.nz (J.A.G.)
* Correspondence: krassie.petrova@aut.ac.nz

Abstract

The government's adoption of cloud computing is critical for digital transformation, but it faces persistent concerns over information security, privacy, governance, and risk. This study examines the factors influencing a government's intention to adopt cloud services, adapting the Unified Theory of Acceptance and Use of Technology (UTAUT) with constructs tailored to the public sector. A cross-sectional survey was conducted across 90 Nigerian government organisations, producing 230 valid responses from IT professionals, administrators, and policy personnel. The statistical analysis of the data was conducted using SPSS and structural equation modelling in AMOS. Validity and reliability were confirmed through composite reliability, Cronbach's alpha, and discriminant validity measures. Findings show that privacy ($\beta = 0.11$, $p < 0.05$), governance framework ($\beta = 0.34$, $p < 0.001$), performance expectancy ($\beta = 0.38$, $p < 0.001$), and information security ($\beta = 0.10$, $p < 0.05$) significantly influence government intention to adopt cloud services. Performance expectancy emerged as the strongest predictor. Contrary to expectations, perceived risk did not significantly moderate the relationships, and interaction terms were non-significant. The final model explained 45% of the variance in adoption intention ($R^2 = 0.45$). The study highlights the importance of strengthening governance frameworks, emphasising tangible performance outcomes, and positioning information security and privacy as an enabler of adoption rather than a barrier. By adapting UTAUT to the government context and disentangling the role of perceived risk, the study offers both theoretical refinement and practical guidance for policymakers aiming to accelerate digital transformation and secure cloud adoption.

Keywords: cloud computing; government adoption; UTAUT; information security; privacy; governance framework; perceived risk

Academic Editors: Leandros Maglaras and Nader Sohrabi Safa

Received: 30 November 2025
Revised: 28 January 2026
Accepted: 28 April 2026
Published: 2 May 2026

1. Introduction

Cloud computing has become a cornerstone of digital transformation initiatives in the public sector, enabling government agencies to modernise service delivery and enhance citizen engagement [1,2]. Cloud-based solutions provide scalable infrastructures for real-time data analytics, reduce operational costs, facilitate interdepartmental collaboration, and support the digitisation of critical public services. Despite these advantages, adoption in government still lags behind the private sector due to a range of technical, organisational, and policy-related inhibitors [3,4]. Among these, information security and privacy concerns represent the most prominent obstacles [5].

The public sector operates under stringent regulatory frameworks and manages highly sensitive citizen and institutional data, making issues of confidentiality, integrity, and availability particularly critical. Security breaches or unauthorised data access can erode citizen trust, compromise public accountability, and result in significant legal and operational consequences. Consequently, risk perceptions regarding the adequacy of security controls, compliance with privacy laws, and adherence to governance frameworks play a decisive role in shaping governments' willingness to adopt cloud services.

The Unified Theory of Acceptance and Use of Technology (UTAUT) has been widely applied to examine technology adoption behaviours, leveraging constructs such as performance expectancy, effort expectancy, social influence, and facilitating conditions [6]. While the UTAUT model explains a substantial proportion of variance (70%) in adoption intention and 50% in technology acceptance, it was primarily designed for general contexts and does not sufficiently capture the unique risk environment of public-sector cloud adoption [7,8]. Nevertheless, information security, privacy, and compliance with governance frameworks are more pronounced in government adoption scenarios than in most private-sector applications. This highlights the need to adapt UTAUT to better reflect the dynamics of government cloud adoption.

To address this gap, this study develops an adapted UTAUT framework that integrates constructs specific to government cloud services. In addition to performance expectancy, the model incorporates: information security, reflecting perceptions of the provider's ability to safeguard sensitive public data; privacy, capturing concerns about unauthorised access and misuse of personally identifiable information (PII); and governance framework, encompassing the policies, regulations, and compliance requirements guiding adoption. Furthermore, the study positions perceived risk as a moderating factor that shapes the influence of these constructs on adoption intention.

Based on this framework, two guiding research questions are formulated:

1. To what extent do adapted constructs influence governments' intention to adopt cloud services?
2. How does perceived risk moderate the relationship between these adapted constructs and the government's adoption intention?

The study makes several key contributions to the understanding of security-oriented factors influencing the adoption of government cloud services, advancing both theoretical and practical perspectives in information security and digital transformation. These contributions are highlighted in the following:

- Adaptation of UTAUT-Based Framework: This study adapts UTAUT with the constructs that are particularly critical to the public-sector security-sensitive contexts and captures the multidimensional challenges of cloud adoption in government. This adaptation provides a novel conceptual bridge between information security theory and organisational technology acceptance models.
- Adapting Perceived Risk as a Moderating Construct: Unlike prior studies that treat risk as a control or antecedent variable, this study introduces perceived risk as a moderator shaping the strength of relationships between core constructs and adoption intention. This empirical exploration adds explanatory power and extends the theoretical boundaries of the UTAUT model in a security-centric context (see Section 4.6: Structural Model and Hypotheses Testing).
- Empirical Validation through Quantitative Analysis: The framework is empirically validated using data from 230 respondents across 90 Nigerian government organisations. Employing Confirmatory Factor Analysis (CFA) and structural equation modelling (SEM), this study rigorously tests the reliability, validity, and interaction effects of the constructs. The model explains 45% of the variance in government intention to adopt

cloud services, underscoring its valuable insights (see Sections 4 and 5: Results and Discussion).

- Theoretical and Policy Implications for Secure Digital Governance: The findings strengthen how governance frameworks and performance expectancy significantly influence cloud adoption intentions, while highlighting the distinct role of perceived risk in shaping security-oriented decisions. The study offers recommendations for policymakers and practitioners seeking to mitigate adoption barriers, enhance governance mechanisms, and promote trust in cloud-based public services. This study further positions government cloud adoption within the broader discourse of secure digital transformation by emphasising trust, security, and regulatory compliance (see Section 5: Discussion).

The remainder of the article is organised as follows: Section 2 reviews the literature on government cloud computing and the UTAUT model. Section 3 develops the theoretical framework and hypotheses, outlining the research methodology, including data collection and analysis procedures. Section 4 presents the empirical findings and analysis. Section 5 discusses the theoretical contributions and practical implications of the study, along with its limitations. Section 6 concludes with the study's key findings and conclusions.

2. Related Work

2.1. Cloud Computing in Government: Opportunities and Benefits

Cloud computing has emerged as a transformative force in the public sector, offering scalability, efficiency, and improved service delivery. Governments increasingly leverage cloud platforms to optimise resource allocation, facilitate inter-agency collaboration, and accelerate the delivery of citizen-facing digital services. Benefits highlighted in prior studies include cost-effectiveness through pay-as-you-go models, flexibility in scaling resources, and enhanced innovation capacity through rapid deployment of digital applications [9].

Studies confirm that cloud adoption can improve transparency, streamline service delivery, and enhance citizen engagement. For example, U.S. federal agencies have used cloud-based solutions to increase efficiency and operational resilience; somewhat differently, the primary function of cloud services in the context of developing economies is still to serve as a digital transformation enabler [10]. Thus, cloud adoption promises not only economic efficiency but also improved public value creation. Consequently, while prior research has highlighted the technological and economic benefits of cloud adoption, there remains limited empirical understanding of how governance, information security, privacy and risk perceptions jointly influence adoption intentions in the government context.

2.2. Policy and Strategic Frameworks for Cloud Adoption

Policy frameworks play a decisive role in shaping government cloud strategies, and many governments have initiated national strategies to promote digital transformation through cloud adoption. The United States pioneered policy-driven adoption through the Cloud First (2010) and Cloud Smart (2019) initiatives, which put a strong emphasis on security, procurement optimisation, and workforce readiness [10]. Similarly, the United Kingdom's G-Cloud framework provides a procurement mechanism that aims to lower entry barriers by embedding compliance obligations [11]. Australia's Cloud Computing Policy prioritises risk management and cost efficiency [12]. However, despite these initiatives, concerns surrounding security, privacy, and data sovereignty remain critical barriers to adoption, particularly where sensitive citizen and national data are involved [12,13]. In developing economies, such as Nigeria, digital governance initiatives are expanding rapidly, yet organisational and technical challenges persist [14]. These include weak gov-

ernance frameworks, inconsistent enforcement of data protection, and limited technical capacity to assess and manage cloud-related risks.

The digital transformation strategies in developing countries focus on regulatory initiatives that are necessary to drive cloud adoption and ensure data sovereignty measures. Yet, policy-driven frameworks may underperform due to the lack of a supporting information security governance structure. According to Choi et al. [11], cloud-first policies must be coupled with continuous security monitoring and compliance enforcement to ensure long-term sustainability. Similarly, it has been demonstrated that security governance frameworks are crucial to establishing trust in sovereign cloud infrastructures [15]. These findings indicate that while policy frameworks stimulate cloud service adoption, the success of the adoption initiatives may depend strongly on removing information security-related adoption barriers and embedding information security governance into the policy implementation project.

2.3. Information Security, Privacy, Perceived Risk and Sovereignty Challenges

Despite the benefits of cloud adoption, considerations about data sensitivity and the criticality of government operations still serve as significant adoption inhibitors. To this end, prior studies have consistently identified information security and privacy challenges as primary barriers [5,16–18].

Breaches in confidentiality, integrity, or availability can undermine citizen trust, disrupt services, and even compromise national security. Consequently, significant research has focused on enhancing data confidentiality, integrity, and traceability across distributed cloud systems. For example, a recent study has proposed lightweight and traceable data circulation encryption (LTP-CLE) for edge computing scenarios [19]. This approach leverages certificateless encryption to eliminate reliance on trusted key generation, thereby enhancing security and traceability and reducing privacy-related challenges. However, the implementation of the protective mechanisms proposed in the literature, such as encryption, anonymisation, and advanced access controls [20], is still limited.

Further challenges include legal and regulatory compliance over data sovereignty and governance, such as requirements for local data residency, compliance with national security regulations, and preference for sovereign cloud providers. For example, Abd Al Ghaffar [21] proposed a risk-based assessment framework for government adoption of cloud services that aligns security strategies with regulatory contexts.

Overall, the proposed mechanisms and approaches primarily address system-level protection and enforcement and do not capture institutional trust and compliance frameworks, which are particularly vital in government adoption scenarios. European governments, in particular, emphasise sovereignty concerns over reliance on foreign-controlled cloud providers [12]. Similarly, Jiménez et al. [13] state that concerns about sovereignty and trust shape government adoption decisions as much as the awareness of the need for strong technical safeguards does.

The technical perspectives remain infrastructure-centric, with a focus on technical optimisation rather than on understanding the behavioural factors influencing governments in their cloud service adoption decisions. Perception about risk plays a critical role, as Prakash et al. [22] show that perceptions about risks related to service downtime, vendor lock-in, and regulatory non-compliance often amplify reluctance to adopt cloud services despite the availability of safeguards. As indicated in Al Mudawi et al. [9], governments frequently trade efficiency gains for stronger security guarantees, illustrating the complex interplay between opportunities and risks in public-sector cloud service adoption.

The transition to cloud computing within government institutions introduces a complex spectrum of risks that can affect trust, compliance, and operational reliability. These

risks are multidimensional, encompassing technological, organisational and regulatory spheres. These risks can be classified into four categories: privacy and data sovereignty, governance, information security, and operational. Understanding and mitigating these risks are essential prerequisites for achieving sustainable adoption of cloud services in government operations. Thus, the government's willingness to adopt cloud services diminished, even in the presence of adequate technical controls, when perceived levels of uncertainty or vulnerability were higher; consequently, perceived risk could significantly influence decision-makers' confidence in adopting cloud services.

Additionally, this study does not seek to construct or validate a technical threat model; it recognises that government agencies operate within a complex security environment that influences willingness to adopt cloud services. The perceived risks associated with cloud computing in the public sector often arise from multiple potential threat vectors (external and internal), vendor dependencies and cloud service providers' vulnerabilities, such as inadequate data protection mechanisms or cross-border data transfers that violate national sovereignty laws.

The government often seek to mitigate these challenges through regulatory governance frameworks, compliance mechanisms, and multi-layered structures. Therefore, this study conceptualised the risk perceptions as a behavioural determinant influencing adoption intention, rather than a technical threat. Inclusion of perceived risk as a moderating construct reflects how government actors interpret and respond to multidimensional security challenges when evaluating cloud service adoption.

The preceding review synthesised prior studies on government cloud adoption and identified key determinants influencing cloud adoption behaviour, particularly in public-sector contexts. The literature consistently highlights that information security [13,16], privacy [17], performance expectancy [18], and governance frameworks [11] are critical constructs shaping institutional adoption decisions. Additionally, perceived risk has been recognised as a factor that affects the strength of these relationships [22].

2.4. Theoretical Models and Research Gaps

While cloud computing has transformed digital service delivery and transformation, government adoption remains hindered by unresolved concerns surrounding security, privacy, governance, and risk perception [5]. Existing models of technology acceptance, such as the Technology Acceptance Model (TAM), Theory of Planned Behaviour (TPB), and UTAUT, have provided valuable insights into individual and organisational technology adoption; however, they fall short in capturing the complex, security-oriented determinants that shape cloud adoption in the public sector.

Technology adoption research often draws on the Unified Theory of Acceptance and Use of Technology (UTAUT) to explain behavioural intentions [6,7]. UTAUT constructs—performance expectancy, effort expectancy, social influence, and facilitating conditions—have explained adoption behaviour in diverse contexts. However, the model has limitations with regard to its applicability to the public sector. Specifically, UTAUT does not explicitly account for security, privacy, governance, and sovereignty constructs, which are central to government cloud adoption [13,16]. Furthermore, there is a call for a better understanding of the factors that challenge cloud adoption to improve competitive advantage in enterprise digital transformation and the globalised digital economy [23].

Most prior studies have focused on either technological or organisational readiness, with limited integration of information security, governance, and perceived risk as dynamic, interacting constructs influencing decision-making. Scholars have increasingly called for extended models that integrate these constructs. For example, Abdulsalam and Hedabou [17] pointed out that models which do not address security and privacy

concerns explicitly may not provide adequate support for decision-making. However, Jiménez, Dittmar and Portillo [21] found that in existing adoption frameworks, the concepts of trust and sovereignty were insufficiently developed as adoption determinants. Furthermore, Prakash, Malaiyappan, Thirunavukkarasu and Devan [22] suggested that perceived risk played the role of a moderating factor that influences the impact of other adoption constructs.

The review of the relevant literature indicates that a theoretical and empirical gap exists in understanding how these multidimensional security-related factors jointly influence the government's intention to adopt cloud services. This study addresses the gap by adapting UTAUT to integrate constructs of information security, privacy, performance expectancy, and governance frameworks, with perceived risk conceptualised as a moderator. This approach provides a comprehensive, quantifiable view for evaluating cloud adoption decisions in a security-sensitive environment. By contextualising institutional decisions within established national security frameworks and the context of digital transformation, this research complements technical literature with an empirically grounded understanding of adoption behaviour. This adaptation offers a more accurate theoretical basis for understanding government cloud adoption dynamics, thereby contributing to both scholarly discourse and policy-oriented practice.

3. Materials and Methods

This study adopts a quantitative research design, grounded in a positivist paradigm, which assumes that technology adoption behaviour can be objectively measured through validated constructs and tested relationships [24]. The choice of a quantitative design aligns with the study's aim of empirically examining the influence of specific constructs on the government's intention to adopt cloud services. More specifically, the study employs deductive reasoning, where existing theories are adapted and tested in a novel context. While UTAUT serves as the core theoretical foundation, the model was adapted to incorporate new constructs (privacy, information security, governance framework) and a moderating variable (perceived risk). This ensures that the design captures both the established determinants of technology adoption and the unique challenges of the government cloud adoption environment.

3.1. Theoretical Foundation

Technology adoption research has long relied on behavioural and organisational models, such as the Technology Acceptance Model (TAM), the Theory of Planned Behaviour (TPB), and the Innovation Diffusion Theory (IDT), each emphasising different predictors of technology use. Venkatesh, Morris, Davis and Davis [7] synthesised these perspectives into the UTAUT, which demonstrated explanatory power, accounting for up to 70% of the variance in behavioural intention, and 50% in technology acceptance. However, as Venkatesh et al. [25] noted, boundary conditions remain unexplored, particularly in sector-specific contexts such as government.

The UTAUT model provides a robust theoretical foundation for examining behavioural intentions towards technology adoption. Its integrating nature and predictive power make it suitable for analysing complex organisational decisions, such as government adoption of cloud services. In this study, UTAUT adaptation to the public-sector context accounts for institutional factors, which are critical determinants in government technology adoption to address broader organisational and regulatory factors challenging cloud adoption from a government perspective. Furthermore, UTAUT continues to serve as a policy-shaping tool by offering a systematic lens through which policymakers can understand and predict institutional readiness to adopt innovative technologies such as cloud services.

The public sector presents such a distinct context, which traditional UTAUT constructs do not fully capture. Unlike private organisations, governments must safeguard highly sensitive data, ensure compliance with sovereignty and legal frameworks, and maintain public trust. These unique challenges require adapting the UTAUT model beyond its generic constructs to capture government-specific adoption dynamics.

The UTAUT research model comprises four constructs (performance expectancy, effort expectancy, social influence, and facilitating conditions) and moderators that significantly direct user acceptance and behaviour usage determinants. The key moderators are gender, age, voluntariness of use, and experience, while the behavioural intention and use behaviour are consistent with the theory in determining the influence of technology usage, such as cloud computing.

UTAUT's original constructs—performance expectancy, effort expectancy, social influence, and facilitating conditions—have been widely validated across contexts [6,26–28]. However, when transposed into public-sector cloud computing, their explanatory power diminishes without adaptation:

- Effort expectancy and facilitating conditions are relevant but secondary in government contexts where adoption is often policy-driven rather than user-driven.
- Social influence in government may not reflect peer or managerial persuasion but rather political mandates, which require reframing.

Thus, this study retains performance expectancy while adapting the model with constructs that explicitly capture security, privacy, and governance concerns, moderated by perceived risk. This conceptualisation aligns with the call for cross-disciplinary constructs to be incorporated into UTAUT and extends its explanatory relevance to government cloud security contexts.

3.2. Adaptation of UTAUT for Government Cloud Adoption

This study adapts the UTAUT framework to examine government cloud adoption by incorporating four critical constructs as identified in Figure 1—privacy, governance framework, information security, and performance expectancy—and a moderating factor, perceived risk. While performance expectancy remains central to the UTAUT core, the additional constructs reflect challenges particularly salient for governments.

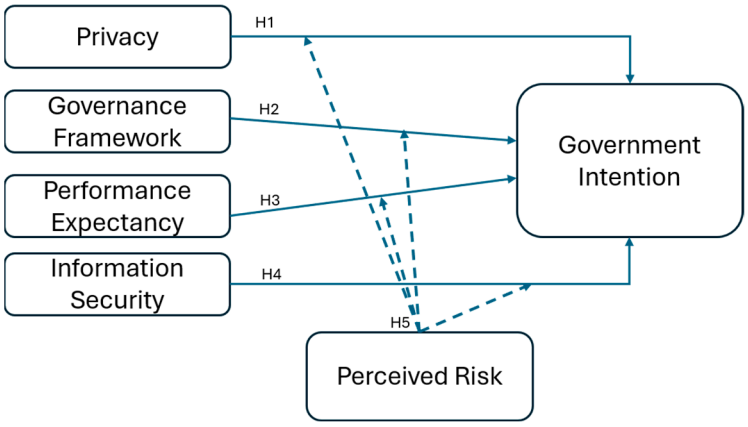

Figure 1. Proposed conceptual model (adapted from [7]).

1. Privacy

Identifying the degree of protection of personally identifiable information (PII) and citizen-sensitive records remains a barrier to cloud adoption [5]. Governments must ensure that cloud providers guarantee the confidentiality of citizens' PII and prevent unauthorised access to it.

2. Governance Framework

National laws, compliance regimes, and sovereignty requirements dictate how cloud adoption unfolds in government [29]. A robust governance framework aligns cloud initiatives with accountability and risk mitigation mandates.

3. Performance Expectancy

As in the original UTAUT, governments adopt technologies they perceive as improving efficiency, scalability, and citizen-facing services [1].

4. Information Security

Given the sensitivity of government data, breaches can erode citizen trust, disrupt critical services, and threaten national security [30]. Thus, perceptions of provider security capabilities are pivotal.

5. Perceived Risk (Moderator)

Governments face compounded risks—technical (downtime, breaches), strategic (vendor lock-in), and regulatory (data sovereignty violations). These risks can either strengthen or weaken the influence of adoption drivers on behavioural intention [31].

Adapting UTAUT with these constructs enables the development of a model that is both theoretically rigorous and contextually relevant [32]. The conceptual model is presented in Figure 1. The hypotheses that link the constructs were drawn from the relationships identified in the literature, ensuring that a theoretical consistency is established between the existing studies and the proposed research model:

H1: *Privacy has a significant positive influence on the government's intention to adopt cloud services. This hypothesis is supported by the findings of the lithe literature in Section 2.3 on the role of privacy concerns in government decision making [17].*

H2: *Governance framework has a significant positive influence on the government's intention to adopt cloud services.*

This hypothesis is supported by the findings of the literature review in Section 2.2 which indicate that policy frameworks stimulate cloud service adoption [11].

H3: *Performance expectancy has a significant positive influence on government intention to adopt cloud services.*

This hypothesis is supported by the findings of the literature review in Section 2.1 which highlight the expectations of the technological and economic benefits of cloud service adoption [18].

H4: *Information security has a significant positive influence on the government's intention to adopt cloud services.*

H5: *Perceived risk moderates the relationship between privacy, governance framework, performance expectancy, and information security, as well as government intention to adopt cloud services.*

Hypotheses H4 and H5 are supported by the findings of the literature review in Section 2.3 about the criticality of information security [13,16] and about the role of perceived risk as a relationship mitigating factor [22].

This adapted UTAUT model thus provides a comprehensive lens for examining government cloud adoption, balancing theoretical robustness with the context-specific challenges of security, privacy, and governance.

3.3. Data Collection Method

A survey-based approach was considered appropriate given its ability to capture perceptions across a wide population of government IT decision-makers and policymakers. This approach supports hypothesis testing while also allowing generalisation of findings within the Nigerian public-sector context.

3.3.1. Survey Instrument

The validated scales from the prior study's survey instrument [32] were used to measure the items. The measurement items for each construct and the corresponding questions are available in Table A1. The items were measured using a five-point Likert scale, ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). This scaling approach captures varying intensities of perception while ensuring comparability with previous UTAUT-based research. The validated measurement instruments employed were used to ascertain the construct dimensionality for this study through the assessed Exploratory Factor Analysis (EFA) [32].

The survey instrument was administered electronically using Qualtrics, a secure web-based survey platform that offers advanced data encryption, anonymity features, and increased accessibility, which aligned with the research ethics requirements for government-related studies by ensuring confidentiality and compliance with data protection regulations. Ethical principles of confidentiality and voluntary participation were observed, consistent with research best practices [24,33].

3.3.2. Participants and Sampling

The target population consisted of employees within Nigerian government ministries, departments, and agencies (MDAs) who are actively involved in information technology, information security, privacy and digital transformation initiatives. Participants included IT administrators, information security and privacy officers, cloud service managers, and policymakers. Given the specificity of the population, a non-probability purposive sampling method was adopted. This approach ensured that only respondents who possess direct knowledge and experience of the subject were employed [34,35]. This ensured that only participants with relevant expertise contributed data, thereby enhancing the validity of responses.

The invitations were distributed to approximately 90 government organisations, and 230 valid responses were obtained; the resulting study dataset is provided as a Supplementary Materials File S1. The sample size was deemed sufficient for structural equation modelling (SEM) analysis and achieved a high completion rate, with the overall response rate considered satisfactory for an institutional-level survey and no evidence of non-response bias. Data were collected using an online survey instrument (Qualtrics), which provided efficiency, cost-effectiveness, and wider geographical coverage. Respondents were assured of confidentiality and anonymity, consistent with ethical research guidelines [33] and the study's ethical approval.

3.4. Data Analysis Methods

To ensure analytical rigour and address the study's objectives, a series of statistical analyses was conducted following standard quantitative research procedures. A two-stage approach was applied.

Descriptive statistics were first employed to summarise the demographic characteristics and key response patterns, providing insight into participants' professional backgrounds and perceptions of cloud service. The statistical package SPSS (v.28) was used for this analysis.

Subsequently, Confirmatory Factor Analysis (CFA) was conducted to confirm the validity of the constructs and the reliability of the measurement items. Reliability analysis was further conducted using composite reliability (CR) and Cronbach's alpha (α). Common method bias was examined using Harman's single-factor test.

Structural equation modelling (SEM) was applied to test the hypothesised relationships between the independent variables, the moderator (perceived risk), and the dependent variable (intention to adopt cloud services). The statistical software AMOS (v. 29) was used to conduct the CFA and SEM.

3.4.1. Measurement Model Analysis

A CFA was conducted to confirm the validity of the constructs and the reliability of the measurement items. The model fit was evaluated using multiple indices such as the Comparative Fit Index (CFI), Tucker–Lewis Index (TLI), and Incremental Fit Index (IFI), as well as Standardised Root Mean Square Residual (SRMR) and Root Mean Square Error of Approximation (RMSEA) [36,37].

3.4.2. Structural Model Testing

The study employed a structural path analysis to test the hypotheses. Applying SEM, the model's path coefficients were estimated using maximum likelihood estimation. Moderator effects of Perceived Risk were examined using mean-centring and interaction terms [38]. The significance was tested using bootstrapping with 2000 samples at 95% bias-corrected confidence intervals.

Additionally, a further check was performed, including multicollinearity assessment through the variance inflation factor (VIF) and tolerance limit (TOL) [37,39,40], as well as common method bias (CMB) testing using Harman's single-factor test [41–43].

4. Results

Overall, the CFA results confirmed the fitness of the model, with all indices (CFI, TLI, IFI, SRMR, and RMSEA) meeting the recommended thresholds and indicating satisfactory model fit. The CR and Cronbach's alpha (α) values exceeded accepted standards, demonstrating internal construct consistency. The Harman's single-factor test confirmed that no single factor accounted for a majority of the variance, thereby reducing the likelihood of bias from self-reported data. The multicollinearity tests confirmed the independence of constructs, ensuring stable regression estimates.

Following measurement validation, bivariate correlations were used to examine the initial relationships among the constructs, and structural path analysis was used to test the hypotheses and the moderating effects of perceived risk. This multistage analytical framework provided robust empirical evidence linking information security, privacy, performance expectancy, and governance frameworks to the government's intention to adopt cloud services. Together, these analyses confirm the model's statistical validity and reliability while providing a comprehensive understanding of the relational influences among key variables.

4.1. Descriptive Statistics

Descriptive statistics were computed to characterise the respondents and provide insight into their background, experience, and perceptions [44]. Out of 230 valid responses, 196 (85.6%) were IT practitioners, administrators, or personnel with expertise

in information security and privacy. One response (0.4%) was missing. In contrast, 16 respondents (7%) did not, while 17 respondents (7.4%) identified as others, including legal officers involved in privacy governance and compliance, who directly contribute to technology adoption and data protection initiatives in government institutions. This indicates that the majority of respondents possess relevant technical knowledge, strengthening the dataset's credibility.

Regarding work experience, 33% of respondents reported having 0–5 years of experience, 24.8% had 6–10 years, 17% had 11–15 years, 10.4% had 16–20 years, and 14.8% had more than 20 years of experience. The distribution across multiple experience categories suggests balanced representation from early career to highly experienced professionals.

When asked about the perceived impact of cloud computing on job performance, 98.3% of respondents agreed that cloud adoption would improve government service delivery and operational efficiency, while only 1.7% disagreed, underscoring the relevance of performance expectancy as a critical construct, despite the identified challenges.

4.2. CFA Results

The Hue et al. [36] threshold criterion for fit indices in structure analysis was applied to validate the six-factor measurement model (Privacy, Governance Framework, Performance Expectancy, Information Security, Perceived Risk, and Government Intention). The following model fit criteria were met: CFI, IFI, TLI $\geq$ 0.90; x2/df $\leq$ 3.0; SRMR $\leq$ 0.08 [45]; and RMSEA $\leq$ 0.06. Further, the CR and Cronbach alpha (α) reliability coefficients were $\geq$0.60 and $\geq$0.70, respectively, for all the measurement scales [36]. Additionally, the discriminant validity (DV), established as the square root of the average variance extracted (AVE), was greater than the correlations among the latent variables in the CFA [36,37].

Model fit indices initially indicated suboptimal results, as shown in Table 1, with the TLI (0.895) falling slightly below the threshold. After removing three poorly performing items (GovtF6, GovtF8, GovtInt6), the model fit improved substantially to the acceptable TLI indices for the recommended threshold value, as suggested by Bentler and Bonett [46] and supported by West et al. [47]. The removal of factor loadings of the component items from the CFA model was based on the standardised residual covariances [37] to further improve the six-factor CFA model fit indices, which were significantly improved, as shown in Figure 2 and Table 2.

Table 1. Model fit measures: Initial estimate.

Measure	Estimate	Threshold	Interpretation
CMIN	672.860	--	--
DF	362.000	--	--
CMIN/DF	1.859	Between 1 and 3	Excellent
CFI	0.906	$\geq$0.90	Acceptable
TLI	0.895	$\geq$0.90	Unacceptable
IFI	0.906	$\geq$0.90	Acceptable
SRMR	0.069	$\leq$0.08	Excellent
RMSEA	0.061	$\leq$0.06	Acceptable

Table 2. Model fit measures: Final estimate.

Measure	Estimate	Threshold	Interpretation
CMIN	466.855	--	--
DF	284.000	--	--

Table 2. *Cont.*

Measure	Estimate	Threshold	Interpretation
CMIN/DF	1.644	Between 1 and 3	Excellent
CFI	0.938	≥0.90	Acceptable
TLI	0.926	≥0.90	Acceptable
IFI	0.938	≥0.90	Acceptable
SRMR	0.064	≤0.08	Excellent
RMSEA	0.053	≤0.06	Excellent

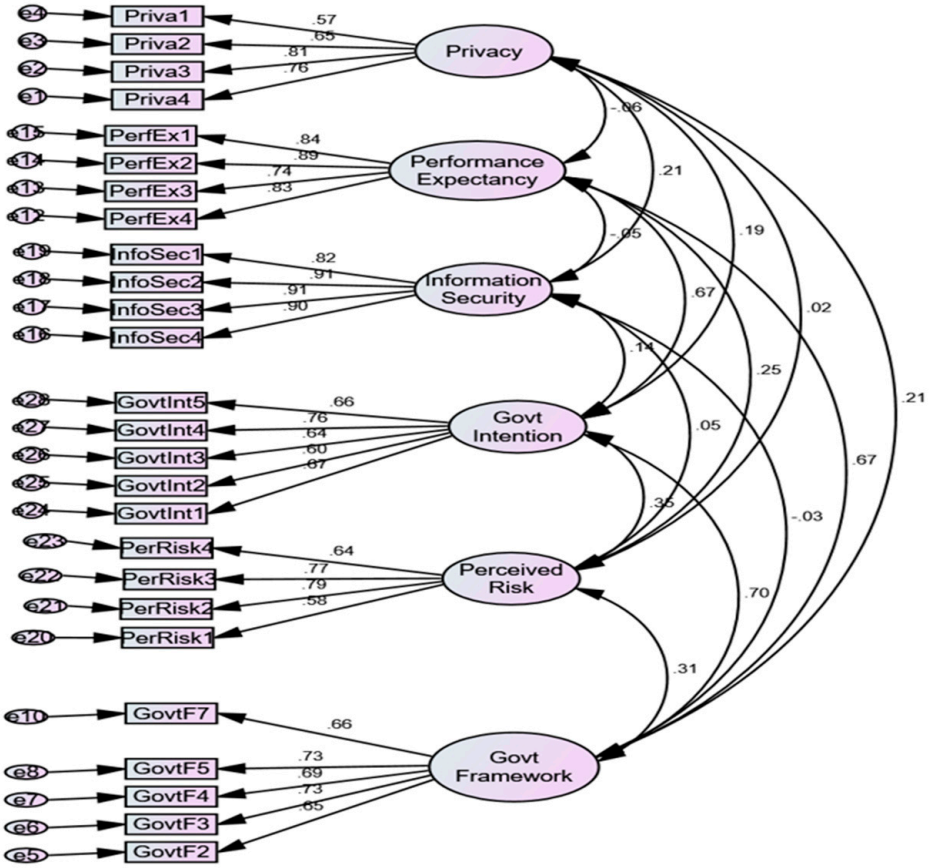

Figure 2. Confirmatory factor analysis model.

4.3. Validity and Reliability Analysis

To assess construct reliability and validity, composite reliability (CR), AVE, and Cronbach's alpha (α) were calculated (Table 3). The results confirm the measurement's reliability and its convergent and discriminant validity.

Table 3. Construct reliability and validity.

Variables	CR	AVE (Convergent Validity)	α	DV
Privacy (Priva)	0.794	0.496	0.785	0.704
Government Framework (GovtF)	0.823	0.482	0.832	0.695
Performance Expectancy (PerfEx)	0.837	0.562	0.831	0.750
Information Security (InfoSec)	0.934	0.781	0.940	0.884
Perceived Risk (PerRisk)	0.791	0.490	0.799	0.700
Government Intention (GovtInt)	0.788	0.428	0.789	0.654

Note: CR = composite reliability, α = Cronbach's alpha, AVE = average variance extracted, DV = discriminant variable.

1. Reliability

All constructs demonstrated acceptable reliability, with CR ranging from 0.788 to 0.934 and Cronbach's alpha (α) from 0.785 to 0.940, both exceeding recommended thresholds [36,37,48,49].

2. Convergent Validity

Most constructs exceeded the AVE threshold of 0.50 [37,48,50], except Government Intention (0.428). However, this was retained because its CR exceeded 0.70, consistent with Fornell and Larcker [46], Brunelle and Lapierre [51], Lam [52] and Menguc and Auh [53].

3. Discriminant Validity

The square roots of AVE for each construct were greater than inter-construct correlations, satisfying Fornell and Larcker's criterion.

4.4. Common Method Bias and Multicollinearity

To address the potential risk of common method variance inherent in self-reported survey data and test for multicollinearity, two diagnostic tests were conducted:

- CMB analysis: Harman's single-factor test [41–43] revealed that the first factor accounted for 24.2% of variance, as shown in Table 4, well below the 50% threshold. This suggests CMB is not a major concern.
- Multicollinearity: The VIF and TOL analyses [40,54] were conducted to check for multicollinearity in the dataset. The values ranged from 1.05 to 1.69, as shown in Table 5, and were below the VIF and TOL cutoff values of 4 and 1, respectively. This confirmed that multicollinearity was not a significant issue.

Table 4. Harman's one-factor common method bias test.

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.297	24.218	24.218	6.297	24.218	24.218
2	3.752	14.432	38.650			
3	2.393	9.205	47.856			
4	2.223	8.548	56.404			
5	1.387	5.334	61.738			
6	1.189	4.572	66.311			
7	0.881	3.388	69.699			
8	0.732	2.817	72.516			
9	0.701	2.694	75.210			
10	0.644	2.476	77.686			
11	0.612	2.353	80.039			
12	0.567	2.180	82.218			
13	0.501	1.928	84.147			
14	0.473	1.821	85.968			
15	0.453	1.743	87.710			
16	0.450	1.732	89.443			
17	0.413	1.589	91.032			
18	0.361	1.390	92.422			
19	0.345	1.325	93.748			
20	0.319	1.228	94.976			
21	0.304	1.168	96.144			
22	0.263	1.013	97.157			
23	0.252	0.970	98.127			

Table 4. *Cont.*

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
24	0.208	0.801	98.928			
25	0.152	0.583	99.511			
26	0.127	0.489	100.000			

Extraction method: Principal Component Analysis.

Table 5. Results of VIF and TOL for the variables.

	Variables	Tolerance	Variance Inflation Factors
Independent Variables	Privacy	0.90	1.10
	Governance Framework	0.67	1.49
	Performance Expectancy	0.68	1.47
	Information Security	0.96	1.05
Moderators	Perceived Risk	0.94	1.07
Dependent Variable	Government Intention	0.59	1.69

4.5. Correlation Analysis

The results of the bivariate correlation analysis, presented in Table 6, showed that privacy (r = 0.13, $p < 0.05$), government framework (r = 0.57, $p < 0.01$), and performance expectancy (r = 0.56, $p < 0.01$) were correlated with government intentions. Additionally, strong correlations were observed between the government framework, performance expectancy, and government intentions. However, the analysis showed no evidence of a correlation between information security and government intentions (r = 0.07, $p = 0.52$). Since correlation does not imply causation [55], the study could not confirm that information security may likely increase government intentions. Nevertheless, further testing is necessary to confirm the causal relationships between the independent and the dependent variables. Moreover, the analysis revealed evidence of a correlation between perceived risk (r = 0.22, $p < 0.01$) and government intentions. The moderate correlations among the variables also confirmed the evidence of no multicollinearity in the dataset [37,56].

Table 6. Results of VIF and TOL for the variables.

	Variables	Mean	SD	1	2	3	4	5
1	Privacy	3.72	1.03	1				
2	Government Framework	4.08	0.81	0.15 *	1			
3	Performance Expectancy	4.20	0.86	−0.09	0.53 **	1		
4	Information Security	3.91	1.22	0.18 **	−0.03	−0.08	1	
5	Perceived Risk	3.86	0.92	0.04	0.22 **	0.21 **	0.04	1
6	Government Intention	4.1	0.74	0.13 *	0.57 **	0.56 **	0.07	0.22 **

* $p < 0.05$ level (2-tailed); ** $p < 0.01$ level (2-tailed).

4.6. Structural Model and Hypothesis Testing

The study applied 2000 bootstrap samples at bias-corrected 95% confidence intervals [57–60]. The structural model in Figure 3 was tested using a structural equation model (SEM) with maximum likelihood estimation [61]. The moderator variables (perceived risk) and independent variables (privacy, government framework, performance expectancy, and information security) were mean-centred according to Shieh [38].

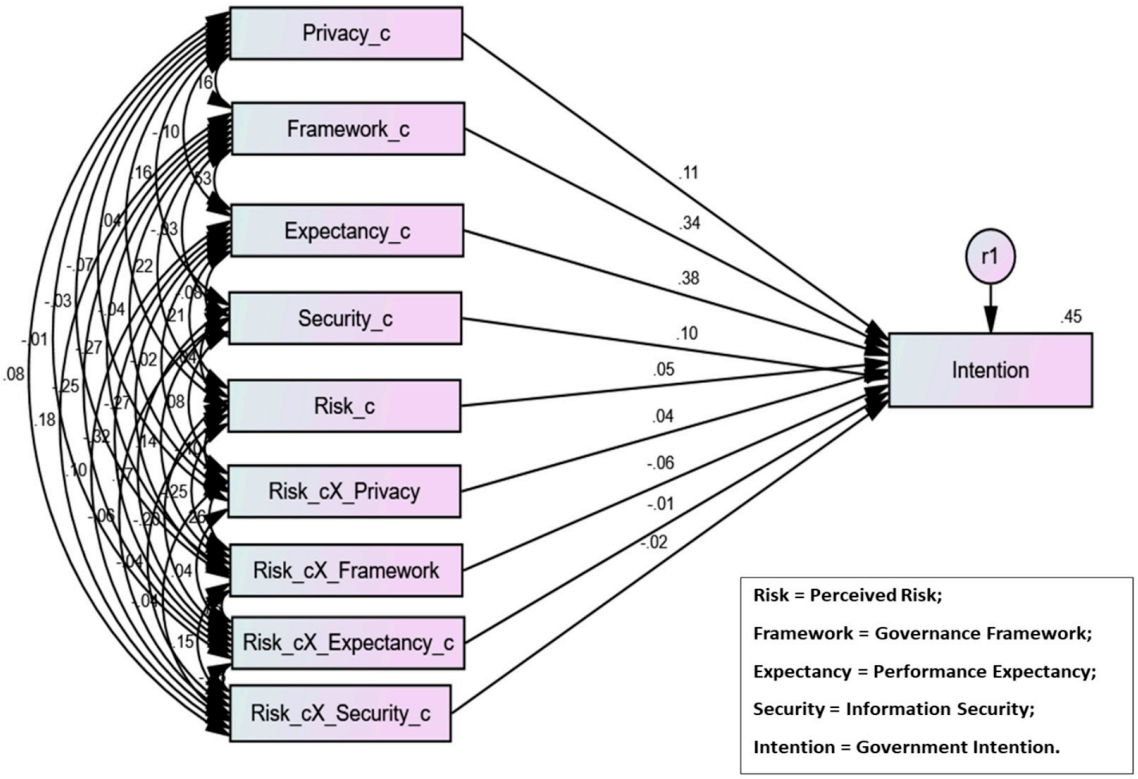

Figure 3. Structural path analysis model.

The structural path analysis model comprises the independent variables (privacy, government framework, performance expectancy, and information security), the moderating variable (perceived risk), the dependent variable (government intention), and the interaction terms (Risk_cX_Privacy, Risk_cX_Framework, Risk_cX_Expectancy, and Risk_cX_Security). These variables formed a single structural path analysis, tested simultaneously in Figure 3.

The path analysis result depicts the following, as listed in Table 7. In general, the model explained 45% of the variance ($R^2 = 0.45$) in government intention to adopt cloud services, indicating a moderate, but meaningful level of explanatory power at ($\beta = 0.45$, $p < 0.001$). Although this value is lower than those reported in some implementations of the original UTAUT model [7,62], it is consistent with technology adoption research within the public-sector and e-government context, where decision-making processes are inherently more complex [63].

1. H1 (Privacy → Intention)

Supported ($\beta = 0.11$, $p < 0.05$). Privacy significantly influences government intentions to adopt cloud services, though with a modest effect size.

2. H2 (Governance Framework → Intention)

Supported ($\beta = 0.34$, $p < 0.001$). Governance emerges as a strong predictor, underscoring the role of regulatory compliance and governance structures in driving adoption intentions for cloud services in government.

3. H3 (Performance Expectancy → Intention)

Supported ($\beta = 0.38$, $p < 0.001$). Performance expectancy was the most influential predictor, highlighting the centrality of the perceived benefits of cloud computing to government services. This suggests that perceived usefulness and efficiency gains significantly enhance adoption intention.

4. H4 (Information Security → Intention)

Supported (β = 0.10, $p < 0.05$). Despite weak correlations in the bivariate analysis, SEM confirmed that information security exerts a significant effect on government intention to adopt cloud services.

5. H5 (Moderation of Perceived Risk)

Not supported. Neither the direct effect of perceived risk (β = 0.50, $p = 0.46$) nor its interaction terms with the independent variables were statistically significant. This implies that the moderator's interactions do not substantially alter the direct relationship between the construct and the government's intention to adopt cloud services.

Table 7. Results of all analyses.

Relationships	Estimates	95% Confidence Intervals		Interpretations
		Lower Bounds	Upper Bounds	
Direct Effects				
Privacy → Government Intention	0.11 *	0.01	0.21	Significant
Government Framework → Government intention	0.34 ***	0.19	0.50	Significant
Performance Expectancy → Government intention	0.38 ***	0.21	0.55	Significant
Information Security → Government intention	0.10 *	0.00	0.19	Significant
Moderator Effect				
Perceived Risk → Government intention	0.50	−0.08	0.17	Non-Significant
Interaction Effects				
Perceived risk_x_Privacy → Government intention	0.04	−0.07	0.14	Non-Significant
Perceived risk_x_Government framework → Government intention	−0.06	−0.32	0.17	Non-Significant
Perceived risk_x_Performance expectancy → Government intention	−0.01	−0.26	0.23	Non-Significant
Perceived risk_x_Information security →Government intention	−0.02	−0.13	0.08	Non-Significant

*: significant at $p < 0.05$; ***: significant at $p < 0.0001$; x: moderates; →: influences.

5. Discussion

This study investigated the challenging factors influencing the Nigerian government's intention to adopt cloud services, guided by the UTAUT framework and adapted to include information security, governance, privacy, and perceived risk. The findings reveal several noteworthy insights. The results of the hypothesis testing confirm that privacy, governance framework, performance expectancy, and information security significantly influence government intention to adopt cloud services. This empirically validates the proposed model and aligns with prior studies that emphasise the multidimensional nature of cloud adoption decisions in the public sector [9,11].

The significant influence of privacy and information security on government intentions to adopt cloud services (H1—β = 0.11, $p < 0.05$) and (H4—β = 0.10, $p < 0.05$) respectively underscores that public institutions prioritise citizens' data protection and confirms perceived security measures directly affect adoption intentions. This reinforces prior studies highlighting privacy and information security as the cornerstone challenges for public-sector cloud adoption [5,16,17]. Furthermore, governments' perceptions about data location and sovereignty could influence trust in the cloud vendors. The findings suggest that privacy

and information security concerns should be given top priority in decision-making frameworks for public adoption, making privacy and security assessment an integral part of every cloud procurement and deployment stage.

Interestingly, while information security concerns are often portrayed as a barrier to adoption, our results show that perceived adequacy of cloud security controls positively predicts intention. This finding contrasts with studies that emphasise security as primarily an inhibitor [12]. One possible explanation is that Nigerian government personnel, particularly IT and privacy specialists, view security not as an absolute deterrent but as a manageable challenge when supported by governance frameworks and compliance mechanisms. This signals a shift from a "risk-avoidance" stance to a risk-management approach in cloud security adoption.

The government framework emerged as one of the strongest predictors (H2—$\beta = 0.34$, $p < 0.001$), indicating that clear institutional support through regulatory and compliance structures and enforcement mechanisms is critical to shaping adoption decisions. This finding aligns with recent research on government cloud strategies [11,13] and highlights the role of policy infrastructure as a trust enabler for cloud adoption. In the Nigerian context, this reinforces the need for a consistent policy and a harmonised governance framework that addresses both regulatory and operational uncertainties.

The performance expectancy displayed the highest predictive strength (H3—$\beta = 0.38$, $p < 0.001$) to the intention, reflecting respondents' strong belief that operational efficiency and service improvement strongly motivate government adoption. This result is consistent with the UTAUT literature [7,25,62] and highlights that, despite concerns about security and sovereignty, perceived benefits remain a decisive factor in driving adoption decisions in government settings. Additionally, demonstrating measurable improvements in process efficiency and transparency can significantly accelerate government adoption of cloud platforms.

Finally, the hypothesised moderating role of perceived risk (H5—$\beta = 0.50$, $p = 0.46$) was not supported. Neither privacy, nor governance, nor performance expectancy, nor information security was significantly influenced by risk perceptions in shaping adoption intentions. This challenges traditional perspectives [64–66] on the role of perceived risk in public-sector technology adoption. This may be related to a context-dependent environment, given the government's perspectives on sensitive issues such as information security, privacy, and performance expectations, which may limit the generalisability of the findings. Therefore, it underscores the importance of risk management protocols, encourages a government shift from reactive to proactive risk perception, and establishes standardised risk management as part of a strategic framework for cloud adoption.

The structural model explained 45% of the variance in government intention to adopt cloud services, indicating a moderate but meaningful explanatory power. This value is lower than that observed in some implementations of the original UTAUT model [7,62]. However, this is consistent with public-sector technology adoption research [63]. In the public sector of developing economies, cloud adoption decisions are shaped not only by individual-level perceptions but also by broader institutional, regulatory, infrastructural, and political constraints, which are difficult to operationalise within the behavioural intention framework. Therefore, the variance value should be interpreted as appropriate for this study context and align with the methodological guidance, which suggests that moderate variance values are common and acceptable in complex socio-technical research settings [67].

These insights contribute to the academic understanding of the government's priority for risk management in digital transformation and its practical implications for developing measures that encourage cloud adoption while ensuring robust security and compliance.

This suggests that once respondents recognise the functional and governance benefits, their risk concerns may recede in importance. Such a result aligns with studies on technology acceptance, which show that risk perceptions decrease as institutional trust and perceived usefulness increase [21,68]. For Nigerian government agencies, this may suggest that risk concerns are perceived as integrated into governance and compliance considerations rather than as an independent barrier.

5.1. Theoretical Contributions

Theoretically, this study extends the UTAUT model to the context of government cloud adoption, demonstrating its robustness while integrating constructs that reflect the public sector's security and governance imperatives. This study contributes to extending the UTAUT model in a developing-country government context, where cloud adoption decisions are shaped by institutional, regulatory, and governance constraints that differ from those in developed economies. Furthermore, the contextualised integration and empirical validation of privacy, information security, governance frameworks, and perceived risk within a single adoption model are applied to government cloud services in a developing nation.

By validating the model through CFA and structural path analysis, the research contributes to the growing literature on cloud adoption by demonstrating that technological adoption in government contexts is driven not only by performance expectancy but also by institutional trust, governance frameworks, and security assurance. Thus, findings support prior studies [11,13] that governance mechanisms significantly influence adoption and reinforce the need for holistic cloud governance frameworks [5] to address the challenges in the public sector.

This study further contributes to the growing body of academic knowledge by questioning the centrality of perceived risk in public institutions and, more specifically, to the understanding of the institutional dimensions of cloud adoption in a developing economy. This result introduces the important boundary condition for risk-based technology adoption theories. Additionally, it contributes to the intersection of cloud adoption, information security, and government IT governance.

1. Adaptation of UTAUT in government cloud adoption

By integrating constructs from privacy, information security, and governance frameworks, the study broadens UTAUT's explanatory scope in contexts where sovereignty and compliance play a decisive role.

2. Challenging the dominance of perceived risk

Contrary to previous studies [64–66], this study challenges traditional perspectives, and perceived risk did not moderate adoption intentions. These findings challenge security-risk-centric models of cloud adoption and suggest that risk is absorbed within governance and compliance frameworks rather than acting as an independent factor. Especially in an environment such as government, where perceived risk is considered context-dependent, this study therefore encourages a shift in government policy from reactive to proactive risk perception and the standardisation of risk management as part of the strategic framework for cloud adoption.

3. Empirical evidence from a developing economy

Most cloud adoption studies are situated in Western or advanced digital economies. By focusing on Nigeria, this study offers a rare empirical perspective from a developing country context, enriching the global IS security discourse and digital transformation.

5.2. Practical Implications

In practice, the study emphasises the need for survey instruments to strengthen governance frameworks, communicate the performance benefits, and reframe security as a strategic enabler rather than a deterrent. For policymakers, the results suggest that well-defined compliance mechanisms and transparent risk communication are more effective than simply emphasising threats. For IT leaders, demonstrating tangible efficiency gains can accelerate adoption and secure institutional support. The findings highlight several actionable points:

1. Strengthen governance frameworks

Clear regulatory guidance, effective compliance enforcement, and continuous policy updates are vital to reducing uncertainty and fostering trust in cloud adoption. The practical implications reemphasise the importance of maintaining cloud security and privacy compliance to protect government-critical data and ensure data sovereignty within a specific location, thereby reinforcing the need for transparency, reducing legal risks, ensuring trust in trans-border data, and encouraging the adoption of cloud services within the government. By addressing compliance and data sovereignty through a comprehensive governance framework, governments can build trust in cloud adoption, maximise cloud benefits, and maintain the integrity and security of their sensitive data assets.

The findings also suggest that government cloud adoption in Nigeria should not be framed exclusively as a policy-driven initiative but as a multi-layered governance challenge requiring a holistic national cloud framework. While Nigeria's National Cloud Computing Policy [69] provides important strategic direction, effective adoption depends on aligning regulatory oversight, institutional governance structures, information security controls, and organisational readiness across government entities. However, the strong influence of governance framework and performance expectancy reflects the institutional nature of cloud adoption decisions in the Nigerian public sector, where compliance, accountability, and inter-agency coordination play central roles.

In general, the results highlight the need for Nigeria to move beyond fragmented policy instruments towards a coordinated cloud governance ecosystem that supports secure, accountable, and scalable government cloud adoption.

2. Promote performance benefits

Demonstrating tangible efficiency and service delivery gains can help strengthen institutional buy-in and reduce resistance to cloud migration. Thus, the implications emphasised that prioritising performance in cloud adoption could help government organisations deliver reliable, cost-effective, and flexible digital services, thereby enhancing public trust and operational effectiveness. Furthermore, governance frameworks could provide the legal and regulatory safeguards needed to ensure secure cloud adoption, thereby promoting accountability and public trust within government agencies and among citizens.

3. Reframe security concerns

Rather than viewing security as a barrier, governments should position it as a strategic enabler, emphasising security-by-design, adherence to international standards, domestication to suit developing nations' security priorities, and transparency from cloud service providers. Similarly, the significance of information security underscores the need for standardised security architectures, certification mechanisms, and enforcement structures that extend beyond policy statements. Moreover, it encourages developing a holistic cloud information security and privacy framework to improve government adoption intentions for cloud [5].

4. Risk communication

Since perceived risk did not independently moderate adoption, communication strategies should focus less on risk avoidance and more on risk management capacity, showcasing how governance and compliance mechanisms mitigate threats. The broad context of these findings emphasises the importance of a robust governance framework and trust-building mechanisms in diminishing the role of risk perception as a barrier to technology adoption in the public sector. More importantly, in cultural and institutional contexts, the findings reflect hierarchical decision-making and regulatory compliance norms prevalent in developing economies, which shape how risk and trust are interpreted in technological innovation. These contextual factors underscore that cloud adoption in government is not merely a technical decision but a governance and policy transformation challenge.

These findings suggest prioritising and strengthening governance frameworks that embed risk management, as well as ensuring compliance with regulatory standards, to facilitate adoption and reduce the deterrent impact of perceived risks, thereby reassuring stakeholders and maintaining public trust. This synthesis provides a pathway for future research to refine technology acceptance models for secure and accountable digital governance.

5.3. Study Limitations

Like all empirical studies, this work has limitations. Its geographic focus on Nigeria may limit generalisability, and its cross-sectional design restricts causal inference. Nonetheless, these findings open pathways for future research, including comparative cross-country analyses, longitudinal studies, and mixed-method investigations that integrate objective security performance data with perceptions. Furthermore, although perceived risk did not moderate the proposed relationship, future studies could explore its role as a mediating construct or examine specific risk dimensions using a mixed-methods approach.

While the study recognises the importance of formal threat modelling and detailed security validation in cloud computing research, its focus is not on technical threat quantification or system-level evaluations, but rather on a quantitative approach using SEM to test behavioural hypotheses. This is to understand the perceived risks and behavioural determinants that influence government cloud adoption decisions.

The constructs of information security, privacy, performance expectancy, governance frameworks, and perceived risks are therefore operationalised as cognitive and governance-related perceptions derived from decision-maker assessments of organisational vulnerabilities, regulatory readiness, and trust in the service. Future research could extend this work by integrating quantitative or simulation-based threat analysis and system-level evaluations into risk assessment to complement behavioural perspectives.

6. Conclusions

This study investigated the factors that challenge the Nigerian government's intention to adopt cloud services, using an adapted UTAUT framework that incorporated privacy, governance framework, information security, and performance expectancy, with perceived risk as a moderating factor. Drawing on survey data from 230 respondents across ministries, departments, and agencies, the study offers new insights into how institutional and technological considerations intersect in the context of public-sector cloud adoption.

The findings reveal four important conclusions. First, privacy, governance frameworks, performance expectancy, and information security significantly predict a government's intention to adopt cloud services. This underscores the dual importance of technical safeguards and institutional mechanisms in enabling adoption. Second, performance

expectancy emerged as the strongest determinant, highlighting that perceived improvements in efficiency and service delivery remain central motivators for adoption, even in environments where security and sovereignty concerns are pronounced. Third, information security was not found to be an absolute barrier; rather, when supported by strong governance frameworks, it became a positive predictor of intention, suggesting a shift toward risk-management-oriented adoption strategies. Finally, perceived risk did not moderate the identified relationships, challenging assumptions that risk independently hinders adoption. Instead, risk appears to be internalised within broader governance and compliance considerations.

This research shows that successful government cloud adoption is less about eliminating risks outright and more about institutionalising governance and demonstrating value. By situating cloud adoption within a security-aware yet performance-driven framework, governments can both safeguard citizen data and unlock the digital transformative potential of cloud technologies. Moreover, the study achieves its contributions by adapting the UTAUT model to incorporate constructs that capture institutional and security-oriented dimensions, thereby contextualising behavioural adoption theory in the public sector. It validates the frameworks using quantitative data from Nigerian government organisations, offering policymakers and practitioners evidence-based insights by identifying governance and security factors that enhance institutional trust and promote effective digital transformation initiatives.

While this study provides valuable insights into the organisational and challenging factors influencing government adoption of cloud services, it does not encompass system-level experimentation or technical performance evaluation. However, future research could be extended to incorporate experimental or simulation-based evaluation to assess the ethical feasibility and performance implications of the proposed information security, privacy, performance expectancy, governance, and perceived risk constructs in real-world cloud and edge environments. Such an integration approach would further strengthen the bridge between behavioural adoption models and technical implementation realities, ensuring more comprehensive policy and architectural recommendations for secure government cloud deployment.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/info17050440/s1, File S1: Study Dataset.

Author Contributions: Conceptualisation, N.U., J.A.G. and K.P.; methodology, N.U., J.A.G. and K.P.; software, N.U.; validation, N.U. and J.A.G.; formal analysis, N.U.; investigation, N.U.; resources, N.U. and J.A.G.; data curation, N.U.; writing—original draft preparation, N.U.; writing—review and editing, N.U., J.A.G. and K.P.; visualisation, N.U. supervision, J.A.G. and K.P.; project administration, J.A.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Auckland University of Technology Ethics Committee (AUTEC) (document number 22/232, dated 2 November 2022). Informed consent was obtained from all participants.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study (see Figure A1 for a copy of the consent form).

Data Availability Statement: The original contributions presented in this study are included in the Supplementary Materials. Further inquiries can be directed to the corresponding author.

Acknowledgments: The authors acknowledge the National Information Technology Development Agency (NITDA), Nigeria, for the PhD research sponsorship support. This article is part of the PhD study of the first author.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AMOS	Analysis of Moment Structures
AVE	Average Variance Extracted
CFA	Confirmatory Factor Analysis
CFI	Comparative Fit Index
CMB	Common Method Bias
CR	Composite Reliability
IFI	Incremental Fit Index
IT	Information Technology
MDAs	Ministry, Departments, and Agencies
PII	Personally Identifiable Information
RMSEA	Root Mean Square Error of Approximation
SEM	Structural Equation Model
SPSS	Statistical Package for the Social Sciences
SRMR	Standardised Root Mean Square Residual
TLI	Tucker–Lewis Index
TOL	Tolerance Limit
UTAUT	Unified Theory of Acceptance and Use of Technology
VIF	Variance Inflation Factor

Appendix A

AUT
TE WĀNANGA ARONUI O TĀMAKI MAKAU RAU

Consent Form

Project title: *Information Security and Privacy Challenges of Cloud-based Computing: A Government Perspective*

Project Supervisor: *Prof. Jairo Gutierrez*

Dr. Krassie Petrova

Researcher: *Ndukwe Ukeje*

- ○ I have read and understood the information provided about this research project in the Information Sheet dated 02 November 2022.
- ○ I have had an opportunity to ask questions and to have them answered.
- ○ I understand that participating in this study is voluntary (my choice) and that I may withdraw from the study at any time without being disadvantaged.
- ○ I understand that the research will protect my confidentiality by identifying, classifying, and coding the information based on organisations, job roles and types. The identity and details of the potential participants will be intentionally concealed and will not in any way be revealed.
- ○ I understand that if I withdraw from the study, I will be offered the choice between removing any data that is identifiable as belonging to me or allowing it to continue to be used. However, once the findings have been produced, removal of my data may not be possible.
- ○ I agree to take part in this research and agree to its publication online and reuse for research purposes.
- ○ I understand that there is no financial compensation from the research, or if published as an article.
- ○ I wish to receive a summary of the research findings through publications and other means (please tick one): Yes○ No○

Participant's signature: .....

Participant's name: .....

Participant's Contact Details (if appropriate):

.....

.....

.....

.....

Date :

Approved by the Auckland University of Technology Ethics Committee on 02 November 2022, AUTEC Reference number 22/232

Note: The participants should retain a copy of this form.

Figure A1. Participants' consent form.

Table A1. Survey instrument as adopted [31].

Constructs	Measurement Items	Questions	Factor Loadings
Privacy	Priva1	I think using government cloud services will expose my privacy	0.803
	Priva2	I will use government cloud services, knowing my privacy is safe	0.704
	Priva3	Existing government regulations are enough to safeguard my privacy	0.907
	Priva4	Privacy issues are a significant challenge to adopting government cloud services	0.842
Governance framework	GovtF2	I will use government cloud services, given the available governance framework	0.737
	GovtF3	A governance framework will help to safeguard my information while utilising cloud services.	0.637
	GovtF4	Having a governance framework will encourage me to accept cloud services	0.749
	GovtF5	I feel that the government's intention to adopt cloud services will improve citizens' participation in governance	0.658
	GovtF6	I feel that government regulations and laws are sufficient to protect the government's critical information in the cloud	0.748
	GovtF7	I feel that having a governance framework will encourage the government's intention to adopt cloud services	0.454
	GovtF8	I feel that government regulations and laws are sufficient to protect citizens' privacy in the cloud	0.762
Performance expectancy	PerfEx1	I feel that cloud computing will be helpful in my daily activities	0.862
	PerfEx2	Using cloud services will increase my productivity	0.862
	PerfEx3	Cloud computing will improve citizens' participation and efficiency in governance	0.78
	PerfEx4	Cloud computing will improve my job performance	0.886
Information security	InfoSec1	I feel that using cloud services will not keep government information safe	0.912
	InfoSec2	Security will influence the government and citizens' adoption of cloud computing	0.946
	InfoSec3	I feel that cloud services are safe to transmit my sensitive information	0.908
	InfoSec4	I will feel secure providing my sensitive information to government cloud services	0.952
Perceived risk	PerRisk1	I feel unsafe providing my personally identifiable information while using cloud services	0.812
	PerRisk2	I am worried about the likelihood of safe cloud services without a governance framework	0.842
	PerRisk3	I am worried that the likelihood of information leaks on the cloud services will affect my performance	0.849
	PerRisk4	I am worried that the likelihood of citizens' information security exposure will depend on the cloud service's safety	0.705

Table A1. *Cont.*

Constructs	Measurement Items	Questions	Factor Loadings
Government intention	GovtInt1	I feel that the government's intention to adopt cloud services will depend on information security measures	0.711
	GovtInt2	I feel that the government's likelihood of losing data and reputation will determine its intention to adopt cloud services	0.848
	GovtInt3	I think the loss of citizen-identifiable information will determine the government's intention to adopt cloud services	0.762
	GovtInt4	I think service delivery performance improvement will determine the government's intention to adopt cloud computing	0.442
	GovtInt5	I feel that having a governance framework will encourage the government's intention to adopt cloud computing	0.792
	GovtInt6	I feel that the government's intention to adopt cloud service will improve citizens' participation in governance	0.612

References

1. Kanchepu, N. Digital transformation in banking industry: Cloud computing as a key enabler. *Int. Numer. J. Mach. Learn. Robot.* **2023**, *7*, 7654.
2. Ogugua Chimezie, O.; Samuel Onimisi, D.; Andrew Ifesinachi, D.; Onwusinkwue, S.; Onyinyechi Vivian, A.; Islam Ahmad Ibrahim, A. Review of Evolving Cloud Computing Paradigms: Security, Efficiency, and Innovations. *Comput. Sci. IT Res. J.* **2024**, *5*, 270–292. [CrossRef]
3. Alamri, N.; Alzahrani, S. Navigating the Clouds: An Exploratory Research of Cloud Computing Adoption in Saudi Arabia's Small and Medium Enterprises. *Eng. Technol. Appl. Sci. Res.* **2024**, *14*, 17859–17869. [CrossRef]
4. Qatawneh, N. Building a framework to drive government systems' adoption of cloud computing through IT knowledge. *Discov. Sustain.* **2024**, *5*, 282. [CrossRef]
5. Ukeje, N.; Gutierrez, J.; Petrova, K. Information security and privacy challenges of cloud computing for government adoption: A systematic review. *Int. J. Inf. Secur.* **2024**, *23*, 1459–1475. [CrossRef]
6. Akinnuwesi, B.A.; Uzoka, F.-M.E.; Fashoto, S.G.; Mbunge, E.; Odumabo, A.; Amusa, O.O.; Okpeku, M.; Owolabi, O. A modified UTAUT model for the acceptance and use of digital technology for tackling COVID-19. *Sustain. Oper. Comput.* **2022**, *3*, 118–135. [CrossRef]
7. Venkatesh, V.; Morris, M.G.; Davis, G.B.; Davis, F.D. User Acceptance of Information Technology: Toward a Unified View. *MIS Q.* **2003**, *27*, 425–478. [CrossRef]
8. Andrews, J.E.; Ward, H.; Yoon, J. UTAUT as a Model for Understanding Intention to Adopt AI and Related Technologies among Librarians. *J. Acad. Librariansh.* **2021**, *47*, 102437. [CrossRef]
9. Al Mudawi, N.; Beloff, N.; White, M. *Developing a Framework of Critical Factors Affecting the Adoption of Cloud Computing in Government Systems (ACCE-GOV)*; Springer: Cham, Switzerland, 2022; pp. 520–538.
10. Maurer, T.; Hinck, G. *Cloud Security: A Primer for Policymakers*; Carnegie Endowment for International Peace: Washington, DC, USA, 2020.
11. Choi, G.-Y.; Seo, J.; Kwon, H.-Y. A Comparative Study of National Cloud Security Strategy and Governance. In Proceedings of the 25th Annual International Conference on Digital Government Research, Taipei, Taiwan, 11–14 June 2024; pp. 241–250.
12. Mitchell, A.D.; Samlidis, T. Cloud services and government digital sovereignty in Australia and beyond. *Int. J. Law Inf. Technol.* **2022**, *29*, 364–394. [CrossRef]
13. Jiménez, D.L.; Dittmar, E.C.; Portillo, J.P.V. Political, Regulatory, and Ethical Concerns of AI, Blockchain, and Cloud Computing in Public Administration. In *Harnessing AI, Blockchain, and Cloud Computing for Enhanced E-Government Services*; IGI Global Scientific Publishing: Hershey, PA, USA, 2025; pp. 33–62.
14. Obia, V. Digital policy and Nigeria's Platform Code of Practice: Towards a radical co-regulatory turn. *Data Policy* **2025**, *7*, e12. [CrossRef]

15. Almahameed, A.A.; Pelegrín-Borondo, J.; López-Galiacho Perona, J.L.; Arias-Oliva, M. Sovereignty, Surveillance, and the Cloud: Geopolitical and Ethical Issues of Global Cloud Computing. In *Ethical and Social Impacts of Information and Communication Technology*; Alvarez, I., Arias-Oliva, M., Dediu, A.-H., Silva, N., Eds.; Springer: Cham, Switzerland, 2026.
16. Ometov, A.; Molua, O.L.; Komarov, M.; Nurmi, J. A Survey of Security in Cloud, Edge, and Fog Computing. *Sensors* **2022**, *22*, 927. [CrossRef]
17. Abdulsalam, Y.S.; Hedabou, M. Security and Privacy in Cloud Computing: Technical Review. *Future Internet* **2022**, *14*, 11. [CrossRef]
18. Jianwen, C.; Wakil, K. A model for evaluating the vital factors affecting cloud computing adoption. *Kybernetes* **2020**, *49*, 2475–2492. [CrossRef]
19. Li, M.; Peng, C.; Liu, H.; Tang, H.; Niu, J.; Cai, C.; Zhang, T. Lightweight Traceable Data Circulation Encryption Scheme for Edge Computing. *Concurr. Comput. Pract. Exp.* **2025**, *37*, e70294. [CrossRef]
20. Sun, Y.; Liu, Q.; Chen, X.; Du, X. An Adaptive Authenticated Data Structure with Privacy-Preserving for Big Data Stream in Cloud. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3295–3310. [CrossRef]
21. Abd Al Ghaffar, H.-t.-A.N. Government cloud computing and national security. *Rev. Econ. Political Sci.* **2024**, *9*, 116–133. [CrossRef]
22. Prakash, S.; Malaiyappan, J.N.A.; Thirunavukkarasu, K.; Devan, M. Achieving regulatory compliance in cloud computing through ML. *AIJMR-Adv. Int. J. Multidiscip. Res.* **2024**, *2*, 1–15.
23. Merlo, T.R.; Fard, F.; Hawamdeh, S. Cloud Computing's Impact on the Digital Transformation of the Enterprise: A Mixed-Methods Approach. *Sustainability* **2025**, *17*, 5755. [CrossRef]
24. Creswell, J.W. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 4th ed.; SAGE Publications: Thousand Oaks, CA, USA, 2014.
25. Venkatesh, V.; Thong, J.Y.; Xu, X. Unified theory of acceptance and use of technology: A synthesis and the road ahead. *J. Assoc. Inf. Syst.* **2016**, *17*, 328–376. [CrossRef]
26. Danila, R.; Saat, R.M.; Bahador, K.M.K. Trust and Religiosity: Integrating Technological Acceptance Factors into the Extended Unified Theory of Acceptance and Use of Technology (UTAUT) Model for Zakat Online Payment Systems. *J. Adv. Res. Appl. Sci. Eng. Technol.* **2025**, *53*, 199–214. [CrossRef]
27. Fachrudin, K.A.; Amin, S.I.M.; Ab Hamid, S.N.; Latifah, S.; Lubis, M.A. Which UTAUT Elements Drive Mobile Banking Adoption in Indonesia, Despite Security and Trust Concerns? *J. Ecohumanism* **2025**, *4*, 682–693. [CrossRef]
28. Omar, A.; Tiwari, V.; Saad, M. Smart technology's potential in smart destinations: A comprehensive UTAUT model with privacy and safety risk moderation. *J. Hosp. Tour. Technol.* **2025**, *16*, 817–835. [CrossRef]
29. Joshi, J.B.D.; Ghafoor, A.; Aref, W.G.; Spafford, E.H. Security and Privacy Challenges of a Digital Government. In *Advances in Digital Government: Technology, Human Factors, and Policy*; McIver, W.J., Elmagarmid, A.K., Eds.; Springer: Boston, MA, USA, 2002; pp. 121–136.
30. Khan, A.; Ibrahim, M.; Hussain, A. An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. *Int. J. Inf. Manag. Data Insights* **2021**, *1*, 100015. [CrossRef]
31. Chitra, M.; Surianarayanan, R.; Mahamuni, V.S.; Mohammed, S.; Keno, M.T.; Boopathi, S. Study on Cloud Computing-Empowered Small and Medium Enterprises. In *Essential Information Systems Service Management*; IGI Global: Hershey, PA, USA, 2025; pp. 189–220.
32. Ukeje, N.; Gutierrez, J.A.; Petrova, K.; Okolie, U.C. An Exploratory Factor Analysis Approach on Challenging Factors for Government Cloud Service Adoption Intention. *Future Internet* **2025**, *17*, 326. [CrossRef]
33. Wolf, C.; Joye, D.; Smith, T.; Fu, Y.-C. *The SAGE Handbook of Survey Methodology*; SAGE Publications: Thousand Oaks, CA, USA, 2016. [CrossRef]
34. Bhattacherjee, A. *Social Science Research: Principles, Methods, and Practices*; University of South Florida: Tampa, FL, USA, 2012.
35. Edgar, T.; Manz, D. *Research Methods for Cyber Security*; Elsevier Science & Technology Books: Rockland, MA, USA, 2017.
36. Hu, L.T.; Bentler, P.M. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Struct. Equ. Model. A Multidiscip. J.* **1999**, *6*, 1–55. [CrossRef]
37. Hair, J.F., Jr. *Multivariate Data Analysis*, 7th ed.; Pearson/Prentice Hall: Upper Saddle River, NJ, USA, 2010.
38. Shieh, G. Clarifying the role of mean centring in multicollinearity of interaction effects. *Br. J. Math. Stat. Psychol.* **2011**, *64*, 462–477. [CrossRef] [PubMed]
39. Shrestha, N. Detecting multicollinearity in regression analysis. *Am. J. Appl. Math. Stat.* **2020**, *8*, 39–42. [CrossRef]
40. Hushchyna, K.; Sabir, Q.U.A.; McLellan, K.; Nguyen-Quang, T. Multicollinearity and Multi-regression Analysis for Main Drivers of Cyanobacterial Harmful Algal Bloom (CHAB) in the Lake Torment, Nova Scotia, Canada. *Environ. Model. Assess.* **2023**, *28*, 1011–1022. [CrossRef]
41. Harman, H.H. *Modern Factor Analysis*; University of Chicago press: Chicago, IL, USA, 1976.

42. Podsakoff, P.M.; MacKenzie, S.B.; Podsakoff, N.P. Sources of method bias in social science research and recommendations on how to control it. *Annu. Rev. Psychol.* **2012**, *63*, 539–569. [CrossRef]
43. Saxena, M.; Bagga, T.; Gupta, S.; Kaushik, N. Exploring Common Method Variance in Analytics Research in the Indian Context: A Comparative Study with Known Techniques. *FIIB Bus. Rev.* **2022**, *13*, 553–569. [CrossRef]
44. Mishra, P.; Pandey, C.M.; Singh, U.; Gupta, A.; Sahu, C.; Keshri, A. Descriptive statistics and normality tests for statistical data. *Ann. Card. Anaesth.* **2019**, *22*, 67–72. [CrossRef] [PubMed]
45. Stevens, J. *Applied Multivariate Statistics for the Social Sciences*, 5th ed.; Routledge: New York, NY, USA, 2009.
46. Bentler, P.M.; Bonett, D.G. Significance tests and goodness of fit in the analysis of covariance structures. *Psychol. Bull.* **1980**, *88*, 588. [CrossRef]
47. West, S.G.; Wu, W.; McNeish, D.; Savord, A. Model fit in structural equation modeling. *Handb. Struct. Equ. Model.* **2023**, *2*, 184–205.
48. Cheung, G.W.; Cooper-Thomas, H.D.; Lau, R.S.; Wang, L.C. Reporting reliability, convergent and discriminant validity with structural equation modeling: A review and best-practice recommendations. *Asia Pac. J. Manag.* **2023**, *41*, 745–783. [CrossRef]
49. Fornell, C.; Larcker, D.F. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]
50. Sarstedt, M.; Ringle, C.M.; Hair, J.F. Partial least squares structural equation modeling. In *Handbook of Market Research*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 587–632.
51. Brunelle, E.; Lapierre, J. Examining the Relationship Between Individual Characteristics, Product Characteristics, and Media Richness Fit on Consumer Channel Preference. In Proceedings of the E-Commerce and Web Technologies, Berlin/Heidelberg, Germany, 3–7 September 2007; pp. 56–67.
52. Lam, L.W. Impact of competitiveness on salespeople's commitment and performance. *J. Bus. Res.* **2012**, *65*, 1328–1334. [CrossRef]
53. Menguc, B.; Auh, S. Creating a firm-level dynamic capability through capitalizing on market orientation and innovativeness. *J. Acad. Mark. Sci.* **2006**, *34*, 63–73. [CrossRef]
54. DeMaris, A. *Regression with Social Data: Modeling Continuous and Limited Response Variables*; Wiley: Indianapolis, IN, USA, 2004.
55. Bracke, S. Correlation and Regression. In *Reliability Engineering: Data Analytics, Modeling, Risk Prediction*; Bracke, S., Ed.; Springer: Berlin/Heidelberg, Germany, 2024; pp. 181–200.
56. Byrne, B.M. *Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming*, 3rd ed.; Routledge: New York, NY, USA; London, UK, 2016.
57. Talsma, K.; Schüz, B.; Schwarzer, R.; Norris, K. I believe, therefore I achieve (and vice versa): A meta-analytic cross-lagged panel analysis of self-efficacy and academic performance. *Learn. Individ. Differ.* **2018**, *61*, 136–150. [CrossRef]
58. Sánchez-Álvarez, N.; Extremera, N.; Fernández-Berrocal, P. The influence of trait meta-mood on subjective well-being in high school students: A random intercept cross-lagged panel analysis. *Educ. Psychol.* **2019**, *39*, 332–352. [CrossRef]
59. Prikhodkina, M.; Melnikov, S. Factors that influence medication adherence in women with fibromyalgia: A path analysis. *J. Clin. Nurs.* **2024**, *33*, 3943–3953. [CrossRef]
60. Zhang, L.; Guo, X. Social support on calling: Mediating role of work engagement and professional identity. *Career Dev. Q.* **2023**, *71*, 97–110. [CrossRef]
61. Okolie, U.C. Work placement learning and students' readiness for school-to-work transition: Do perceived employability and faculty supervisor support matter? *J. Vocat. Behav.* **2022**, *139*, 103805. [CrossRef]
62. Venkatesh, V.; Thong, J.Y.L.; Xu, X. Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Q.* **2012**, *36*, 157–178. [CrossRef]
63. Dwivedi, Y.K.; Rana, N.P.; Jeyaraj, A.; Clement, M.; Williams, M.D. Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a Revised Theoretical Model. *Inf. Syst. Front.* **2019**, *21*, 719–734. [CrossRef]
64. Akram, M.S.; Malik, A.; Shareef, M.A.; Awais Shakir Goraya, M. Exploring the interrelationships between technological predictors and behavioral mediators in online tax filing: The moderating role of perceived risk. *Gov. Inf. Q.* **2019**, *36*, 237–251. [CrossRef]
65. Kumar, R.; Singh, R.; Kumar, K.; Khan, S.; Corvello, V. How Does Perceived Risk and Trust Affect Mobile Banking Adoption? Empirical Evidence from India. *Sustainability* **2023**, *15*, 4053. [CrossRef]
66. Mutahar, A.M.; Aldholay, A.; Isaac, O.; Jalal, A.N.; Kamaruddin, F.E.B. The Moderating Role of Perceived Risk in the Technology Acceptance Model (TAM): The Context of Mobile Banking in Developing Countries. In Proceedings of the International Conference on Emerging Technologies and Intelligent Systems, Cham, Switzerland, 2–3 September 2022; pp. 389–403.
67. Hair, J.F.; Risher, J.J.; Sarstedt, M.; Ringle, C.M. When to use and how to report the results of PLS-SEM. *Eur. Bus. Rev.* **2019**, *31*, 2–24. [CrossRef]

68. Sun, P. Security and privacy protection in cloud computing: Discussions and challenges. *J. Netw. Comput. Appl.* **2020**, *160*, 102642. [CrossRef]
69. NITDA. National Cloud Policy. 2025. Available online: www.nitda.gov.ng (accessed on 24 December 2025).