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

Ndukwe Ukeje , Jairo Gutierrez , Krassie Petrova *

Posted Date: 4 December 2025

doi: 10.20944/preprints202512.0357.v1

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

 doi:10.20944/preprints202512.0357.v1

Article

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

Ndukwe Ukeje, Jairo A. Gutierrez and Krassie Petrova *

Auckland University of Technology, Auckland, New Zealand

* 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

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

 doi:10.20944/preprints202512.0357.v1

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 information security, privacy, performance expectancy, and governance framework constructs influence governments' intention to adopt cloud services?
2. How does perceived risk moderate the relationship between these constructs and the government's adoption intention?

The contribution of this study is in twofold (theoretical and practical). Theoretically, it advances the understanding of cloud adoption in the public sector by adapting UTAUT to incorporate constructs that are critical in security-sensitive contexts. Practically, the study offers recommendations for policymakers and practitioners seeking to mitigate adoption barriers, strengthen governance mechanisms, and enhance trust in cloud-based public services. The study situates government cloud adoption within the broader discourse of secure digital transformation by emphasising trust, security, and regulatory compliance.

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 and outlines the research methodology, including the procedures for data collection and analysis. Section 4 presents the empirical findings and analysis. Sections 5 discusses the theoretical contributions and the and practical implications of the study and its limitations. Section 6 concludes with a summary of the study and its key points.

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 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 reported efficiency gains and operational resilience through the use of cloud-based solutions, while developing economies view

 doi:10.20944/preprints202512.0357.v1

cloud services as enablers for bridging digital transformation [10]. Thus, cloud adoption promises not only economic efficiency but also improved public value creation.

2.2. Policy and Strategic Frameworks for Cloud Adoption

Policy frameworks play a decisive role in shaping government cloud strategies. The United States pioneered policy-driven adoption through the Cloud First (2010) and Cloud Smart (2019) initiatives, which emphasised security, procurement optimisation, and workforce readiness [10]. In Europe, the United Kingdom's G-Cloud framework provides a procurement mechanism designed to lower barriers to entry while embedding compliance obligations [11]. Australia's Cloud Computing Policy prioritises risk management and cost efficiency [12], while digital transformation strategies in developing countries, such as Nigeria, explore regulatory initiatives necessary to drive cloud adoption and ensure data sovereignty measures.

Yet, studies warn that policy-driven frameworks often underperform if not supported by strong information security governance. Choi et al. (2023) argue that cloud-first policies must be coupled with continuous security monitoring and compliance enforcement to ensure long-term sustainability. Similarly, demonstrate that security governance frameworks are crucial to establishing trust in sovereign cloud infrastructures. These findings highlight that while policy frameworks stimulate adoption, the persistence of barriers necessitates the embedding of governance and security into policy implementation.

2.3. Information Security, Privacy, and Sovereignty Challenges

Despite the benefits of cloud adoption, governments still face significant inhibitors rooted in the sensitivity of public data and the criticality of government operations. Studies consistently identify information security and privacy challenges as primary barriers [5,13–15]. Breaches in confidentiality, integrity, or availability can undermine citizen trust, disrupt services, and even compromise national security.

Privacy-preserving mechanisms, such as encryption, anonymisation, and advanced access controls, have been proposed [16], but their implementation remains uneven. Abd Al Ghaffar [17] introduces a risk-based assessment framework tailored to government adoption, underscoring the importance of aligning security strategies with regulatory contexts.

The challenge extends beyond technical security to issues of digital sovereignty and trust. European governments, in particular, emphasise sovereignty concerns over reliance on foreign-controlled cloud providers [12]. Similarly, Jiménez, *et al.* [18] argue that sovereignty and trust shape government adoption decisions as much as technical safeguards do. In practice, sovereignty concerns manifest in requirements for local data residency, compliance with national security regulations, and preference for sovereign cloud providers.

Finally, perceived risks play a crucial role in shaping adoption intentions. Prakash, *et al.* [19] show that risks related to service downtime, vendor lock-in, and regulatory non-compliance often amplify reluctance, even when safeguards are in place. This aligns with Al Mudawi, Beloff and White [9] demonstration, that governments frequently trade efficiency gains for stronger security guarantees, illustrating the complex interplay between opportunities and risks in public-sector adoption.

2.4. Theoretical Models and Research Gaps

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, in the public sector, the model has limitations. Specifically, UTAUT does not explicitly account for security, privacy, governance, and sovereignty constructs, which are central to government cloud adoption [13,18].

 doi:10.20944/preprints202512.0357.v1

Scholars have increasingly called for extended models that integrate these constructs. Abdulsalam and Hedabou [14] stressed that without explicitly addressing security and privacy concerns, models risk oversimplifying government decision-making. Jiménez, Dittmar and Portillo [18] highlighted trust and sovereignty as under-theorised determinants in adoption frameworks. Similarly, Prakash, Malaiyappan, Thirunavukkarasu and Devan [19] emphasised that perceived risk functions as a moderating factor that shapes the influence of other constructs.

This study addresses these gaps by adapting UTAUT to integrate constructs of information security, privacy, performance expectancy, and governance frameworks, with perceived risk conceptualised as a moderator. 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 [20]. 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.* [21] noted, boundary conditions remain unexplored, particularly in sector-specific contexts such as government.

The public sector presents such a distinct context, where 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 [6,22–24]. 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.

 doi:10.20944/preprints202512.0357.v1

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 into UTAUT and extends its explanatory relevance to cloud security contexts in government.

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.

1. Privacy

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

2. Governance Framework

National laws, compliance regimes, and sovereignty requirements dictate how cloud adoption unfolds in government [25]. 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[26]. 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[27].

Adapting UTAUT with these constructs enables the development of a model that is both theoretically rigorous and contextually relevant [28]. The conceptual model is presented in Figure 1. Based on the adapted UTAUT, the following hypotheses are formulated:

H1: *Privacy has a significant positive influence on the government's intention to adopt cloud services.*

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

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

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.*

 doi:10.20944/preprints202512.0357.v1

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

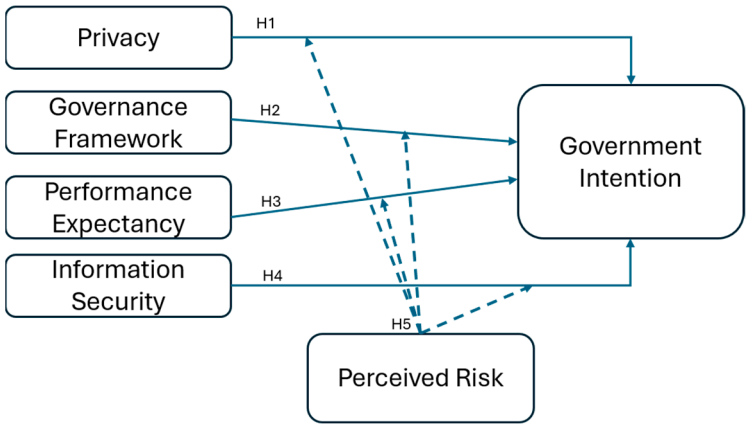

Figure 1. Proposed conceptual model (Adapted from [7]).

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 [28] were used to measure the items. 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) [28].

The survey instrument was administered electronically through Qualtrics, which ensured anonymity, reduced administrative costs, and increased accessibility. Ethical principles of confidentiality and voluntary participation were observed, consistent with research best practices [20,29].

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 [30,31]. This ensured that only participants with relevant expertise contributed data, thereby enhancing the validity of responses.

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 [29] and the study's ethical approval. Invitations were distributed to approximately 90 government organisations, yielding 230 valid responses suitable for analysis. The overall response rate was considered satisfactory for organisational surveys, with no evidence of non-response bias.

 doi:10.20944/preprints202512.0357.v1

3.4. Data Analysis Methods

The collected data were analysed using SPSS (v.29) for descriptive statistics, and AMOS (v.29) for Confirmatory Factor Analysis (CFA) and Structural Equation Modelling (SEM). A two-stage approach was conducted:

3.4.1. Measurement Model Analysis

Confirmatory Factor Analysis (CFA) was conducted to confirm the validity of the constructs and the reliability of the measurement items. A model fit was evaluated using the multiple indices $\chi^2/df \leq 3.0$, Comparative Fit Index (CFI ≥ 0.90), Tucker–Lewis Index (TLI ≥ 0.90), Incremental Fit Index (IFI ≥ 0.90), Standardised Root Mean Square Residual (SRMR ≤ 0.08), and Root Mean Square Error of Approximation (RMSEA ≤ 0.06) [32,33]. The CFA was conducted in AMOS.

3.4.2. Structural Model Testing

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 path coefficients were estimated using maximum likelihood estimation. Moderator effects of Perceived Risk were examined using mean-centring and interaction terms [34]. 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 < 4.0) and tolerance limit (TOL ≤ 1) [33,35,36], as well as common method bias (CMB) testing using Harman's single-factor test [37–39].

4. Results

4.1. Descriptive Statistics

Descriptive statistics were computed to characterise the respondents and provide insight into their background, experience, and perceptions [40]. Out of 230 valid responses, 196 (85.6%) were IT practitioners, administrators, or personnel with expertise in information security and privacy. This indicates that the majority of respondents possessed relevant technical knowledge, strengthening the credibility of the dataset.

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. [32] threshold criterion for fit indices in structure analysis was applied to to validate the six-factor measurement model (Privacy, Governance Framework, Performance Expectancy, Information Security, Perceived Risk, and Government Intention). Based on the following model fit criterion: Comparative Fit Index (CFI), Incremental Fit Index (IFI), Tucker-Lewis Index (TLI) ≥ 0.90; x2/df ≤ 3.0; standard root mean squared residual (SRMR) ≤ 0.08 [41], and root mean square error of approximation (RMSEA) ≤ 0.06. Further, the composite reliability (CR) and Cronbach alpha (α) reliability coefficients were ≥ 0.60 and 0.70, respectively, for all the measurement scales [32]. Additionally, the discriminant validity (DV) that was established as the square root of the average variance extracted (AVE) was greater than the correlations of the latent variables in the CFA [32,33].

 doi:10.20944/preprints202512.0357.v1

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 [42] and supported by West, *et al.* [43]. The removal of factor loadings of the component items from the CFA model was based on the standardised residual covariances [33] to further improve the six-factor CFA model fit indices, which significantly improved the model fit indices, 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	≥0.90	Acceptable
TLI	0.895	≥0.90	Unacceptable
IFI	0.906	≥0.90	Acceptable
SRMR	0.069	≤0.08	Excellent
RMSEA	0.061	≤0.06	Acceptable

Table 2. Model fit measures: Final estimate.

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

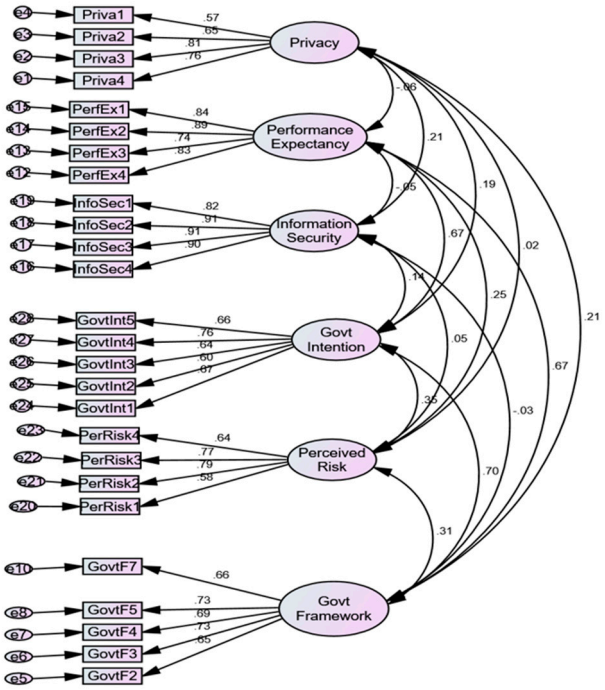

Figure 2. Confirmatory Factor Analysis Model.

 doi:10.20944/preprints202512.0357.v1

4.3. Validity and Reliability Analysis

To assess construct reliability and validity, Composite Reliability (CR), Average Variance Extracted (AVE), and Cronbach's Alpha (α) were calculated (Table 3). The results confirm the reliability of the measurement, as well as its convergent and discriminant validity.

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 [32,33,44,45].

2. Convergent Validity

Most constructs exceeded the AVE threshold of 0.50 [33,44,46], except Government Intention (0.428). However, this was retained because its CR exceeded 0.70, consistent with Fornell and Larcker [45], Brunelle and Lapierre [47], Lam [48] and Menguc and Auh [49].

3. Discriminant Validity

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

Table 3. Model fit measures: Initial estimate.

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.

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:

- Common Method Bias (CMB): Harman's single-factor test [37–39] 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 variance inflation factor (VIF) and tolerance limit (TOL) technique analysis [36,50] 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 cutoff of 4.0, confirming 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			

 doi:10.20944/preprints202512.0357.v1

6	1.189	4.572	66.311
7	.881	3.388	69.699
8	.732	2.817	72.516
9	.701	2.694	75.210
10	.644	2.476	77.686
11	.612	2.353	80.039
12	.567	2.180	82.218
13	.501	1.928	84.147
14	.473	1.821	85.968
15	.453	1.743	87.710
16	.450	1.732	89.443
17	.413	1.589	91.032
18	.361	1.390	92.422
19	.345	1.325	93.748
20	.319	1.228	94.976
21	.304	1.168	96.144
22	.263	1.013	97.157
23	.252	.970	98.127
24	.208	.801	98.928
25	.152	.583	99.511
26	.127	.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. Common Method Bias and Multicollinearity

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 [51], the study could not confirm that information security may likely increase government intentions. Nevertheless, further testing is necessary to confirm the causal relationship between the independent variables 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 [33,52].

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		

 doi:10.20944/preprints202512.0357.v1

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 < .05 level (2-tailed); ** p < .01 level (2-tailed).

4.6. Structural Model and Hypothesis Testing

The study employed a structural path analysis to test the hypothesis and applied 2000 bootstrap samples at bias-corrected 95% confidence intervals [53–56]. The structural model in Figure 3 was tested using a structural equation model (SEM) with maximum likelihood estimation [57]. The moderator variables (perceived risk) and independent variables (privacy, government framework, performance expectancy, and information security) were mean-centred according to Shieh [34].

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.

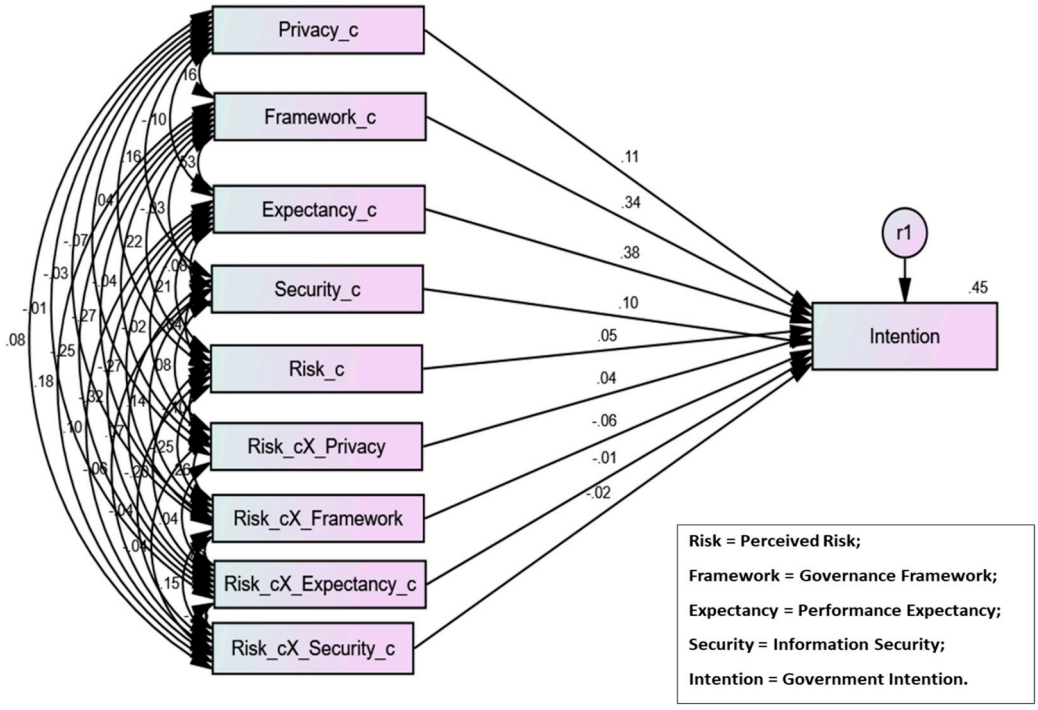

Figure 3. Structural path analysis model.

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 substantial explanatory power at ($\beta = 0.45$, $p < 0.001$).

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 policies, regulations, and compliance in driving the adoption intention of cloud services in government.

 doi:10.20944/preprints202512.0357.v1

3. H3 (Performance Expectancy → Intention)

Supported (β = 0.38, p < 0.001). Performance expectancy was the most influential predictor, highlighting the centrality of perceived benefits of cloud computing to government services.

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 had no increasing effect on 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 → Intention	0.11*	0.01	0.21	Significant
Government Framework → Intention	0.34***	0.19	0.50	Significant
Performance Expectancy → Intention	0.38***	0.21	0.55	Significant
Information Security → Intention	0.10*	0.00	0.19	Significant
Moderator Effect				
Perceived Risk → Intention	0.50	-0.08	0.17	Non-Significant
Interaction Effects				
Risk_x_Privacy → Intention	0.04	-0.07	0.14	Non-Significant
Risk_x_Framework → Intention	-0.06	-0.32	0.17	Non-Significant
Risk_x_Expectancy → Intention	-0.01	-0.26	0.23	Non-Significant
Risk_x_Security → Intention	-0.02	-0.13	0.08	Non-Significant

Risk = Perceived Risk; Framework = Governance Framework; Expectancy = Performance Expectancy; Security = Information Security; Intention = Government Intention.

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 with constructs related to information security, governance, privacy, and perceived risk. The findings reveal several noteworthy insights.

First, privacy, governance framework, performance expectancy, and information security were all found to significantly influence government intention to adopt cloud services. This reinforces prior studies highlighting privacy and information security as the cornerstone challenges for public-sector cloud adoption [5,13,14]. The findings suggest that privacy concerns should be given top priority in decision-making frameworks for public adoption, making privacy assessment an integral part of every cloud procurement and deployment stage.

In particular, the significant role of governance frameworks suggests that institutional support through clear policies, compliance standards, and enforcement mechanisms is critical to shaping adoption decisions. This finding aligns with recent research on government cloud strategies [11,18] and highlights the role of policy infrastructure as a trust enabler for cloud adoption.

Second, performance expectancy emerged as the strongest predictor of intention, reflecting respondents' strong belief that cloud services enhance efficiency and service delivery. This result is consistent with the UTAUT literature [7,21,58] and highlights that, despite concerns about security and sovereignty, perceived benefits remain a decisive factor in driving adoption decisions in government settings.

 doi:10.20944/preprints202512.0357.v1

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.

Finally, the hypothesised moderating role of perceived risk was not supported. Neither privacy, governance, performance expectancy, nor information security was significantly influenced by risk perceptions in shaping adoption intentions. This could be related to sector-specific (public) studies, considering the government's perspectives on sensitive issues such as information security, privacy, and performance expectancy, which may limit the generalisability of the findings.

These insights contribute to the academic understanding of the government's priority on risk management in digital transformation and its practical implications for developing measures that encourage cloud adoption while ensuring robust security and compliance mechanisms. This suggests that once respondents recognise the functional and governance benefits, their risk concerns may recede in importance. Such a result aligns with studies in technology acceptance, where risk perceptions decrease as institutional trust and perceived usefulness increase [19,59]. For Nigerian government agencies, this may suggest that risk concerns are perceived as being integrated into governance and compliance considerations, rather than operating as an independent barrier.

5.1. Theoretical Contributions

Theoretically, this study extends the UTAUT model to a government cloud adoption context, demonstrating its robustness while integrating constructs that reflect the security, sovereignty, and governance imperatives of the public sector. It contributes to the growing academic knowledge by questioning the centrality of perceived risk in public institutions and technically contributes to the understanding of the institutional dimensions of cloud adoption in a developing economy. More specifically, the study contributes to the growing body of knowledge at 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 [60–62], this study challenges the traditional perspectives, and perceived risk did not moderate adoption intentions. These finding challenges 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

Practically, the study emphasises the need for governments to strengthen governance frameworks, communicate performance benefits, and reframe security as a strategic enabler rather

 doi:10.20944/preprints202512.0357.v1

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 enforcement of compliance, 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 in protecting government-critical data and ensuring 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.

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 how prioritising performance in cloud adoption could assist government organisations in delivering reliable, cost-effective, and flexible digital services, enhancing public trust and operational effectiveness. Furthermore, governance frameworks could offer the legal and regulatory mitigation necessary to ensure secure cloud adoption, promoting accountability and public trust within government agencies and 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 and domesticating it to suit developing nations' security priorities, and transparency from cloud service providers. Moreover, developing a holistic cloud information security and privacy framework to improve government cloud adoption intentions.

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. These findings suggest prioritising and strengthening governance frameworks, as well as ensuring compliance with regulatory standards, rather than focusing solely on reducing perceived risk to reassure stakeholders and maintain public trust.

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.

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

 doi:10.20944/preprints202512.0357.v1

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.

In conclusion, 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.

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

Funding: his 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. s.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study (see Appendix A.1 for a copy of the consent form).

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Acknowledgments: The authors acknowledged 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:

MDPI	Multidisciplinary Digital Publishing Institute
AMOS	Analysis of Moment Structures
AVE	Average Variance Extracted
CFA	Confirmatory Factor Analysis
CFI	Comparative Fit Index
CMB	Common Method Bias
CR	Composite Reliability

 doi:10.20944/preprints202512.0357.v1

DOAJ	Directory of open access journals
IFI	Incremental Fit Index
IT	Information Technology
LD	Linear dichroism
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
TLA	Three letter acronym
TLI	Tucker-Lewis Index
TOL	Tolerance Limit
UTAUT	Unified Theory of Acceptance and Use of Technology
VIF	Variance Inflation Factor

Appendix A

Participant's Consent Form

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.

 doi:10.20944/preprints202512.0357.v1

References

1. Kanchepu, N. Digital transformation in banking industry: cloud computing as a key enabler. International Numeric Journal of Machine Learning and Robots 2023, 7.
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. Computer Science & IT Research Journal 2024, 5, 270-292, doi:10.51594/csitrj.v5i2.757.
3. Alamri, N.; Alzahrani, S. Navigating the Clouds: An Exploratory Research of Cloud Computing Adoption in Saudi Arabia's Small and Medium Enterprises. Engineering, Technology & Applied Science Research 2024, 14, 17859-17869, doi:10.48084/etasr.8435.
4. Qatawneh, N. Building a framework to drive government systems' adoption of cloud computing through IT knowledge. Discover Sustainability 2024, 5, 282, doi:10.1007/s43621-024-00427-8.
5. Ukeje, N.; Gutierrez, J.; Petrova, K. Information security and privacy challenges of cloud computing for government adoption: a systematic review. International Journal of Information Security 2024, 23, 1459-1475, doi:10.1007/s10207-023-00797-6.
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. Sustainable Operations and Computers 2022, 3, 118-135.
7. Venkatesh, V.; Morris, M.G.; Davis, G.B.; Davis, F.D. User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly 2003, 27, 425-478, doi:10.2307/30036540.
8. Andrews, J.E.; Ward, H.; Yoon, J. UTAUT as a Model for Understanding Intention to Adopt AI and Related Technologies among Librarians. The Journal of Academic Librarianship 2021, 47, 102437, doi:https://doi.org/10.1016/j.acalib.2021.102437.
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). Cham, 2022; pp. 520-538.
10. Maurer, T.; Hinck, G. Cloud security: a primer for policymakers; Carnegie Endowment for International Peace: 2020.
11. Choi, G.-Y.; Seo, J.; Kwon, H.-Y. A Comparative Study of National Cloud Security Strategy and Governance. In Proceedings of the Proceedings of the 25th Annual International Conference on Digital Government Research, 2024; pp. 241-250.
12. Mitchell, A.D.; Samlidis, T. Cloud services and government digital sovereignty in Australia and beyond. International Journal of Law and Information Technology 2022, 29, 364-394, doi:10.1093/ijlit/eaac003.
13. Ometov, A.; Molua, O.L.; Komarov, M.; Nurmi, J. A Survey of Security in Cloud, Edge, and Fog Computing. Sensors 2022, 22, doi:10.3390/s22030927.
14. Abdulsalam, Y.S.; Hedabou, M. Security and Privacy in Cloud Computing: Technical Review. Future Internet 2022, 14, 11, doi:10.3390/fi14010011.
15. Jianwen, C.; Wakil, K. A model for evaluating the vital factors affecting cloud computing adoption. Kybernetes 2020, 49, 2475-2492, doi:10.1108/K-06-2019-0434.
16. Sun, Y.; Liu, Q.; Chen, X.; Du, X. An Adaptive Authenticated Data Structure With Privacy-Preserving for Big Data Stream in Cloud. IEEE Transactions on Information Forensics and Security 2020, 15, 3295-3310, doi:10.1109/TIFS.2020.2986879.
17. Abd Al Ghaffar, H.-t.-A.N. Government cloud computing and national security. Review of Economics and Political Science 2024, 9, 116-133.
18. 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: 2025; pp. 33-62.
19. Prakash, S.; Malaiyappan, J.N.A.; Thirunavukkarasu, K.; Devan, M. Achieving regulatory compliance in cloud computing through ML. AIJMR-Advanced International Journal of Multidisciplinary Research 2024, 2.
20. Creswell, J.W. Research design : qualitative, quantitative, and mixed methods approaches, Fourth edition. ed.; SAGE Publications: Thousand Oaks, 2014.

 doi:10.20944/preprints202512.0357.v1

21. Venkatesh, V.; Thong, J.Y.; Xu, X. Unified theory of acceptance and use of technology: A synthesis and the road ahead. Journal of the association for Information Systems 2016, 17, 328-376.
22. 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. Journal of Advanced Research in Applied Sciences and Engineering Technology 2025, 53, 199-214.
23. 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? Journal of Ecohumanism 2025, 4, 682–693-682–693.
24. Omar, A.; Tiwari, V.; Saad, M. Smart technology's potential in smart destinations: a comprehensive UTAUT model with privacy and safety risk moderation. Journal of Hospitality and Tourism Technology 2025.
25. 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 US: Boston, MA, 2002; pp. 121-136.
26. Khan, A.; Ibrahim, M.; Hussain, A. An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. International Journal of Information Management Data Insights 2021, 1, 100015, doi:10.1016/j.jjimei.2021.100015.
27. 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: 2025; pp. 189-220.
28. 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.
29. Leeuw, E.d.; Berzelak, N. The SAGE Handbook of Survey Methodology. 2016, doi:10.4135/9781473957893.
30. Bhattacherjee, A. Social science research: Principles, methods, and practices; University of South Florida: 2012.
31. Edgar, T.; Manz, D. Research Methods for Cyber Security; Elsevier Science & Technology Books: Rockland, MA, UNITED STATES, 2017.
32. Hu, L.t.; Bentler, P.M. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling: A Multidisciplinary Journal 1999, 6, 1-55, doi:10.1080/10705519909540118.
33. Hair, J.F., Jr. Multivariate data analysis, Seventh edition. ed.; Pearson/Prentice Hall: Upper Saddle River, NJ, 2010.
34. Shieh, G. Clarifying the role of mean centring in multicollinearity of interaction effects. British Journal of Mathematical and Statistical Psychology 2011, 64, 462-477, doi:https://doi.org/10.1111/j.2044-8317.2010.02002.x.
35. Shrestha, N. Detecting multicollinearity in regression analysis. American Journal of Applied Mathematics and Statistics 2020, 8, 39-42.
36. 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. Environmental Modeling & Assessment 2023, 28, 1011-1022, doi:10.1007/s10666-023-09907-z.
37. Harman, H.H. Modern factor analysis; University of Chicago press: 1976.
38. Podsakoff, P.M.; MacKenzie, S.B.; Podsakoff, N.P. Sources of method bias in social science research and recommendations on how to control it. Annual review of psychology 2012, 63, 539-569.
39. 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 Business Review 2022, 0, 23197145221099098, doi:10.1177/23197145221099098.
40. Mishra, P.; Pandey, C.M.; Singh, U.; Gupta, A.; Sahu, C.; Keshri, A. Descriptive statistics and normality tests for statistical data. Annals of cardiac anaesthesia 2019, 22, 67-72.
41. Stevens, J. Applied multivariate statistics for the social sciences, Fifth edition. ed.; Routledge: New York, 2009.

 doi:10.20944/preprints202512.0357.v1

42. Bentler, P.M.; Bonett, D.G. Significance tests and goodness of fit in the analysis of covariance structures. Psychological bulletin 1980, 88, 588.
43. West, S.G.; Wu, W.; McNeish, D.; Savord, A. Model fit in structural equation modeling. Handbook of structural equation modeling 2023, 2, 184-205.
44. 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 Pacific Journal of Management 2023, doi:10.1007/s10490-023-09871-y.
45. Fornell, C.; Larcker, D.F. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research 1981, 18, 39-50, doi:10.2307/3151312.
46. Sarstedt, M.; Ringle, C.M.; Hair, J.F. Partial least squares structural equation modeling. In Handbook of market research; Springer: 2021; pp. 587-632.
47. 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, 2007; pp. 56-67.
48. Lam, L.W. Impact of competitiveness on salespeople's commitment and performance. Journal of Business Research 2012, 65, 1328-1334, doi:https://doi.org/10.1016/j.jbusres.2011.10.026.
49. Menguc, B.; Auh, S. Creating a firm-level dynamic capability through capitalizing on market orientation and innovativeness. Journal of the academy of marketing science 2006, 34, 63-73.
50. DeMaris, A. Regression with social data : modeling continuous and limited response variables; Wiley: Indianapolis, Ind., 2004.
51. Bracke, S. Correlation and Regression. In Reliability Engineering: Data analytics, modeling, risk prediction, Bracke, S., Ed.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2024; pp. 181-200.
52. Byrne, B.M. Structural equation modeling with AMOS : basic concepts, applications, and programming, Third edition. ed.; Routledge: New York, New York ; London, England, 2016.
53. 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. Learning and Individual Differences 2018, 61, 136-150, doi:https://doi.org/10.1016/j.lindif.2017.11.015.
54. 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. Educational Psychology 2019, 39, 332-352, doi:10.1080/01443410.2018.1543854.
55. Prikhodkina, M.; Melnikov, S. Factors that influence medication adherence in women with fibromyalgia: A path analysis. Journal of Clinical Nursing 2024.
56. Zhang, L.; Guo, X. Social support on calling: Mediating role of work engagement and professional identity. The Career Development Quarterly 2023, 71, 97-110.
57. Okolie, U.C. Work placement learning and students' readiness for school-to-work transition: Do perceived employability and faculty supervisor support matter? Journal of Vocational Behavior 2022, 139, 103805, doi:https://doi.org/10.1016/j.jvb.2022.103805.
58. 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 Quarterly 2012, 36, 157-178, doi:10.2307/41410412.
59. Sun, P. Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications 2020, 160, doi:10.1016/j.jnca.2020.102642.
60. 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. Government Information Quarterly 2019, 36, 237-251, doi:https://doi.org/10.1016/j.giq.2018.12.007.
61. 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.
62. 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 Proceedings of International Conference on Emerging Technologies and Intelligent Systems, Cham, 2022//, 2022; pp. 389-403.

 doi:10.20944/preprints202512.0357.v1