future internet

MDPI

Article

An Exploratory Factor Analysis Approach on Challenging Factors for Government Cloud Service Adoption Intention

Ndukwe Ukeje [1], Jairo A. Gutierrez [1,*], Krassie Petrova [1] and Ugochukwu Chinonso Okolie [2]

[1] Department of Computer and Information Sciences, Auckland University of Technology, Auckland 1010, New Zealand; ndukwe.ukeje@autuni.ac.nz (N.U.); krassie.petrova@aut.ac.nz (K.P.)
[2] Department of Vocational & Technical Education, Alex Ekwueme Federal University, Nduru-Alike 480101, Nigeria; okolie.chinonso@funai.edu.ng
* Correspondence: jairo.gutierrez@aut.ac.nz

Abstract

This study explores the challenges hindering the government's adoption of cloud computing despite its benefits in improving services, reducing costs, and enhancing collaboration. Key barriers include information security, privacy, compliance, and perceived risks. Using the Unified Theory of Acceptance and Use of Technology (UTAUT) model, the study conceptualises a model incorporating privacy, governance framework, performance expectancy, and information security as independent variables, with perceived risk as a moderator and government intention as the dependent variable. The study employs exploratory factor analysis (EFA) based on survey data from 71 participants in Nigerian government organisations to validate the measurement scale for these factors. The analysis evaluates variable validity, factor relationships, and measurement reliability. Cronbach's alpha values range from 0.807 to 0.950, confirming high reliability. Measurement items with a common variance above 0.40 were retained, explaining 70.079% of the total variance on the measurement items, demonstrating reliability and accuracy in evaluating the challenging factors. These findings establish a validated scale for assessing government cloud adoption challenges and highlight complex relationships among influencing factors. This study provides a reliable measurement scale and model for future research and policymakers on the government's intention to adopt cloud services.

Keywords: information security; privacy; government; cloud services; UTAUT; EFA

Academic Editors: Thomas Loruenser and Stephan Krenn

Received: 24 June 2025
Revised: 15 July 2025
Accepted: 18 July 2025
Published: 23 July 2025

Citation: 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. https://doi.org/10.3390/fi17080326

1. Introduction

The strategic adoption of cloud computing by government departments represents a critical pathway to economic and social development in emerging economies. In developing countries like Nigeria, cloud technologies offer the transformative potential to improve public service accessibility, reduce socioeconomic disparities, and foster inclusive governance through efficient digital service delivery [1–3]. The digital transformational journey of Nigeria is particularly compelling given its position as Africa's largest economy and most populous nation, where over 220 million citizens require efficient public services amid persistent infrastructure deficits and resource constraints [4]. Notwithstanding the projections that cloud adoption could generate NGN 30.2 trillion between 2023 and 2033, only 27% of Nigerian organisations adopted cloud computing as of 2021, significantly lower than the 49% adoption rate in Western Europe, highlighting the urgency of addressing adoption barriers [5]. Cloud adoption enables governments to overcome resource

constraints, democratise access to public services, and create development opportunities previously hindered by technological limitations [6]. However, significant barriers continue to impede the full realisation of these development benefits through government cloud adoption [7–9]. These challenges primarily encompass information security vulnerabilities, privacy concerns, regulatory compliance issues, and the complexity of cloud infrastructure implementation, all of which directly impact development outcomes by undermining citizen trust and institutional effectiveness.

Information security and privacy challenges have consistently ranked among the most persistent concerns in cloud computing adoption [10,11], with particular implications for development in resource-constrained contexts. In Nigeria's unique context, these challenges are compounded by the country's complex governance structure with varying levels of digital maturity and cybersecurity capabilities [12,13]. As governments increasingly rely on cloud platforms for government-to-government (G2G) and government-to-citizen (G2C) systems, they face escalating information security threats and privacy risks that can erode the developmental gains of digital transformation [14–17]. Addressing these challenges is essential not only for operational efficiency but also for building the trust necessary for citizens to participate in digitally enabled development initiatives. Yet, existing measurement instruments could not capture the unique nature of Nigeria's governance structure, regulatory compliance, and cultural and regional contexts that characterised Nigeria's cloud adoption landscape.

While extensive research has examined cloud computing adoption in developed economies and emerging studies have explored cloud adoption challenges in developing countries, a critical gap exists in understanding the unique nature and challenges within the Nigerian context. This gap is particularly significant for Nigeria, due to the absence of literature that captures relevant aspects of research unique to government cloud computing adoption challenges. This study addresses a critical gap in understanding how security and privacy concerns influence the development potential of government cloud adoption in emerging economies. Specifically, we investigate the following question: "What measurement scales can accurately assess these challenging factors influencing government intention to adopt cloud services and enhance development outcomes?" This research question directly explores the intersection of technological adoption barriers and their implications for human and social development through digital governance.

Through a comprehensive literature review, we identified key challenging factors and relevant theoretical frameworks for examining government cloud adoption within a development context. We adapted the Unified Theory of Acceptance and Use of Technology (UTAUT) [18] to conceptualise a model with new constructs specifically relevant to government cloud adoption in developing nations. Subsequently, we conducted exploratory factor analysis (EFA) to evaluate the validity of our measurement variables, develop theoretical understandings of the constructs, discover relationships between factor scores and variables, and analyse how these relationships influence development outcomes.

This study makes several significant contributions to IT for development discourse. First, it illuminates how addressing technological adoption barriers can accelerate social and economic development through improved public service delivery in resource-constrained environments. Second, it provides validated measurement scales for examining specific challenges hindering development-oriented cloud computing adoption in government contexts. Finally, it establishes a foundation for developing strategies to mitigate identified challenges in cloud environments, ensuring citizen privacy protection while maintaining the confidentiality, integrity, and availability (CIA) of government cloud-based services.

2. Literature Review

2.1. Cloud Computing as a Driver of Development

Cloud computing represents a transformative technology that can significantly impact economic, social, and human development, particularly in developing countries like Nigeria. The COVID-19 pandemic accelerated global digital transformation, highlighting the critical role of cloud technologies in ensuring service continuity and fostering inclusive development during crises [19]. For the global government, cloud computing offers a pathway to modernise public services in reducing inequality, increasing citizen participation, and creating sustainable socioeconomic growth opportunities.

The development impact of government cloud adoption extends beyond technological efficiency to encompass broader human development indices. As Muda, Tumsa [20] emphasises, IT for development and a cloud-enabled e-government framework can strengthen democratic institutions, reduce corruption through transparency, and improve vital services to previously underserved communities, thereby providing a significant transformation towards sustainable development goals. However, these development benefits remain constrained by persistent challenges to information security, privacy, and governance frameworks [21–23].

2.2. Overview of Cloud Computing

Cloud computing has been commonly described as a model for enabling convenient on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and utilised with minimal effort or interaction [24]. For example, Hurwitz and Kirsch [25] considered it as a method for providing shared computing resources that are readily available for utilisation by standardisation and automation. Furthermore, Ukeje [26] highlighted its accessibility and the sharing of computing resources and services from a pool of readily available infrastructures, irrespective of place or time.

From an IT development perspective, cloud computing represents what Wenzek [27] describes as a "leapfrogging technology", enabling resource-constrained governments to bypass traditional infrastructure investments while delivering sophisticated digital services that promote both economic growth and social inclusion. This aspect of cloud computing is particularly relevant, as it addresses both the limitations and capabilities constraints that often hinder technological progress in developing economies [28].

The cloud computing deployment and service delivery models promote availability and comprise five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [25,29,30]. There are two primary cloud computing deployment models: public cloud and private cloud. However, combining personal computing resources and public services within the same environment and interaction is considered a hybrid cloud environment. Conversely, prior research has identified other cloud environments, such as multi-cloud, where various public cloud services are used within the same cloud environment to support different businesses and services.

The three service delivery models for cloud computing infrastructure, as recognised by the USA's National Institute of Standards and Technology (NIST), are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [29], which are described as follows:

Infrastructure as a Service (IaaS) provides aggregated physical resources like servers, storage, provision processing, and networks for cloud consumers to run and deploy arbitrary software, including applications and operating systems [21]. It is considered an economic choice as organisations can meet their requirements without buying or providing any infrastructure. IaaS cloud providers are responsible for securing provisional infrastructures and ensuring operational procedures comply with the applicable laws and regulations.

In developing contexts, IaaS has been shown to reduce capital expenditure barriers that have historically limited public sector digital transformation in resource-constrained environments [31].

Platform as a Service (PaaS) is a cloud-based computing environment where applications can be developed, run, and managed. The PaaS model runs on top of the IaaS services. As in the work of Hurwitz and Kirsch [25] and Liu, Tong [29], NIST describes the model as the ability to grant cloud consumers access to create, modify, and deploy applications using programming languages, libraries, services, and other relevant tools provided by cloud providers. Abdulsalam and Hedabou [21] indicate that PaaS offers a trusted environment for consumers to secure the storage and processing of confidential information, for instance, in the use of a cryptographic co-processor to protect against unauthorised access. It was designed to maximise users' control when managing features related to the privacy of sensitive information, which is accomplished through user data privacy methods and self-installed configurable software. For developing nations, PaaS creates opportunities for indigenous innovation and knowledge creation by fostering internal growth-driven dependence.

Software as a Service (SaaS) represents applications or software running on the cloud infrastructure. The applications and software cloud service providers provided are accessible to cloud consumers through various means. Hurwitz and Kirsch [25] highlighted that SaaS applications typically manage customer data, enhancing SaaS vendors' responsibility to secure and protect information effectively. From a development standpoint, SaaS democratises access to sophisticated applications that would otherwise be cost prohibitive for public administration in developing economies, thereby reducing digital divides and promoting capability enhancement, as articulated in Sen's capability approach to development [32,33].

2.3. Information Security, Privacy, and Their Development Implications

Information security refers to the procedures to protect an information asset while sustaining its confidentiality, integrity, and availability characteristics [34]. Similarly, Khan, Ibrahim [35] regards it as a process that is adopted for safeguarding information assets. Arafat [36] refers to information security as a security chain that is as strong as its weakest link. Without proper techniques and a strategy to hold the chain together, there are always weaknesses that will be exploited by threats to organisational business objectives and service delivery. While there is no commonly adopted definition of information security, one can argue that the NIST definition has been widely accepted [37]. Therefore, the research adopts the Kissel [37] definition in the NIST glossary of key information security terms as "protecting information and information systems from unauthorised access, use, disclosure, disruption, modifications, or destruction to provide confidentiality, integrity, and availability".

In the context of development, information security takes on additional significance beyond organisational risk management. As Numan and Sunna [38] and Smith [39] argue, robust information security is essential for building citizen trust in digital governance, a precondition for achieving development outcomes through IT initiatives. In economies with limited institutional trust, such as many developing nations, security breaches in government systems can severely undermine development efforts by eroding public confidence and participation in digital initiatives [40].

The tremendous increase in personal data generated daily due to social networks, modern communications channels, and a wide range of analytics engines that provide insights into unique individual movements, interests, and activities has elevated the risk to individuals' privacy. The increased risks to citizens' personal information from various

cloud activities necessitated safeguards and privacy protection. For example, Sun [17] described the structural characteristics of the cloud computing environment as the leading cause of security problems, attributed to the privacy disclosure risk posed by cloud service providers (CSPs) when outsourcing information transmission, processing, and storage processes. According to Politou, Alepis [23], there is no universally acceptable definition of privacy, though it has been discussed in various forms and contexts. This research refers to privacy as a substantive citizen's right to data protection. Abed and Chavan [41] identified significant challenges for multinational corporations in cloud computing related to data protection and privacy.

There has been an ongoing discussion about information security and privacy in cloud computing at various levels, be it industry or academia [21–23,42–44]. Information security and privacy issues around cloud storage and computational security have been researched extensively [17,45–48]. However, scientific contributions that have been published in conference proceedings and international journals [43,49] indicate a clear understanding of security and privacy risks in cloud computing.

Despite the potential achievement of various cloud computing services and deployment models through technology, security, compliance, privacy, and legal matters are challenges that still hinder its adoption in government. The authors of [21] identified security and privacy as open issues in cloud computing adoption due to the outsourced data, dynamic abstraction, and scalability that have unlimited security boundaries and infrastructure. The information security and privacy issues of cloud computing have become increasingly important due to the sensitive information processed and stored in a cloud environment [50].

2.4. Theoretical Framework and Development Contexts

Recent scholars in IT for development have emphasised the need to contextualise appropriate theoretical frameworks when examining technology adoption in developing nations [51,52]. As Neves, Oliveira [53] and Straub [54] posited, no single theory or framework can accurately explain technology adoption without considering the specific development context. This observation is particularly relevant for government cloud adoption in Nigeria, where institutional, infrastructural, and socioeconomic factors create a unique environment for technological implementation.

The UTAUT provides a solid foundation for examining technology adoption factors but requires adaptation to address the specific development challenges faced by governments in emerging economies. Building on Walsham, Robey [55] and Osei-Bryson, Brown's [56] call for contextually sensitive theoretical approaches in IT for development research, we adapt the UTAUT to incorporate development-specific constructs, including governance frameworks, information security, privacy, and perceived risk, all factors that take a heightened significance in a context where institutional capacity and trust may be limited.

Zhou, Zhang [57] surveyed cloud computing providers' concerns about information security and privacy and identified security and privacy as the significant barriers to cloud computing adoption. Mohammed, Ibrahim [58] found security and privacy as significant factors that influenced the adoption of cloud computing for e-government implementation, while other notable researchers identified information security and privacy as key barriers and challenges to the government's intention to adopt cloud services [16,31,59–63].

Furthermore, the ITU [42] paper on privacy for cloud computing highlighted the difficulties faced by CSPs in ensuring data-level compliance with geographic restrictions on data transfers. This bolsters the need for cloud consumers to maintain compliance controls that expressly meet privacy- and security-related requirements. Ometov, Molua [16] and

Jiménez and Anaya [61] believe that technology could be adopted to mitigate the issues. Still, other researchers [64–66] suggest that developing a process, such as a governance framework, would better address the challenges and encourage adoption. Therefore, assessing these challenging factors influencing the government's intention to adopt cloud services and to enhance socioeconomic development outcomes is paramount.

2.5. Research Problem and Development Significance

Compliance and operational risk factors have significantly challenged how the government perceives cloud computing due to regulatory requirements, vulnerabilities, and best practices in cloud environments [67]. Cloud computing introduces significant security risks, including unauthorised access, data breaches, and a lack of control over sensitive data due to the cloud's multitenant approach. Abd Al Ghaffar [7] identified compliance with country regulations as a critical challenge to cloud computing adoption, as data protection and sovereignty differ across borders. These factors remain key concerns in cloud computing, as organisations are required to adopt a country-specific regulatory and data protection framework for effective governance.

The developmental significance of these challenges is profound. As Joshi, Ghafoor [68] argued, the preparedness in addressing security and privacy concerns can severely limit the development potential of digital governance initiatives. In Nigeria and similar contexts, these limitations can manifest as restricted service delivery, diminished citizen trust, and, ultimately, reduced impact on economic and social development indicators [69].

Based on our review of the literature at the intersection of cloud computing and development studies, we identify a critical research gap: the lack of validated measurement scales for assessing factors that influence government cloud adoption from development perspectives. This gap limits our understanding of how technological barriers relate to development outcomes and hinders the formulation of effective policies and frameworks to harness cloud computing benefits for inclusive growth.

Therefore, this study adapts the UTAUT to conceptualise a model and develop measurement scales that cover the identified challenging factors to the government adoption of cloud computing services, helping researchers and the government to measure and understand the challenging factors and chart a path in proffering effective mitigation strategies to ensure secure cloud adoption by the government. Hence, the research question "What measurement scales can accurately assess these challenging factors influencing government intention to adopt cloud services and enhance development outcomes?" was formulated to guide the study.

3. Research Design and Conceptual Model

Scholars adopted different and multiple theories to address different factors and behavioural intentions to adopt a technology [70–73]. This study adapts the UTAUT as a model that allows the identification of new construct variables to address the challenges of cloud service adoption within the government context; this study develops and validates the measurement scales for the model's constructs.

The UTUAT model was developed considering other theoretical models such as the Technology Acceptance Model (TAM), Theory of Planned Behaviour (TPB), Theory of Reasoned Action (TRA), Innovation Diffusion Theory (IDT), Motivation Model (MM), and Social Cognitive Theory (SCT) [18,74], amongst others. However, while contextualised, the UTAUT is not necessarily the major component of a new theory; it serves as a stepping stone to identifying a new approach to address identified challenges. This paradigm shift is the most promising direction for future research, which can make a significant contribution

to the UTAUT literature and advance continuous research on technology acceptance and use in developing economies.

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.

- Performance Expectancy
  According to Venkatesh, Morris [18], one of the root constructs in the UTAUT is performance expectancy, which determines perceived usefulness. Performance expectancy is the degree to which individuals believe using a system will enhance job performance. Amron, Ibrahim [75] captured it as the level at which users believe using government cloud services will help them achieve performance, which is considered in the research.
- Effort Expectancy
  Effort expectancy is the level of ease of use associated with using the system [18]. The construct is significant in contexts where ease of use is important and will be a vital determinant of an individual's intention to adopt the system. The ease-of-use root construct that contributed to the formation of effort expectancy indicates that the measurement scale should measure how easy it is to learn how to operate the system. According to Amron, Ibrahim [75], individuals with adequate effort expectancy have significant intentions to accept technology.
- Social Influence
  The social factors (as outlined in the measurement scale, the organisation has supported the use of the system) were identified as one of the root constructs in determining social influence. Social influence, as described by Venkatesh, Morris [18], is the degree to which individuals perceive the importance that others ascribe to using the system. It is the direct determinants of behavioural intention influenced by how others perceive the use of the technology [74]. This study will not consider social influence, as it does not significantly relate to what the research intends to examine.
- Facilitating Conditions
  According to Venkatesh, Morris [18], facilitating conditions are the level at which an individual believes that an organisation and technical infrastructure exist to support the use of the system. The construct captures operational concepts that include technological and organisational environments designed to remove barriers to using the system. Considering the facilitating conditions, the study assumes that individuals believe that government institutions have a mechanism to mitigate the barrier to adopting cloud services. The security and privacy challenges that hinder the adoption of cloud computing in government can be addressed through organisational support and the development of a governance framework to support government use of cloud computing for trusted service delivery to citizens.

Despite the high variance explained by the UTAUT for behavioural research, Venkatesh, Morris [18] encouraged further work to identify and test additional boundary conditions of the model to understand technology adoption and usage behaviour better. The additional boundary conditions might occur in moderating influences, different technologies such as cloud computing, user groups, and other organisational contexts (government institutions) [18]. The outcome of any proposed studies will enhance the UTAUT and account for additional variance in behaviour. This supports why the study considers new constructs to achieve the research objectives, understand the impact of the

new constructs in determining government intention to adopt cloud services, and mitigate the identified challenges.

3.1. Conceptual Model

The conceptual model presented in this section was based on the theories and models for technology adoption. This study develops the measurement items for the identified constructs by adapting from existing studies. With regard to other outlined technology acceptance models and theories, Venkatesh, Morris [18] established that the UTAUT outperformed these models by explaining 70% of the variance in behavioural intention and 50% in technology acceptance. Furthermore, the UTAUT has been extensively used for technology acceptance and behavioural intention [76]. Therefore, the study assumed that the UTAUT had significant predictive capability with constructs matching the factors and constructs related to the government's intention to adopt cloud computing, which is proposed in this study. This study adapts the UTAUT to incorporate constructs relating to the factors that affect government intention to adopt cloud services.

Thus, the study adapted the UTAUT to examine the identified challenging factors of cloud computing to the government's behavioural intention to adopt it. In a study to investigate the factors influencing the behaviour intention of acceptance and use of digital technology to tackle COVID-19, Akinnuwesi, Uzoka [76] modified the UTAUT for COVID-19 digital tracking technology (CDTT) acceptance and use in developing country contexts. Their study indicated that performance expectancy strongly impacts the intention to accept and use technology. As applied to this study, the UTAUT and model were adapted to hold that the independent variables (privacy, governance framework, performance expectancy, and information security) would influence or explain the dependent variables (government intention) while being moderated by perceived risk because the government's intention to adopt cloud services would depend on the influence of the factors identified. Moreover, the variable constructs from the UTAUT have been observed to influence intentions to use and accept technology.

This study proposed a conceptual research model in Figure 1, based on the UTUAT model with adapted variables (factors) such as privacy, governance framework, information security, and associated perceived moderator risk due to its comprehensive ability to model technology adoption, such as cloud computing, in a structured and institutional public sector environment. Furthermore, looking at the research questions and objectives, which required multi-dimensional constructs and the dynamic nature of the public sector socioeconomic and regional environment. The UTAUT offered the necessary structural foundation to capture behavioural intention and public sector technology adoption support. The model's adaptability also allowed for the contextual adaptation of variables, making it robust yet flexible enough for the specific demands of this study. By adapting the UTAUT with a governance and risk-oriented approach to security challenges, this study offers a model that is both empirically grounded and policy-aware, better suited to the realities of cloud computing adoption in the government sector.

The research model enables the research to adapt these new constructs in line with Sharma and Mishra's [77] recommendation that constructs from other disciplines could be tested within the UTAUT model. Also, Venkatesh, Thong [73] recommended further work to identify and test additional boundary conditions of the model to understand technology adoption and usage behaviour better.

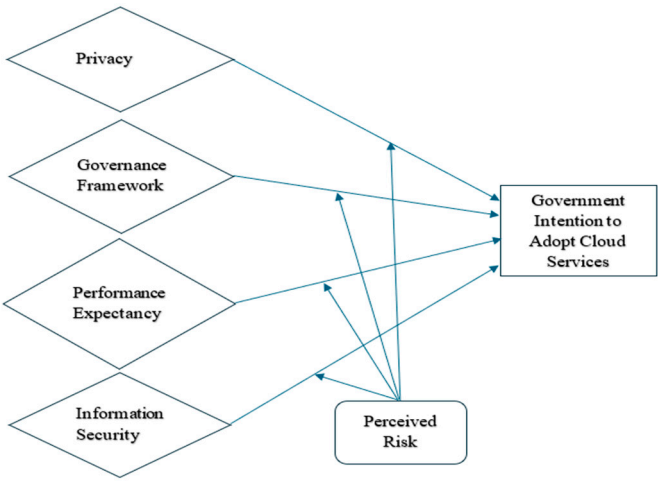

Figure 1. Conceptualised model for the study (adapted from the UTAUT model [18]).

3.2. Research Constructs

The following factors were identified as the research constructs based on various viewpoints: privacy, governance framework, performance expectancy, information security, and perceived risk. For instance, positivist viewpoints relied on measurement and reason [78]. In the study, it was acknowledged that the effect of people is revealed from measurable or quantifiable activity. The constructs for this study were determined through knowledge and theoretical processes that identified the challenging factors of cloud computing and the government's intention to adopt cloud services. Additionally, the cultural and socioeconomic situation of the region was also considered in identifying the construct determinants for this study. This is consistent with the suggestion that the subjective norms construct may be inadequate in reflecting normative influence on intentions or behaviour [79].

The selection of the constructs in this study was driven by both theoretical and contextual relevance to cloud computing adoption within the public sector; therefore, this study proposed construct variables influencing cloud users' viewpoints and responses towards the challenging factor in government cloud computing adoption. These new constructs were considered to examine their influence on the government's intention to adopt cloud services significantly. The performance expectancy was retained from the UTAUT due to its strong validation in influencing behavioural intention to adopt and use information systems and information technology within the study's contextual objectives and public sector contexts. Additionally, it was to retain its relevance in assessing the critical perceived usefulness in improving governance and recognising the benefits of technology adoption to improve user experience for citizens accessing government services [18,80].

However, to align the model more precisely with the governmental digital transformation priorities, information security, privacy, governance framework, and perceived risk were added. Their inclusion was based on a critical review of the literature that covers e-government and cloud adoption within the public sector, where trust, regulatory compliance, and governance are identified as pivotal factors influencing technology acceptance in government agencies. Additionally, the cultural and socioeconomic situation of the region was also considered in identifying the construct determinants for this study.

The inclusion of information security reflects concerns around data breaches, unauthorised access and general breach of confidentiality, integrity, and the availability of government information within the CSP's environment. These are heightened within the public cloud environment, especially where national data infrastructures are involved and public sector data are sensitive and related to national security, citizens' records, and other critical resources [81,82]. Furthermore, privacy was introduced as a separate construct,

capturing individual perceptions of how personally identifiable information (PII) is protected, monitored, and possibly misused within a cloud environment. This is highlighted as a key barrier to public cloud adoption in government sectors [17] and observed not just a legal or ethical requirement for cloud providers [83] and the government; instead, it is the foundational element that can significantly influence the behavioural intention of the government to adopt cloud services and identify reliable cloud providers when a public cloud is considered as an option.

The governance framework construct was added to address the institutional mechanisms, standards, and socioeconomic issues and structures that facilitate digital transformation in the public sector [84], ensuring that policy, risk management, and compliance obligations are factored into the behavioural intention model to adopt cloud computing in government [67]. Finally, perceived risk was introduced as a moderating variable, which is theoretically justified by prior models in the e-service and trust literature [85,86]. In this context, perceived risk was introduced to moderate the relationship between determinant constructs and behavioural intention to adopt cloud services, under the assumption that even when government organisations intend to adopt cloud technology, heightened risk perceptions such as lack of control over sensitive data and data sovereignty concerns may inhibit adoption in government. This is relevant in the public sector, where legal liability, citizen trust, institutional accountability, and data sovereignty are tightly related to cloud computing risks.

- Privacy

  Privacy is a substantive right to protect citizens' data. Abed and Chavan [41] identified data protection and privacy as significant challenges for multinational corporations in cloud computing. Government institutions aim to achieve better service delivery by adopting cloud computing, but various information security and privacy issues have been a significant concern [58,87]. Privacy has been labelled as one of the leading roles in the adoption of cloud computing because cloud services and technology operate in a manner that access could be granted to users' personally identifiable information (PII) through a virtualised environment; this is evident in the work of Ukeje, Gutierrez [9], where privacy was identified as a significant challenge to the government's intention to adopt cloud services. Arafat [36] also confirmed that cloud computing security, especially data security and privacy protection, is the primary inhibitor for adopting cloud computing services.

  Additionally, privacy captures individual perceptions of how personally identifiable information (PII) is protected, monitored, and possibly misused within a cloud environment. This is highlighted as a key barrier to public cloud adoption in government sectors [17] and observed not just a legal or ethical requirement for cloud providers [81], and the government; instead, it is the foundational element that can significantly influence the behavioural intention of the government to adopt cloud services and identify reliable cloud providers when a public cloud is considered as an option. Therefore, this study proposed a construct to examine the significant influence of privacy on the government's intention to adopt cloud services.
- Governance Framework

  A governance framework is vital in integrating cloud computing services into government structures and processes. The study proposed a governance framework as the new construct. The governance processes cut across policies, laws, regulations, compliance rules, and frameworks [88] that guide the implementation and adoption of cloud computing for service delivery. The governance framework encompasses several other components, including data protection, regulations, compliance, strategies, and the roles and responsibilities of stakeholders. The process ensures citizens'

privacy and security protection through an outlined framework that guides various attributes like confidentiality, integrity, and availability.

From the public sector, a process-oriented and institutional perspective, governance frameworks establish the normative and structural boundaries within which adoption decisions are made. The governance processes are a top management support priority, as they will ultimately affect adoption decisions [89] and build its intention for cloud services adoption. Governments are typically risk averse and operate in highly regulated environments, making top–down regulatory and strategic decisions central to any adoption initiatives. Effective governance frameworks can mitigate perceived institutional risk, enhance inter-agency collaboration, and ensure compliance with national or sectoral regulations [83].

This study examines the level of protection and the relationship the governance framework has with the government's intention to adopt cloud services and, therefore, proposes the governance framework as a construct ensuring compliance in influencing cloud services adoption in government.

- Performance Expectancy

  Performance expectancy, which is one of the UTAUT variables, has been identified to influence behavioural intention to adopt and use information systems and information technology [90,91]. According to Amron, Ibrahim [75] and Venkatesh, Thong [73], these attributes encompass the overall performance and features of technologies that influence adoption decisions. According to Venkatesh, Morris [18], one of the root constructs in determining performance expectancy is perceived usefulness (the degree to which a person believes that using a particular system or technology would enhance their job performance). Performance expectancy (PE) is the level at which users believe using cloud services will help achieve performance improvement [75] and efficiency in governance. Nguyen, Nguyen [74] perceived the usefulness of cloud services in achieving performance (objectives) in governance through citizen participation and effective service delivery. This relates to the proposed research model, where the perceived usefulness of cloud services will positively enhance and influence the government's intention to adopt them.

  This construct variable positions an innovative organisation to have a significant advantage over others through the perceived significant influence of performance expectancy on government intention to adopt cloud services and has a strong validation influencing behavioural intention to adopt and use information systems and information technology within the study's contextual objectives and public sector contexts. Therefore, it is ideal to contend that the performance expectancy influences the government's intention to adopt cloud services.

- Information Security

  Information security is critical to protecting critical citizen and government information stored and in transit in cloud computing. Information security generally focuses on protecting confidentiality, integrity, and availability. Amron, Ibrahim [75] highlighted vulnerability within the virtual machine environment of a cloud model that reveals stored and shared data on a cloud platform, which constitutes a security breach that could affect the usage and intention to adopt cloud services for service delivery. The research highlighted various security risks that exist in the use of cloud computing, some of which are associated with cloud technology, misuse of the cloud application by the cloud providers (internal staff), and mismanaging cloud users' details. Information security is considered critical to adopting government cloud services. Vurukonda and Rao [92] identified that the exponential increase in cloud users could lead to more significant security threats to cloud clients. Any successful attack on any entity could

lead to a breach that allows unauthorised access to the data of all cloud users. This risk impact slows down the government's intention to adopt cloud services. These are heightened within the public cloud environment, especially where national data infrastructures are involved and public sector data are sensitive and related to national security, citizens' records, and other critical resources [87–89]. Therefore, information security was proposed to address the need to protect government information to ensure reliable cloud-based services, given the sensitivity of government data and the critical need to ensure robust security measures to influence citizen trust and the adoption of cloud services.

- Perceived Risk

  Perceived risk was further adapted to moderate various identified variables related to the government's intention to adopt cloud services. The survey conducted by Riffai, Grant [93] observed that the moderating effects of the UTAUT model were inconsistent with the intention of technology acceptance. Despite the findings, this study examines the moderating effect of perceived risk to the identified challenging factors (information security and privacy) of government intention to adopt cloud services and the effect of performance expectancy on the government intention and use of cloud services. Further, it explores the moderating effect of the governance framework on the government's intention to adopt cloud services. This is in relation to the willingness to adopt technology, which depends on the level of risk value; the higher the risk, the less desire to accept it [94].

  Most studies examined risk as an external factor (moderator) that influences variables of the UTAUT model [95,96]. In this study, it will be observed as the moderator that influences the performance, the likelihood of potential loss of information, and privacy in the use and adoption of cloud services, while there is no effective governance framework. It was further described as the crucial moderator of various significant determinants of an organisation's intention to adopt cloud services. Alalwan, Dwivedi [95] claimed that perceived risk hinders behavioural intention in the UTAUT, while Chao [97] argued that no study had examined perceived risk as a moderating factor with the UTAUT model, which was postulated in the relationship between effort expectancy and behavioural intention. Therefore, this study adapted perceived risk as the moderator for the relationship between the independent variables (privacy, governance framework, performance expectancy, and information security) and the dependent variable (government intention to adopt cloud services). Thus, perceived risk was proposed as a moderate construct for this study.

4. Research Methodology

This research adopts a quantitative methodology to validate and establish reliable measurement scales that accurately assess the factors challenging the government's intention to adopt cloud services while connecting these adoption decisions to development outcomes in Nigeria. Our approach investigates the relationship between validated measurement constructs and government cloud adoption intentions, with the consideration of how these technological transitions influence socioeconomic development. The methodological focus directly addresses our primary research question: "What measurement scales can accurately assess these challenging factors influencing government intention to adopt cloud services and enhance development outcomes?".

The quantitative approach enables us to determine the statistical validity and reliability of the measurement instruments in the Nigerian government context while establishing causal relationships between properly measured factors and development-oriented outcomes. This research acknowledges the positivist epistemological position while collecting

statistical data that can validate measurement scales appropriate for the development context [98,99]. The methodology emphasises the validation of measurement scales specifically adapted for the Nigerian government context, ensuring that instruments can accurately measure adoption factors and support development in emerging economies. This validation process is essential for establishing measurement equivalence across different regions and contexts, ensuring that the findings accurately align with local realities rather than imported assumptions about technology adoption in Nigeria.

4.1. Data Collection Methods

This study was conducted under the ethical approval of the AUT Ethics Committee (AUTEC) 22/232 on 2 November 2022, with informed consent obtained through an anonymous online survey approach.

- Data Survey
  We employed a structured questionnaire survey designed [100] to test and validate measurement scales for both technology adoption factors and their perceived influence on government intention to adopt cloud services. The survey instrument was specifically constructed to evaluate whether measurement scales could maintain a validity suitable in the Nigerian government context, where challenging factors significantly influence cloud computing adoption decisions. While questionnaires can be subject to non-response and sampling bias, the cross-sectional survey questionnaire approach [101] was particularly appropriate for testing measurement scales across Nigeria's diverse governmental landscape.
  The survey approach facilitated the collection of sufficient data to conduct the psychometric analyses of the measurement scales, allowing us to determine which constructs effectively capture the relationships between cloud adoption challenging factors. We incorporated specific development-oriented measures to assess whether the scales adequately capture the unique challenges faced within public organisations.
- Data Collection
  The data collection procedure gathered responses necessary for psychometric validation of measurement scales from the key stakeholders responsible for technological decision making in Nigerian government institutions. An online survey approach was selected to ensure measurement equivalence across diverse government settings while minimising coverage and non-response errors [102]. The merits of adopting an Internet survey proved particularly relevant for scale validation [98], allowing us to reach a statistically significant sample across Nigeria's dispersed government agencies.
  The anonymous online survey targeted participants from relevant Nigerian government organisations within the ministries, departments, and agencies (MDAs), including IT administrators, information security and privacy personnel, and others familiar with cloud computing. This sampling strategy ensured we could validate measurement scales across the full spectrum of stakeholders involved in government technology adoption decisions that impact IT development outcomes. Our methodology included measures to validate the measurement scales developed in the contexts that adequately captured the development dimensions of cloud adoption.
- Survey Instrument
  The survey instrument was meticulously designed to test and validate measurement scales for factors influencing government cloud adoption in developing regions like Nigeria, and we adopted a structured questionnaire format to systematically evaluate the psychometric properties of scales measuring privacy concerns, governance frameworks, performance expectancy, information security, and perceived risk, as well as their relationships.

A 5-point Likert scale was used to measure respondents' viewpoints, ranging from "Strongly Disagree (1) to "Strongly Agree" (5). This response format was selected based on the proven reliability of previous studies and its appropriateness for the Nigerian cultural context. Additional demographic questions using continuous (ratio-scaled) and dichotomous responses were included to enable an analysis of how institutional factors could influence the measurement scale.

The research instrument adapted scales from previous studies [18,97,103,104], with careful modifications to ensure contextual relevance to Nigerian government settings and development priorities. While the foundational scales came from UTAUT research [18,105,106], we conceptualised the instrument to establish a measurement scale including items that are pertinent to information security and privacy concerns, public trust, cloud service accessibility, and performance and adoption in government.

4.2. Data Analysis Methods

Statistical Package for Social Sciences (SPSS) software V29 was used for analysis due to its robust capabilities for psychometric evaluation and scale validation [107]. The survey responses underwent rigorous cleaning and screening of data to ensure the integrity of psychometric analyses. The study applied exploratory factor analysis as a primary analytical technique to assess the construct validity of the measurement scales [108] in the Nigerian government context. This approach allowed us to establish the extent of the measurement constructs in determining the dimensional structure when applied to government cloud adoption intention in developing regions.

Factor analysis helped to evaluate score validity, factor scores, and measurement invariance [109,110], establishing whether the measurement scales accurately capture cloud adoption factors in Nigerians' unique organisational context. Beyond factor analysis, we employed reliability assessment through Cronbach's alpha and composite reliability measures to determine the internal consistency of our measurement scales. Additionally, convergent and discriminant validity analyses were conducted to establish whether the measurement scales appropriately differentiated between distinct but related constructs in the government-oriented adoption model.

The analysis explicitly examined whether established measurement scales for privacy concerns, governance frameworks, performance expectancy, information security, and perceived risk sustained psychometric properties when applied to government cloud adoption intention in Nigerian government contexts. By validating measurement scales appropriate for the Nigerian context, our methodology provides a foundation for accurately assessing how the measurement scale could transform secure cloud computing adoption in government and serve as a transformative force in public sector modernisation and IT development.

5. Data Analysis Results and Research Findings

Statistical analysis was conducted to evaluate the psychometric features of the measurement item scales based on the valid 71-response data collected during the study. Given that the measurement scales were adapted (the researcher made extensive modifications) to suit the research objectives, all measurement scales were subjected to exploratory factor analysis (EFA). Hence, this study applied EFA to assess the suitability of the measurement instrument in examining the challenging factors influencing government intention to adopt cloud services.

5.1. Coefficient of Reliability

This study analysed the reliability of the scale items before conducting the EFA. The Cronbach alpha coefficient reliability analysis was used to measure the internal reliability of a psychometric measurement score for the identified sample in the response, based on the recommended threshold of acceptable 0.70 and above [111,112]. The reliability results in Table 1 indicate that Cronbach's alpha coefficient of reliability for all constructs ranges from 0.807 to 0.950, which is above the recommended threshold. Therefore, all measurement items in the constructs were confirmed to be reliable and acceptable for further testing the EFA for this study.

Table 1. Coefficient of reliability.

S/N	Variables	Number of Measurement Items	Cronbach's Alpha Reliability
1	Privacy (Priva)	4	0.847
2	Governance framework (GovtF)	8	0.807
3	Performance expectancy (PerfEx)	4	0.932
4	Information security (InfoSec)	4	0.950
5	Perceived risk (PerRisk)	4	0.844
6	Government intention (GovtInt)	6	0.815

5.2. Exploratory Factor Analysis (EFA)

Researchers commonly use EFA to discover a small number of latent constructs for a more significant number of observed variables to identify influencing factors and analyse their relationship [113]. However, Thompson [110] and Hooper [109] highlighted various purposes for which factor analysis can be conducted: to evaluate the score validity of measurement variables (questions), develop a theory regarding the constructs, discover the relationship between factor scores and variables, and further analyse the relationship of the variables. Hence, this study applied EFA to explore the measurement variables (questions) score validity and their relationship to the identified constructs to measure government intention to adopt cloud services.

Several researchers acknowledged conducting EFA using various factorisation techniques such as principal component analysis, maximum likelihood analysis, and principal axis factoring [109,114,115]. Principal component analysis describes the relationship between the variables by developing components that summarise the relationship between the correlations [110,114]. Principal axis factoring is the least-squares inference of common factors, while maximum likelihood analysis estimates the values for model parameters and exhibits hypothetical benefits [116].

According to Mabel and Olayemi [117] and De Winter and Dodou [116], many researchers have argued that there is no evidence regarding preferred techniques to adopt for different factor patterns or sample sizes. However, Mabel and Olayemi [117] acknowledged the importance of principal components analysis for all uniform variable distributions and samples. Nevertheless, principal component analysis has been considered more efficient [118,119], and thus, the researcher used principal component analysis for factorisation to ascertain the validity of the measurement scale.

Researchers suggested that a sample size is required for reliable factors and that the sample size is determined as a function of the number of variables being analysed [118,120]. However, Guadagnoli and Velicer's [120] findings show that the assessed component pattern is based on the number of variables that define the component's factor loadings. Stevens [118] further suggested that factor loadings should be greater than 0.40; however,

if a component has four or more variables with a factor loading above 0.60, then the component pattern may be interpreted irrespective of the sample size; in contrast, a component of about ten or more variables with a low loading of 0.40 is reliable with a low sample size. Therefore, to retain the individual items in the measurement scales in line with Pallant [107], such component items must have a minimum factor loading of above 0.40 on the relevant factors [121–123].

- Kaiser–Meyer–Olkin (KMO) and Bartlett's Test
  The two statistical measures, the Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy and Bartlett's Test of Sphericity, give the statistical significance tests of the correlations to indicate the reliability between the pairs of the variables and sampling adequacy [107,114]. Tabachnick and Fidell [114] identify Kaiser's measure of sampling adequacy as the ratio of the sum of the squared correlations to the sum of the squared correlations plus the sum of squared partial correlations. Pallant [107] suggested checking for data suitability for factor analysis by confirming the value of the Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy value of 0.6 and above, as recommended by Tabachnick and Fidell [114], and Bartlett's Test of Sphericity value should be significant at 0.05 and smaller.
  This study applies the Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy and Bartlett's Test of Sphericity to assess the factorability of the responses and ensure that the factor analysis is appropriate [107,114,124]. Stevens [118] suggested applying KMO and Bartlett's test when a researcher uses component analysis with a small sample size. The analysis in Table 2 shows the Kaiser–Meyer–Olkin (KMO) measure of the sampling adequacy value of 0.731, and Bartlett's test of statistical significance indicates <0.001 ($p \leq 0.001$); therefore, the factor analysis is appropriate for the study, as specified by Pallant [107] and Tabachnick and Fidell [114].
- Communality Coefficients Values
  Communality of a variable, as stated by Stevens [118] and Tabachnick and Fidell [114], connotes the number of variances on a variable that account for the set of factors, which is the sum of the square loadings for the variable through the factors. The communality values for the factors measured were also considered in addition to the factor loading of the items. Tabachnick and Fidell [114] described very low communality values as an indication that the variables are unrelated to other variables; therefore, the variable is usually an outlier among different variables and should be ignored or deleted in factor analysis. Thus, this study removed common variance values of less than 0.40 from the measurement scales, as Tabachnick and Fidell [114] recommended. Therefore, component item 1 for government framework (GovtF1) was removed, as shown in communality values for the components in Table 3.
- Total Variance Explained
  The principal components analysis determines and extracts the number of factors (components) with eigenvalues of 1 or more, which is the common criterion to ascertain useful factors. According to Stevens [118], the eigenvalue indicates the number of variances reported by each factor. This is relevant to determining the number of components that meet Kaiser's criterion of eigenvalues greater than 1. However, six components are retained in Table 4, as Tabachnick and Fidell [114] specify that a reasonable number of four to six factors is optimal for the total variance explained. The result analysis explained that 70.079% of the total variance consisted of the six factors (privacy, governance framework, performance expectancy, information security, perceived risk, and government intentions), as supported by Tabachnick and Fidell [114].

- Rotated Component Matrix
  To further interpret the retention of the six components, the study analysed the components' rotation matrix with varimax and Kaiser normalisation rotation. The rotation component matrix analysis results in Table 5 show that the first factor was the performance expectancy scale with four (4) items, and the factor loadings ranged between 0.780 and 0.886, explaining 24.798% of the variance. The second factor was the governance framework scale, with seven items, and the factor loading ranged between 0.454 and 0.762, explaining 12.707% of the variance. The third measurement scale is the information security scale with four items, and the factor loading ranged between 0.908 and 0.952, explaining 10.950% of the variance. The fourth factor is privacy, with four items, and the factor loadings ranged between 0.704 and 0.907, explaining 8.789% of the variance. The fifth factor is perceived risk, and the scale has four items with factor loadings ranging between 0.705 and 0.849, explaining 7.771% of the variance. Lastly, the sixth factor is the government intention variable with six items, and the factor loading ranged between 0.442 and 0.848, explaining 5.064% of the variance.
  The 70.079% total variance explained by the EFA indicates that the scale successfully explains the measured quality of the measurement instrument and the underlying relationship of the measured variables in examining the influence of the challenging factors on the government's intention to adopt cloud services. Although GovtInt4 has a 0.442 loading slightly above the minimum acceptable loadings, it was retained due to its theoretical relevance and the assertion that a component's items with a minimum factor loading of above 0.40 on the relevant factors [107,121–123] could be retained. However, we acknowledge the lower loading compared to other items and recommend its re-evaluation in future studies. Appendix A.1 shows the constructs and the measurement items with their factor loadings.

Table 2. Kaiser–Meyer–Olkin (KMO) and Bartlett's Test.

KMO and Bartlett's Test		
Kaiser–Meyer–Olkin measure of sampling adequacy		0.731
Bartlett's Test of Sphericity	Approx. Chi-Square	1455.806
	df	435
	Sig.	<0.001

Table 3. Communality coefficient values.

Measurement Scale Common Variance Values			Measurement Scale Common Variance Values Above 0.40		
Communalities			Communalities		
	Initial	Extraction		Initial	Extraction
Priva1	1.000	0.694	Priva1	1.000	0.694
Priva2	1.000	0.570	Priva2	1.000	0.570
Priva3	1.000	0.835	Priva3	1.000	0.835
Priva4	1.000	0.729	Priva4	1.000	0.729
GovtF1	1.000	0.309	GovtF2	1.000	0.646
GovtF2	1.000	0.646	GovtF3	1.000	0.621
GovtF3	1.000	0.621	GovtF4	1.000	0.672
GovtF4	1.000	0.672	GovtF5	1.000	0.662
GovtF5	1.000	0.662	GovtF6	1.000	0.611
GovtF6	1.000	0.611	GovtF7	1.000	0.485
GovtF7	1.000	0.485	GovtF8	1.000	0.645
GovtF8	1.000	0.645	PerfEx1	1.000	0.817

Table 3. *Cont.*

Measurement Scale Common Variance Values			Measurement Scale Common Variance Values Above 0.40		
Communalities			**Communalities**		
	Initial	**Extraction**		**Initial**	**Extraction**
PerfEx1	1.000	0.817	PerfEx2	1.000	0.846
PerfEx2	1.000	0.846	PerfEx3	1.000	0.643
PerfEx3	1.000	0.643	PerfEx4	1.000	0.837
PerfEx4	1.000	0.837	InfoSec1	1.000	0.858
InfoSec1	1.000	0.858	InfoSec2	1.000	0.900
InfoSec2	1.000	0.900	InfoSec3	1.000	0.859
InfoSec3	1.000	0.859	InfoSec4	1.000	0.936
InfoSec4	1.000	0.936	PerRisk1	1.000	0.736
PerRisk1	1.000	0.736	PerRisk2	1.000	0.717
PerRisk2	1.000	0.717	PerRisk3	1.000	0.777
PerRisk3	1.000	0.777	PerRisk4	1.000	0.671
PerRisk4	1.000	0.671	GovtInt1	1.000	0.666
GovtInt1	1.000	0.666	GovtInt2	1.000	0.755
GovtInt2	1.000	0.755	GovtInt3	1.000	0.692
GovtInt3	1.000	0.692	GovtInt4	1.000	0.610
GovtInt4	1.000	0.610	GovtInt5	1.000	0.729
GovtInt5	1.000	0.729	GovtInt6	1.000	0.496
GovtInt6	1.000	0.496			

Extraction method: principal component analysis.

Table 4. Total variance explained.

Total Variance Explained									
Component	**Initial Eigenvalues**		**Cumulative %**	**Extraction Sums of Squared Loadings**			**Rotation Sums of Squared Loadings**		
	Total	**% of Variance**		**Total**	**% of Variance**	**Cumulative %**	**Total**	**% of Variance**	**Cumulative %**
1	7.439	24.798	24.798	7.439	24.798	24.798	5.046	16.821	16.821
2	3.812	12.707	37.505	3.812	12.707	37.505	3.848	12.827	29.648
3	3.285	10.95	48.455	3.285	10.95	48.455	3.613	12.042	41.69
4	2.637	8.789	57.244	2.637	8.789	57.244	3.066	10.22	51.909
5	2.331	7.771	65.015	2.331	7.771	65.015	2.969	9.895	61.804
6	1.519	5.064	70.079	1.519	5.064	70.079	2.482	8.274	70.079
7	1.127	3.756	73.835						
8	0.929	3.098	76.932						
9	0.742	2.473	79.405						
10	0.72	2.401	81.806						
11	0.668	2.227	84.033						
12	0.542	1.808	85.841						
13	0.504	1.678	87.52						
14	0.483	1.611	89.13						
15	0.438	1.46	90.591						
16	0.365	1.216	91.806						
17	0.345	1.15	92.956						
18	0.296	0.986	93.942						
19	0.282	0.939	94.881						
20	0.273	0.909	95.79						
21	0.221	0.736	96.525						

Table 4. *Cont.*

Total Variance Explained									
Component	Initial Eigenvalues		Cumulative %	Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance		Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
22	0.204	0.681	97.207						
23	0.18	0.599	97.806						
24	0.162	0.54	98.346						
25	0.125	0.415	98.761						
26	0.116	0.387	99.148						
27	0.096	0.32	99.468						
28	0.072	0.24	99.708						
29	0.045	0.151	99.859						
30	0.042	0.141	100						

Extraction method: principal component analysis.

Table 5. Rotated component matrix.

Rotated Component Matrix [a]						
	Component					
	1	2	3	4	5	6
Priva1				0.803		
Priva2				0.704		
Priva3				0.907		
Priva4				0.842		
GovtF1						
GovtF2		0.737				
GovtF3		0.637				
GovtF4		0.749				
GovtF5		0.658				
GovtF6		0.748				
GovtF7		0.454				
GovtF8		0.762				
PerfEx1	0.862					
PerfEx2	0.862					
PerfEx3	0.780					
PerfEx4	0.886					
InfoSec1			0.912			
InfoSec2			0.946			
InfoSec3			0.908			
InfoSec4			0.952			
PerRisk1					0.812	
PerRisk2					0.842	
PerRisk3					0.849	
PerRisk4					0.705	

Table 5. *Cont.*

Rotated Component Matrix [a]						
	Component					
	1	2	3	4	5	6
GovtInt1						0.711
GovtInt2						0.848
GovtInt3						0.762
GovtInt4						0.442
GovtInt5						0.792
GovtInt6						0.612

Extraction method: principal component analysis. Rotation method: varimax with Kaiser normalisation. [a] Rotation converged in 6 iterations.

6. Discussion

This study contributes to the ongoing research on IT for development by examining how factors challenging government cloud adoption influence the developmental outcomes of enhanced public service delivery, digital inclusion, and governance transformation in Nigeria. By adapting the UTAUT to extended identified constructs, our research demonstrates the model's importance in understanding how government technological behavioural intention to adopt shapes development pathways in emerging economies [125]. Developing robust measurement scales for assessing factors influencing government cloud adoption provides valuable tools for evaluating IT-led development initiatives in public sector contexts.

Our exploratory factor analysis demonstrated that the identified factors account for 70.079% of the total variance, indicating a strong explanatory power of the measurement scale [114]. This reinforces the importance of variance-based statistical techniques in assessing technology adoption models within development contexts [126]. The analysis supports the validity of our constructs as measurement items loaded strongly on their respective factors, with each construct representing a unique dimension that captures different aspects of secure cloud governance relationships in the government. Moreover, the factors were uncorrelated, showing that each construct represents a unique dimension, reducing overlap and improving interpretability within our conceived conceptual model.

6.1. Development Impact of the Key Factors

Performance expectancy accounted for the highest variance (24.798%), underscoring its critical role in influencing government cloud adoption intent and subsequent development outcomes. This highlights how perceived benefits of cloud services—such as efficiency, cost reduction, and service improvement—can drive transformative change in how governments deliver essential services to citizens, particularly in resource-constrained and required secure and trusted environments [127]. When governments recognise cloud computing's potential to enhance service accessibility and reduce digital divides, they are more likely to invest in these technologies as development enablers.

The governance framework factor, contributing 12.70% of the variance, emphasises the importance of institutional structures and policy-level support in cloud adoption decisions and leveraging cloud technologies for development. This factor encompasses regulation and compliance mechanisms that are essential for ensuring a secure cloud adoption, contributing to inclusive and sustainable development rather than exacerbating existing inequalities in terms of accessibility and affordability [128]. Our findings align with previ-

ous studies that underline the need for governance frameworks to mitigate information security and privacy challenges while maximising the developmental benefits [9,64,129].

Information security (10.950% variance) and privacy (0.789% variance) reflect the technological and ethical concerns that often hinder cloud adoption in government contexts where public trust, data protection, and sovereignty are essential for IT development. The high factor loadings for information security between 0.908 and 0.952 and privacy between 0.704 and 0.907 demonstrate how these concerns significantly shape government intentions toward adopting cloud technologies that could otherwise accelerate development initiatives. This indicates that governments may hesitate to embrace cloud-enabled development pathways without explicit assurances regarding data sovereignty and citizen privacy protection.

Perceived risk, which moderates the independent factors, explains 7.771% of the variance, with factor loadings ranging from 0.705 to 0.849. This demonstrates how risk perception influences the technology–development relationship, as governments remain cautious about the potential consequences of cloud adoption that could undermine IT development. Including perceived risk in our measurement scale highlights its significant role in moderating the challenges of cloud adoption and its potential developmental benefits in understanding risk perception in cloud computing for government institutions.

The government intentions factor (5.064% variance) reflects how institutional readiness and strategic priorities influence the adoption of development-enabling cloud services. This aligns with the UTAUT model that highlights the importance of leadership in shaping technological trajectories, particularly in contexts where information security and privacy play a role in IT implementation perception that directly impacts developmental outcomes for service delivery, enhanced transparency, and increased citizen participation.

The high Cronbach's alpha values (0.807–0.950) confirm the reliability of the constructs for measuring the relationships between the cloud adoption factors and intention to utilise the cloud for developmental services in government contexts.

6.2. Academic Relevance and Contribution to IT for Development

Our study provides comprehensive, psychometrically validated measurement scales specifically designed to assess challenging government cloud adoption factors in relation to government intention to adopt the cloud for developmental outcomes. This addresses a fundamental regional and specific gap in IT for the development literature within government contexts, where measurement instruments do not provide sufficient adaptation for the challenging factors of cloud adoption in government [130]. The strong explanatory power of our measurement scales (accounting for 70.079% of total variance) demonstrates their effectiveness in capturing the challenging factors and government intention to adopt the cloud for service delivery and development objectives in emerging economies. These validated scales enable academics to conduct more rigorous comparative studies across different contexts and regions, reducing measurement errors affecting cross-cultural technology adoption research and improving IT for development.

Through our factor analysis, we empirically demonstrate how traditional adoption factors interact differently in development contexts. Particularly notable is the heightened importance of governance frameworks (12.70% variance) and information security concerns (10.950% variance), reflecting the specific challenges governments face in developing regions where institutional structures often evolve alongside technological capabilities.

This study opens new pathways for quantitative research that can reliably assess how specific technologically challenging factors influence adoption intention and contribute to development decisions within government contexts. This methodological contribution is particularly valuable for researchers as the validated measurement scale provides re-

searchers with a reliable instrument for investigating cloud computing's role in advancing development goals through improved services and accelerating IT development in the challenging and resource-constrained public sector. Additionally, the high internal consistency of our measurement scales (Cronbach's alpha 0.807–0.950) demonstrates that properly adapted instruments can achieve strong reliability even in contexts traditionally considered challenging for quantitative research. Therefore, the methodological success challenges assumptions about the limitations of quantitative methods in IT development research and encourages more methodologically pluralistic approaches [131,132].

6.3. Practitioners' Relevance and Contribution to IT for Development

Our validated measurement scales provide government officials, development agencies, and technology implementers with reliable tools to assess their readiness for cloud adoption and identify specific barriers that hinder the realisation of development benefits. This allows for targeted interventions rather than generic technology-push approaches that have often failed in development contexts.

Our inclusion of perceived risk as a moderating factor (7.771% variance) provides practitioners with a framework to evaluate cloud adoption risks specifically from development perspectives. This enables better risk mitigation strategies that consider not just technical concerns but also socioeconomic developmental impacts. Furthermore, identifying governance frameworks as a critical factor offers policymakers concrete evidence of the need for comprehensive policy development that balances innovation with protection. This is particularly relevant for developing regions, where technological leapfrogging opportunities must be balanced with appropriate regulatory frameworks.

The high variance explained by performance expectancy (24.798%) provides justification for development agencies and governments to focus resources on demonstrating and communicating the specific development outcomes that cloud adoption can facilitate, including improved service delivery to underserved populations, enhanced transparency, and more efficient resource allocation. Additionally, our research helps cloud providers better understand how their solutions need to be adapted to address the specific development challenges and priorities of government institutions. This facilitates more effective partnerships between technology providers and development agencies seeking to leverage cloud technologies for social and economic development.

6.4. Theoretical Implications

Our adaptation of the UTAUT for government cloud adoption in Nigeria represents a significant theoretical advancement in understanding how established technology acceptance models must be modified to account for development improvements in emerging economies. While the UTAUT has been integrated in different contexts [70,71] and originally conceptualised for commercial settings, this research demonstrates how these models could be adapted to the specific dynamics to explain technology adoption decisions in public institutions.

The emergence of governance frameworks as a significant factor (12.70% variance) advances theoretical understanding of the interplay between institutional structures and technology adoption for development purposes. These findings expand beyond traditional UTAUT constructs [12] to incorporate governance elements that are particularly relevant in a development context, where institutional capacity may evolve alongside technological capabilities. Additionally, it further contributes by demonstrating how information security and privacy concerns take a distinctive characteristic in development contexts through enhancing the theoretical understanding of how security and privacy considerations in cloud computing adoption are influenced by development-specific factors such as data

sovereignty concerns, citizen trust in government institutions, and varying regulations. This significance underscores the criticality of managing both government and citizen-sensitive data in development contexts, where trust and data sovereignty concerns impact technology acceptance.

This study provides a theoretical framework for evaluating how specific cloud computing adoption factors can be assessed for developmental potential through empirical validation of the measurement scales and factors influencing government adoption intentions. This theoretical contribution helps to bridge the gap between the technology adoption literature and development studies by providing specific constructs that connect cloud adoption concerns and government intentions to utilise cloud services for socioeconomic development.

6.5. Practical Implications

This study offers several actionable insights for governments, policymakers, and cloud service providers aiming to mitigate the challenges associated with cloud service adoption. The validated measurement scale can be adopted by policymakers in conducting studies that will enhance governance frameworks to address the challenges of cloud adoption. The high reliability of the measurement items could suggest possible areas that the government can prioritise during decision making regarding cloud investments based on the most critical influencing factors by measuring changes in the identified factors over time. Stakeholders can assess the effectiveness of interventions aimed at facilitating cloud adoption for government development purposes. This practical application could enable more evidence-based decision making and the continuous improvement of technology interventions in development contexts.

The government and policymakers are expected to apply the scale to prioritise areas of concern, such as information security and privacy challenges, and strategically measure and balance the benefits of cloud adoption while mitigating data protection and sovereignty concerns. This suggests that cloud implementations that address citizen concerns about data protection are more likely to gain government acceptance, ultimately enabling the realisation of development benefits. Moreover, equipping government and cloud service providers with the necessary tools to measure adoption barriers ensures efficient and secure integration in the public sector.

Additionally, this study provides a reliable model for future research and policymaking in government at the intersection of cloud computing adoption and development objectives in government contexts. This contributes to the growing body of knowledge on how IT implementation, particularly cloud computing, can serve as a catalyst for sustainable development through improved governance, service delivery, and digital inclusion.

6.6. Adaptability of the Measurement Scale in Diverse Regions and Institutions

While our study provides a measurement scale for examining government cloud adoption intentions, its broader contribution to IT for development lies in its adaptability across diverse regions and institutional contexts. The scale's psychometric properties suggest that the core constructs—performance expectancy, governance framework, information security, privacy, perceived risk, and government intentions—represent dimensional government cloud adoption decisions in the developmental contexts. However, the successful application of the measurement scale across different regions requires careful consideration of contextual factors that may influence both the relevance of constructs and their measurement properties. The governance framework construct may be perceived differently among federal versus state governments, while cultural dimensions may influence perceptions and prioritise information security and privacy concerns. Additionally, different stages of

regional economic development may require contextualisation of performance expectancy items to reflect development priorities.

Furthermore, the region and institutions' economic development levels and technological infrastructure development may prioritise adaptability and testing to reflect various concerns. For instance, regions with limited cybersecurity capacity may show heightened sensitivity to information security and privacy, while those with more developed digital infrastructures may have different risk perception patterns. Therefore, the regional or institutional adaptation of the measurement scale may consider cultural, economic, government structure, and statistical validation approaches to ensure that the constructs capture how cloud adoption contributes to achieving specific development objectives relevant to each region or institutional context.

Cloud adoption in developing contexts like Nigeria is shaped not only by technological readiness but also by legal sovereignty. The current reliance on foreign cloud infrastructures raises important issues of jurisdiction and regulatory alignment; therefore, a regional cloud governance framework would be recommended. Additionally, policymakers can integrate the scale into readiness assessments, while development partners and cloud providers may use it to identify trust and security bottlenecks that hinder inclusive cloud deployment and adoption.

7. Conclusions, Limitations, and Future Research Directions

This study establishes a validated measurement scale to examine the challenging factors influencing government intention to adopt cloud services. It explains the intricate relationship between these factors in advancing government developmental purposes. These findings answer the research question with clarity and depth while demonstrating how cloud adoption in government settings can serve as a catalyst for socioeconomic development. The measurement items recorded strong factor loadings with a total variance of 70.079% explained, demonstrating the reliability and accuracy of the scale in evaluating the government's intention to adopt cloud services as development enablers.

The high coefficient of reliability (between 0.807 and 0.950) confirms the measurement scale's appropriateness for examining the identified challenging factors in development-oriented cloud adoption decisions. Therefore, contributes to the IT for development field in several significant ways. First, it provides empirically validated constructs that connect technological (cloud computing) adoption decisions to development outcomes through government service delivery. Second, it highlights how barriers to cloud adoption, such as information security concerns, privacy considerations, and governance frameworks, could motivate governments' hesitation to embrace cloud-enabled development pathways without explicit assurances regarding data sovereignty and citizen privacy protection. Third, it demonstrates how performance expectancy in development contexts is closely tied to technology's perceived benefits of cloud services, such as efficiency, cost reduction, and service improvement, which can drive transformative changes to how governments deliver essential services to citizens, particularly in resource-constrained and secure and trusted environments.

The research offers practical guidance on navigating cloud adoption challenges and how government and industry practitioners can more effectively leverage cloud technologies to drive innovation, enhance service delivery, improve resource allocation efficiency, and ultimately accelerate development outcomes. Future research could explore how these identified factors manifest across different government development concepts and regions. By building on these validated measurement scales, the IT for development community can further enhance our understanding of how cloud and other emerging technologies can

be effectively leveraged to address persistent IT development challenges through improved government service delivery in the digital transformation age.

Though the study successfully identified and validated the challenging factors influencing government cloud adoption, its scope is limited to a specific region and organisational context. Future research could explore the applicability of this measurement scale in diverse contexts, including private sector organisations or across different countries. In our future study, the validated measurement instrument will be used to gather responses for further analysis to test the hypotheses and discuss the overall impact of the conceptual model on the research. We acknowledge that while the findings of the current research may seem exclusive to Nigeria, the findings may benefit other developing countries with similar governance structures, regulatory environments, and technological infrastructure. Our research employed cross-sectional data to capture the perceptions of our targeted population. While we acknowledge that cross-sectional data cannot capture changes over time, we recommend that future research could explore longitudinal approaches or comparative studies across different regions to provide a more nuanced understanding.

Author Contributions: Conceptualisation, N.U.; Methodology, N.U.; Validation, N.U.; Formal analysis, N.U., J.A.G. and K.P.; Investigation, N.U.; Data curation, N.U.; Writing—original draft, N.U.; Writing—review & editing, N.U., J.A.G., K.P. and U.C.O.; Supervision, J.A.G. and K.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Informed Consent Statement: Informed consent for participation was obtained from all participants involved in the study.

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 support. This study is part of the ongoing PhD study of the first author.

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

Appendix A

Appendix A.1

Table A1. Constructs and measurement items.

Constructs and Measurement Items			
Constructs		**Measurements Items**	**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

Table A1. *Cont.*

Constructs and Measurement Items			
Constructs		**Measurements Items**	**Factor Loadings**
	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
	InfoSec1	I feel that using cloud services will not keep government information safe	0.912
Information security	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
	PerRisk1	I feel unsafe providing my personally identifiable information while using cloud services	0.812
Perceived risk	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
	GovtInt1	I feel that the government's intention to adopt cloud services will depend on information security measures	0.711
Government intention	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. Poudel, N. The Impact of Big Data-Driven Artificial Intelligence Systems on Public Service Delivery in Cloud-Oriented Government Infrastructures. *J. Artif. Intell. Mach. Learn. Cloud Comput. Syst.* **2024**, *8*, 13–25.

2. Ghazaryan, E. Cloud Computing as a Catalyst for Digital Transformation in Enterprises. *Am. J. Eng. Technol.* **2025**, *7*, 170–177. [CrossRef]
3. Worldbank. Cloud Services Advance Digital Transformation for Governments. 2022. Available online: https://www.worldbank.org/en/news/feature/2022/06/07/cloud-services-advance-digital-transformation-for-governments (accessed on 23 June 2025).
4. ITA. Nigeria Country Commercial Guide. 2024. Available online: https://www.trade.gov/nigeria-country-commercial-guide (accessed on 23 June 2025).
5. Emmanson, J. Cloud Adoption in Nigeria To Yield N30.2 Trillion By 2033, Report Says. 2023. Available online: https://leadership.ng/cloud-adoption-in-nigeria-to-yield-n30-2-trillion-by-2033-report-says/ (accessed on 23 June 2025).
6. Guo, Y.-G.; Yin, Q.; Wang, Y.; Xu, J.; Zhu, L. Efficiency and optimization of government service resource allocation in a cloud computing environment. *J. Cloud Comput.* **2023**, *12*, 18. [CrossRef] [PubMed]
7. Abd Al Ghaffar, H.-t.-A.N. Government cloud computing and national security. *Rev. Econ. Political Sci.* **2024**, *9*, 116–133. [CrossRef]
8. Santos, A.; Martins, J.; Pestana, P.D.; Gonçalves, R.; Mamede, H.S.; Branco, F. Factors Affecting Cloud Computing Adoption in the Education Context—Systematic Literature Review. *IEEE Access* **2024**, *12*, 71641–71674. [CrossRef]
9. 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]
10. Ari, A.A.A.; Ngangmo, O.K.; Titouna, C.; Thiare, O.; Kolyang; Mohamadou, A.; Gueroui, A.M. Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges. *Appl. Comput. Inform.* **2024**, *20*, 119–141.
11. Kshetri, N. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommun. Policy* **2013**, *37*, 372–386. [CrossRef]
12. Onwuegbuna, G.; Etim, E.; Fatile, J. Impact of the 'new normal'—Induced digital transformation on public service delivery and governance in Nigeria: Challenges and opportunities. In *Responsible Management of Shifts in Work Modes–Values for a Post Pandemic Future*; Emerald Publishing Limited: Leeds, UK, 2022; Volume 1, pp. 197–215.
13. Yagboyaju, D.A.; Akinola, A.O. Nigerian State and the Crisis of Governance: A Critical Exposition. *SAGE Open* **2019**, *9*, 2158244019865810. [CrossRef]
14. Wang, S.; Shahzad, M.F.; Ashfaq, M. Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Comput. Secur.* **2024**, *147*, 104051. [CrossRef]
15. Ang'udi, J.J. Security challenges in cloud computing: A comprehensive analysis. *World J. Adv. Eng. Technol. Sci.* **2023**, *10*, 155–181. [CrossRef]
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] [PubMed]
17. Sun, P. Security and privacy protection in cloud computing: Discussions and challenges. *J. Netw. Comput. Appl.* **2020**, *160*, 102642. [CrossRef]
18. Venkatesh, V.; Morris, M.G.; Davis, G.B.; Fred, D. Davis User Acceptance of Information Technology: Toward a Unified View. *MIS Q.* **2003**, *27*, 425–478. [CrossRef]
19. Alhomdy, S.; Thabit, F.; Abdulrazzak, F.H.; Haldorai, A.; Jagtap, S. The role of cloud computing technology: A savior to fight the lockdown in COVID 19 crisis, the benefits, characteristics and applications. *Int. J. Intell. Netw.* **2021**, *2*, 166–174. [CrossRef]
20. Muda, J.; Tumsa, S.; Tuni, A.; Sharma, D.P. Cloud-enabled E-governance framework for citizen centric services. *J. Comput. Commun.* **2020**, *8*, 63–78. [CrossRef]
21. Abdulsalam, Y.S.; Hedabou, M. Security and Privacy in Cloud Computing: Technical Review. *Future Internet* **2022**, *14*, 11. [CrossRef]
22. Patel, A.; Shah, N.; Ramoliya, D.; Nayak, A. A detailed review of Cloud Security: Issues, Threats & Attacks. In Proceedings of the 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA 2020), Coimbatore, India, 5–7 November 2020; pp. 758–764.
23. Politou, E.; Alepis, E.; Virvou, M.; Patsakis, C. Privacy and Personal Data Protection. In *Privacy and Data Protection Challenges in the Distributed Era*; Springer International Publishing: Cham, Switzerland, 2022; pp. 7–12.
24. Mell, P.; Grance, T. *The NIST Definition of Cloud Computing*; National Institute of Standards & Technology: Gaithersburg, MA, USA, 2011; p. 2.
25. Hurwitz, J.S.; Kirsch, D. *Cloud Computing for Dummies*; John Wiley & Sons: Hoboken, NJ, USA, 2020.
26. Ukeje, N. Cloud Computing and Sustainable Environment. In Proceedings of the 2014 Electronics and Telecommunications Research Seminar Series: 13th Workshop Proceedings, University of Bradford, Bradford, UK, 1 April 2014.
27. Wenzek, H. Leapfrogging ICT with Cloud Computing in Emerging Countries. In *ICT for the Next Five Billion People*; Springer: Berlin/Heidelberg, Germany, 2010.
28. Younus, M.; Purnomo, E.P.; Nurmandi, A.; Mutiarin, D.; Manaf, H.A.; Mumtaz, F.; Khairunnisa, T. Analyzing the trend of government support for cloud computing usage in e-government architecture. *J. Cloud Comput.* **2025**, *14*, 14. [CrossRef]

29. Liu, F.; Tong, J.; Mao, J.; Bohn, R.; Messina, J.; Badger, L.; Leaf, D. NIST cloud computing reference architecture. *NIST Spec. Publ.* **2011**, *500*, 292.
30. Kent, S. *Federal Cloud Computing Strategy*; Executive Office of the President of the United States: Washington, DC, USA, 2019.
31. Shafiu, I.; Wang, W.Y.C.; Singh, H. Drivers and barriers in the decision to adopt IaaS: A public sector case study. *Int. J. Bus. Inf. Syst.* **2016**, *21*, 249–267. [CrossRef]
32. Arciprete, C.; Ciani, F. Bridging the Disability Gap in Employment: Insights from an Employability Assessment Tool based on the ICF and the Capability Approach. *J. Hum. Dev. Capab.* **2025**, *26*, 295–305. [CrossRef]
33. Sen, A. *Development as Freedom*; Oxford Uiversity Press: Oxford, UK, 2000; Volume 10, p. 258.
34. Whitman, M.E.; Mattford, H.J. *Management of Information Security*, 6th ed.; Cengage Learning: South Melbourne, VA, Australia, 2019.
35. 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]
36. Arafat, M. Information security management system challenges within a cloud computing environment. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, Amman, Jordan, 26–27 June 2018; pp. 1–6.
37. Kissel, R. *Glossary of Key Information Security Terms*; Diane Publishing: Collingdale, PA, USA, 2011.
38. Numan, D.; Sunna, R. Achieving Digital Trust Through IT Governance and Cybersecurity. 2023. Available online: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/achieving-digital-trust-through-it-governance-and-cybersecurity (accessed on 14 July 2025).
39. Smith, J. Building Trust in Government Through Digital Transformation. 2024. Available online: https://www.government-transformation.com/en/citizen-experience/building-trust-in-government-through-digital-transformation (accessed on 14 July 2025).
40. Shandler, R.; Gomez, M.A. The hidden threat of cyber-attacks—Undermining public confidence in government. *J. Inf. Technol. Politics* **2023**, *20*, 359–374. [CrossRef]
41. Abed, Y.; Chavan, M. The Challenges of Institutional Distance: Data Privacy Issues in Cloud Computing. *Sci. Technol. Soc.* **2019**, *24*, 161–181. [CrossRef]
42. ITU. Privacy in Cloud Computing.pdf. In *ITU-T Technology Watch Report March 2012*; International Telecommunication Union: Geneva, Switzerland, 2012.
43. Pearson, S.; Benameur, A. Privacy, security and trust issues arising from cloud computing. In Proceedings of the 2010 IEEE Second International Conference on Cloud Computing Technology and Science, Indianapolis, IN, USA, 30 November–3 December; IEEE: New York, NY, USA, 2010.
44. Parikh, S.; Dave, D.; Patel, R.; Doshi, N. Security and Privacy Issues in Cloud, Fog and Edge Computing. *Procedia Comput. Sci.* **2019**, *160*, 734–739. [CrossRef]
45. Wei, L.; Zhu, H.; Cao, Z.; Dong, X.; Jia, W.; Chen, Y.; Vasilakos, A.V. Security and privacy for storage and computation in cloud computing. *Inf. Sci.* **2014**, *258*, 371–386. [CrossRef]
46. Manda, M.I.; Backhouse, J. Addressing trust, security and privacy concerns in e-government integration, interoperability and information sharing through policy: A case of South Africa. In Proceedings of the CON-IRM 2016 Proceedings, 67, Cape Town, South Africa, 18–20 May 2016; Available online: https://aisel.aisnet.org/confirm2016/67 (accessed on 14 July 2025).
47. El-Kafrawy, P.M.; Abdo, A.A.; Shawish, A.F. Shawish, Security Issues Over Some Cloud Models. *Procedia Comput. Sci.* **2015**, *65*, 853–858. [CrossRef]
48. Nishad, L.S.; Akriti Paliwal, J.; Pandey, R.; Beniwal, S.; Kumar, S. Security, Privacy Issues and challenges in Cloud Computing: A Survey. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, Udaipur, India, 4–5 March 2016; Association for Computing Machinery: New York, NY, USA, 2016; p. 47.
49. Fernandes, D.A.; Soares, L.F.; Gomes, J.V.; Freire, M.M.; Inácio, P.R. Security issues in cloud environments: A survey. *Int. J. Inf. Secur.* **2014**, *13*, 113–170. [CrossRef]
50. Soni, P.K.; Dhurwe, H. Challenges and Open Issues in Cloud Computing Services. In *Advanced Computing Techniques for Optimization in Cloud*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2024; pp. 19–37.
51. Emeras, J.; Varrette, S.; Plugaru, V.; Bouvry, P. Amazon Elastic Compute Cloud (EC2) versus In-House HPC Platform: A Cost Analysis. *IEEE Trans. Cloud Comput.* **2019**, *7*, 456–468. [CrossRef]
52. Abulhaija, S.; Arroyabe, M.F.; Kwong, C.; Zeng, W. Exploring the impact of external rewards on e-government services adoption: Empirical evidence from Jordan. *Public Manag. Rev.* **2025**, 1–27. [CrossRef]
53. Neves, C.; Oliveira, T.; Cruz-Jesus, F.; Venkatesh, V. Extending the unified theory of acceptance and use of technology for sustainable technologies context. *Int. J. Inf. Manag.* **2025**, *80*, 102838. [CrossRef]
54. Straub, E.T. Understanding Technology Adoption: Theory and Future Directions for Informal Learning. *Rev. Educ. Res.* **2009**, *79*, 625–649. [CrossRef]

55. Walsham, G.; Robey, D.; Sahay, S. Foreword: Special Issue on Information Systems in Developing Countries. *MIS Q.* **2007**, *31*, 317–326. [CrossRef]
56. Osei-Bryson, K.-M.; Brown, I.; Meso, P. Advancing the Development of Contextually Relevant ICT4D Theories—From Explanation to Design. *Eur. J. Inf. Syst.* **2022**, *31*, 1–6. [CrossRef]
57. Zhou, M.; Zhang, R.; Xie, W.; Qian, W.; Zhou, A. Security and privacy in cloud computing: A survey. In Proceedings of the 2010 Sixth International Conference on Semantics, Knowledge and Grids, Washington, DC, USA, 1–3 November 2010; IEEE: New York, NY, USA, 2010.
58. Mohammed, F.; Ibrahim, O.; Ithnin, N. Factors influencing cloud computing adoption for e-government implementation in developing countries. *J. Syst. Inf. Technol.* **2016**, *18*, 297–327. [CrossRef]
59. Wilson, B.M.R.; Khazaei, B.; Hirsch, L. Enablers and Barriers of Cloud Adoption among Small and Medium Enterprises in Tamil Nadu. In Proceedings of the 2015 IEEE International Conference on Cloud Computing in Emerging Markets, CCEM 2015, Bangalore, India, 25–27 November 2015.
60. Miorandi, D.; Rizzardi, A.; Sicari, S.; Coen-Porisini, A. Sticky Policies: A Survey. *IEEE Trans. Knowl. Data Eng.* **2020**, *32*, 2481–2499. [CrossRef]
61. Jiménez, S.D.O.; Anaya, E.A. A Survey on Information Security in Cloud Computing. *Comput. Sist.* **2020**, *24*, 819–833.
62. Kumar, R.; Goyal, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Comput. Sci. Rev.* **2019**, *33*, 1–48. [CrossRef]
63. Chikhaoui, E.; Sarabdeen, J.; Parveen, R. Privacy and security issues in the use of clouds in e-health in the Kingdom of Saudi Arabia. In Proceedings of the 28th International Business Information Management Association Conference—Vision 2020: Innovation Management, Development Sustainability, and Competitive Economic Growth, Seville, Spain, 9–10 November 2016.
64. Gasiba, T.E.; Andrei-Cristian, I.; Lechner, U.; Pinto-Albuquerque, M. Raising Security Awareness of Cloud Deployments using Infrastructure as Code through CyberSecurity Challenges. In Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021; pp. 1–8.
65. Manzoor, A. *Cloud Computing Applications in the Public Sector, in Cloud Computing Technologies for Connected Government*; IGI Global Scientific Publishing: Hershey, PA, USA, 2016; pp. 215–246.
66. Sharma, M.; Sehrawat, R. Quantifying SWOT analysis for cloud adoption using FAHP-DEMATEL approach: Evidence from the manufacturing sector. *J. Enterp. Inf. Manag.* **2020**, *33*, 1111–1152. [CrossRef]
67. Ali, O.; Osmanaj, V. The role of government regulations in the adoption of cloud computing: A case study of local government. *Comput. Law Secur. Rev.* **2020**, *36*, 105396. [CrossRef]
68. Joshi, J.B.; 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, USA, 2002; pp. 121–136.
69. Muhammed, K.; Zaharaddeen, I.; Rumana, K.; Turaki, A.M. Cloud Computing Adoption in Nigeria: Challenges and Benefits. *Int. J. Sci. Res. Publ.* **2015**, *5*, 1–7.
70. Wang, L.; Zhang, Q.; Ding, Y.-Y.; Wong, P.P.W. The Effect of Social and Personal Norm on Intention to Patronize Green Hotels: Extension of Theory of Planned Behavior. *J. China Tour. Res.* **2023**, *19*, 311–334. [CrossRef]
71. Al-Adwan, A.S.; Li, N.; Al-Adwan, A.; Abbasi, G.A.; Albelbisi, N.A.; Habibi, A. Extending the Technology Acceptance Model (TAM) to Predict University Students' Intentions to Use Metaverse-Based Learning Platforms. *Educ. Inf. Technol.* **2023**, *28*, 15381–15413. [CrossRef] [PubMed]
72. Habibi, A.; Riady, Y.; Al-Adwan, A.S.; Albelbisi, N.A. Beliefs and Knowledge for Pre-Service Teachers' Technology Integration during Teaching Practice: An Extended Theory of Planned Behavior. *Comput. Sch.* **2023**, *40*, 107–132. [CrossRef]
73. 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]
74. Nguyen, T.D.; Nguyen, D.T.; Cao, T.H. Acceptance and use of information system: E-learning based on cloud computing in Vietnam. In Proceedings of the Information and Communication Technology-EurAsia Conference, Bali, Indonesia, 14–17 April 2014; pp. 139–149.
75. Amron, M.T.; Ibrahim, R.; Bakar, N.A.A. Cloud computing acceptance among public sector employees. *Telkomnika (Telecommun. Comput. Electron. Control)* **2021**, *19*, 124–133. [CrossRef]
76. 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]
77. Sharma, R.; Mishra, R. A review of evolution of theories and models of technology adoption. *Indore Manag. J.* **2014**, *6*, 17–29.
78. Hiller, J. *Epistemological Foundations of Objectivist and Interpretivist Research in An Introduction to Music Therapy Research*; Murphy, K.M., Wheeler, B.L., Eds.; Barcelona Publishers: New Braunfels, TX, USA, 2016; pp. 99–127.

79. Hagger, M.S. *The Reasoned Action Approach and the Theories of Reasoned Action and Planned Behavior*; Oxford University Press: Oxford, UK, 2019. [CrossRef]
80. Kala, D.; Chaubey, D.S.; Meet, R.K.; Al-Adwan, A.S. Impact of user satisfaction with e-government services on continuance use intention and citizen trust using TAM-ISSM framework. *Interdiscip. J. Inf. Knowl. Manag.* **2024**, *19*, 001. [CrossRef]
81. Ciancarini, P.; Giancarlo, R.; Grimaudo, G. Digital Transformation in the Public Administrations: A Guided Tour for Computer Scientists. *IEEE Access* **2024**, *12*, 22841–22865. [CrossRef]
82. Paul, D.; Soundarapandiyan, R.; Krishnamoorthy, G. Security-First Approaches to CI/CD in Cloud-Computing Platforms: Enhancing DevSecOps Practices. *Aust. J. Mach. Learn. Res. Appl.* **2021**, *1*, 184–225.
83. Okon, S.U.; Olateju, O.O.; Ogungbemi, O.S.; Joseph, S.A.; Olisa, A.O.; Olaniyi, O.O. Incorporating Privacy by Design Principles in the Modification of AI Systems in Preventing Breaches Across Multiple Environments, Including Public Cloud, Private Cloud, and On-Prem. *J. Eng. Res. Rep.* **2024**, *26*, 136–158. [CrossRef]
84. Najibi, M.; Hadavinejad, M. From E-Government Readiness to Public Trust: Explaining the Mediating Role of Organizational Transparency. *State Stud.* **2024**, *10*, 305–328.
85. 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]
86. Akram, M.S.; Malik, A.; Shareef, M.A.; Goraya, M.A.S. 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]
87. Faqih, K.M.S. Factors influencing the behavioral intention to adopt a technological innovation from a developing country context: The case of mobile augmented reality games. *Technol. Soc.* **2022**, *69*, 101958. [CrossRef]
88. Joshi, A.; Benitez, J.; Huygh, T.; Ruiz, L.; De Haes, S. Impact of IT governance process capability on business performance: Theory and empirical evidence. *Decis. Support Syst.* **2022**, *153*, 113668. [CrossRef]
89. Salem, M.M.; Hwang, G.-H. Critical Factors Influencing Adoption of Cloud Computing for Government Organizations in Yemen. *J. Distrib. Sci.* **2016**, *14*, 37–47. [CrossRef]
90. 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]
91. Rana, N.P.; Dwivedi, Y.K.; Lal, B.; Williams, M.D.; Clement, M. Citizens' adoption of an electronic government system: Towards a unified view. *Inf. Syst. Front.* **2017**, *19*, 549–568. [CrossRef]
92. Vurukonda, N.; Rao, B.T. A Study on Data Storage Security Issues in Cloud Computing. *Procedia Comput. Sci.* **2016**, *92*, 128–135. [CrossRef]
93. Riffai, M.M.M.A.; Grant, K.; Edgar, D. Big TAM in Oman: Exploring the promise of on-line banking, its adoption by customers and the challenges of banking in Oman. *Int. J. Inf. Manag.* **2012**, *32*, 239–250. [CrossRef]
94. Hanafizadeh, P.; Behboudi, M.; Koshksaray, A.A.; Tabar, M.J.S. Mobile-banking adoption by Iranian bank clients. *Telemat. Inform.* **2014**, *31*, 62–78. [CrossRef]
95. Alalwan, A.A.; Dwivedi, Y.K.; Rana, N.P.; Algharabat, R. Examining factors influencing Jordanian customers' intentions and adoption of internet banking: Extending UTAUT2 with risk. *J. Retail. Consum. Serv.* **2018**, *40*, 125–138. [CrossRef]
96. Martins, C.; Oliveira, T.; Popovič, A. Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *Int. J. Inf. Manag.* **2014**, *34*, 1–13. [CrossRef]
97. Chao, C.-M. Factors determining the behavioral intention to use mobile learning: An application and extension of the UTAUT model. *Front. Psychol.* **2019**, *10*, 1652. [CrossRef]
98. Creswell, J.W. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 4th ed.; SAGE Publications: Thousand Oaks, CA, USA, 2014.
99. Ahmadin, M. Social Research Methods: Qualitative and Quantitative Approaches. *J. Kaji. Sos. Dan Budaya: Tebar Sci.* **2022**, *6*, 104–113.
100. Bhattacherjee, A. *Social Science Research: Principles, Methods, and Practices*; University of South Florida: Tampa, FL, USA, 2012.
101. Vicente, P.; Reis, E. Using questionnaire design to fight nonresponse bias in web surveys. *Soc. Sci. Comput. Rev.* **2010**, *28*, 251–267. [CrossRef]
102. Leeuw, E.d.; Berzelak, N. *The SAGE Handbook of Survey Methodology*; SAGE Publications Ltd: London, UK, 2016.
103. de Sena Abrahão, R.; Moriguchi, S.N.; Andrade, D.F. Intention of adoption of mobile payment: An analysis in the light of the Unified Theory of Acceptance and Use of Technology (UTAUT). *RAI Rev. Adm. Inov.* **2016**, *13*, 221–230. [CrossRef]
104. Khalilzadeh, J.; Ozturk, A.B.; Bilgihan, A. Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry. *Comput. Hum. Behav.* **2017**, *70*, 460–474. [CrossRef]
105. Venkatesh, V.; Thong, J.Y.; 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]
106. Zhou, T.; Lu, Y.; Wang, B. Integrating TTF and UTAUT to explain mobile banking user adoption. *Comput. Hum. Behav.* **2010**, *26*, 760–767. [CrossRef]

107. Pallant, J. *SPSS Survival Manual: A Step by Step Guide to Data Analysis Using, IBM SPSS*, 7th ed.; Allen & Unwin: Crows Nest, Australia, 2020.
108. Lesia, M.P.; Aigbavboa, C.O.; Thwala, W.D. Factors influencing residential location choice in South Africa: Exploratory factor analysis (EFA) and confirmatory factor analysis (CFA). *J. Hous. Built Environ.* **2024**, *39*, 133–160. [CrossRef]
109. Hooper, D. *Exploratory Factor Analysis in Approaches to Quantitative Research—Theory Its Practical Application: A Guide to Dissertation Students*; Chen, H., Ed.; Oak Tree Press: Cork, Ireland, 2012.
110. Thompson, B. *Exploratory and Confirmatory Factor Analysis: Understanding Concepts and Applications*, 1st ed.; American Psychological Association: Washington, DC, USA, 2004.
111. Antunes, A.A.M.; Neves, G.A.; Rojas, B.P.S.; Vaz, D.V. Test-retest reliability and internal structure of the Brazilian version of the impact on participation and autonomy (IPA-Br4) for individuals with physical disabilities. *Braz. J. Phys. Ther.* **2025**, *29*, 101152. [CrossRef]
112. Ustun, A.B.; Karaoglan-Yilmaz, F.G.; Yilmaz, R.; Ceylan, M.; Uzun, O. Development of UTAUT-based augmented reality acceptance scale: A validity and reliability study. *Educ. Inf. Technol.* **2024**, *29*, 11533–11554. [CrossRef]
113. Yong, A.G.; Pearce, S. A beginner's guide to factor analysis: Focusing on exploratory factor analysis. *Tutor. Quant. Methods Psychol.* **2013**, *9*, 79–94. [CrossRef]
114. Tabachnick, B.G.; Fidell, L.S. *Using Multivariate Statistics*, 6th ed.; Pearson Education: Boston, MA, USA, 2013.
115. Väänänen, N.; Vilhunen, K. Exploratory factor analysis of sustainable craft theory among Finnish craft hobbyists. *Craft Res.* **2024**, *15*, 13–40. [CrossRef]
116. De Winter, J.C.F.; Dodou, D. Factor recovery by principal axis factoring and maximum likelihood factor analysis as a function of factor pattern and sample size. *J. Appl. Stat.* **2012**, *39*, 695–710. [CrossRef]
117. Mabel, O.A.; Olayemi, O.S. A comparison of principal component analysis, maximum likelihood and the principal axis in factor analysis. *Am. J. Math. Stat.* **2020**, *10*, 44–54.
118. Stevens, J. *Applied Multivariate Statistics for the Social Sciences*, 5th ed.; Routledge: New York, NY, USA, 2009.
119. Akbulut, Y. *SPSS Applications in Social Sciences*; Ideal Culture Publishing: Istanbul, Turkey, 2010.
120. Guadagnoli, E.; Velicer, W.F. Relation of sample size to the stability of component patterns. *Psychol. Bull.* **1988**, *103*, 265. [CrossRef]
121. Fornell, C.; Larcker, D.F. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]
122. 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*, 785–787. [CrossRef]
123. Hair, J.F., Jr. *Multivariate Data Analysis*, 7th ed.; Pearson/Prentice Hall: Upper Saddle River, NJ, USA, 2010.
124. Büyüköztürk, Ş. *Data Analysis for Social Sciences Manual Statistics, Research Pattern SPSS Applications and Reviews*; Pegem Academy Publishing: Ankara, Turkey, 2018; pp. 001–214.
125. Yaseen, H.; Al-Adwan, A.S.; Nofal, M.; Hmoud, H.; Abujassar, R.S. Factors Influencing Cloud Computing Adoption Among SMEs: The Jordanian Context. *Inf. Dev.* **2023**, *39*, 317–332. [CrossRef]
126. Lazar, I.M.; Panisoara, G.; Panisoara, I.O. Digital technology adoption scale in the blended learning context in higher education: Development, validation and testing of a specific tool. *PLoS ONE* **2020**, *15*, e0235957. [CrossRef] [PubMed]
127. Mahmood, M.; Vishanth, W.; Chen, W. The influence of transformed government on citizen trust: Insights from Bahrain. *Inf. Technol. Dev.* **2019**, *25*, 275–303. [CrossRef]
128. Levite, A.E.; Kalwani, G. *Cloud Governance Challenges: A Survey of Policy and Regulatory Issues*; Carnegie Endowment for International Peace: Washington, DC, USA, 2020.
129. Obi, O.C.; Akagha, O.V.; Dawodu, S.O.; Anyanwu, A.C.; Onwusinkwue, S.; Ahmad, I.A.I. Comprehensive review on cybersecurity: Modern threats and advanced defense strategies. *Comput. Sci. IT Res. J.* **2024**, *5*, 293–310. [CrossRef]
130. Markey, S.; Greg, H.; Manson, D. Closing the implementation gap: A framework for incorporating the context of place in economic development planning. *Local Environ.* **2008**, *13*, 337–351. [CrossRef]
131. Savela, T. The advantages and disadvantages of quantitative methods in schoolscape research. *Linguist. Educ.* **2018**, *44*, 31–44. [CrossRef]
132. Dow, S.C. Methodological Pluralism and Pluralism of Method. In *Foundations for New Economic Thinking: A Collection of Essays*; Palgrave Macmillan UK: London, UK, 2012; pp. 129–139.