Journal of Computer Science, Technology and Innovation (JCSTI)

EFFECT OF TECHNOLOGICAL SECURITY CAPABILITY ON SECURE CLOUD ADOPTION AMONG KENYAN STATE CORPORATIONS

Samson Odhiambo, Ms. Jenu John and **Mr. Nyakoni Omwando**

Journal of Computer Science, Technology and Innovation (JCSTI)
ISSN: 1364-4009
Vol.3, Issue.No.2, 2026

Effect of Technological Security Capability On Secure Cloud Adoption Among Kenyan State Corporations

Samson Odhiambo
Corresponding Author, Kenya Methodist University
Ms. Jenu John
Lecturer, Kenya Methodist University Department of Computer Science School of Science and Technology
Mr. Nyakoni Omwando
Lecturer, Kenya Methodist University Department of Computer Science School of Science and Technology

Article History:
Published on: 06/07/2026
***DOI*:**
https://doi.org/10.5281/zenodo.21215712
***How to cite*:** Odhiambo, S., John, J., & Omwando, N. (2026). Effect of Technological Security Capability On Secure Cloud Adoption Among Kenyan State Corporations. *Journal of Computer Science, Technology and Innovation (JCSTI)*, 3(2), 1–16.
https://doi.org/10.5281/zenodo.21215712

Abstract:
***Purpose of the Study*:** This study examined the effect of technological security capability on secure cloud adoption among Kenyan state corporations. Specifically, it assessed whether technological security measures, including identity and access management, encryption, security monitoring, incident response readiness, and vulnerability assessment, significantly influence the secure adoption of cloud computing within public sector institutions.
Methodology: The study adopted a quantitative cross-sectional survey design guided by the Technology–Organisation–Environment (TOE) framework. Data were collected using structured questionnaires from ICT decision-makers in Kenyan state corporations. Responses from 112 participants were analyzed using SPSS Version 29 and SmartPLS 4 through Partial Least Squares Structural Equation Modelling (PLS-SEM).
Findings: The findings revealed that technological security capability had a positive but statistically non-significant effect on secure cloud adoption ($\beta = 0.303$, $t = 1.587$, $p = 0.057$). State corporations reported moderate to high levels of technological security capability, with data encryption receiving the highest ratings and cyber incident response readiness the lowest. The results suggest that while technological security controls contribute to secure cloud adoption, they are insufficient on their own. Their effectiveness depends on complementary organisational capabilities, governance structures, operational competencies, and enabling digital infrastructure that collectively support secure implementation and management of cloud computing environments.
Conclusion: The study concludes that technological security capability is a necessary but insufficient determinant of secure cloud adoption among Kenyan state corporations. Sustainable adoption requires integrating technical security controls with organisational readiness, governance mechanisms, skilled personnel, and supportive infrastructure to achieve secure, resilient, and effective cloud computing implementation.

Keywords: *Technological Security Capability, Secure Cloud Adoption, State Corporations, Kenya, TOE Framework, PLS-SEM, Identity and Access Management, Cloud Security*

1. INTRODUCTION

1.1 Background of the Study

Cloud computing has revolutionized the way governments and organizations acquire, manage, and deliver information technology services by enabling on-demand access to computing resources through internet-based platforms. Compared to traditional on-premise infrastructure, cloud computing offers improved scalability, operational flexibility, cost efficiency, business continuity, and rapid deployment of digital services (Armbrust et al., 2010). Consequently, governments worldwide have increasingly embraced cloud computing as a strategic enabler of digital transformation, e-government, and public service modernization. However, as organizations migrate critical workloads and sensitive information to cloud environments, technological security capability has become an essential requirement for ensuring secure cloud adoption. Technological security capability refers to an organization's ability to implement and manage technical safeguards such as identity and access management (IAM), encryption, security monitoring, vulnerability management, and incident response mechanisms that protect cloud-hosted systems and information assets (Kshetri, 2013). Strong technological security capabilities significantly reduce cybersecurity risks while enhancing confidence in cloud computing adoption (Reece et al., 2023).

From a global perspective, developed economies have invested substantially in technological security capabilities to facilitate secure cloud adoption within government institutions. In the United Kingdom, the government's Cloud First Policy has been supported by robust cybersecurity governance through the National Cyber Security Centre (NCSC), enabling secure migration of public services while ensuring compliance with strict information security and privacy regulations. This approach has strengthened resilience against evolving cyber threats and enhanced public confidence in digital government services (Reece et al., 2023). Similarly, Singapore has emerged as one of Asia's leading digital governments through its Government on Commercial Cloud (GCC) initiative, which incorporates advanced encryption technologies, centralized identity management, zero-trust architecture, and continuous security monitoring. These technological security investments have enabled secure delivery of digital public services while minimizing cybersecurity risks associated with cloud infrastructure (Amini & Imani, 2021). These international experiences demonstrate that technological security capability is a critical determinant of successful cloud adoption.

At the regional level, African governments have increasingly recognized cloud computing as a catalyst for digital transformation and improved public service delivery, although technological security capabilities remain uneven across countries. In Ghana, cloud adoption has accelerated under the national digital transformation agenda, supported by improvements in cybersecurity legislation, digital identity systems, and institutional cybersecurity frameworks. Nevertheless, inadequate cybersecurity infrastructure and shortages of skilled personnel continue to constrain

secure cloud implementation within many public institutions (Amini & Imani, 2021). In South Africa, cloud adoption has expanded rapidly across both public and private sectors following increased investment in cybersecurity governance, implementation of the Cybercrimes Act, and establishment of national cybersecurity strategies. Despite these advances, cyberattacks targeting government systems have continued to expose weaknesses in cloud security management, highlighting the importance of strengthening technological security capabilities to safeguard critical information assets (Chigada & Madzinga, 2021). These regional experiences illustrate that technological security capability remains central to successful cloud adoption across African public institutions.

Within the Kenyan context, cloud computing has become a key pillar of public sector digital transformation. The Government of Kenya has promoted cloud adoption through the Kenya National ICT Policy (2020) and the Kenya Cloud Policy (2025), both of which encourage state corporations to migrate digital services to secure cloud environments to improve efficiency, interoperability, and citizen service delivery. Additionally, increasing digitization of government functions has expanded reliance on cloud platforms for managing financial systems, health information, procurement processes, education services, and citizen databases. However, this digital transformation has simultaneously increased exposure to cybersecurity threats, making technological security capability indispensable for secure cloud adoption. Effective implementation of identity and access management systems, encryption technologies, continuous monitoring, vulnerability management, and incident response mechanisms has therefore become essential for protecting sensitive government information and maintaining public trust (Communications Authority of Kenya, 2023).

Despite these policy initiatives, empirical evidence indicates that technological security capability remains a significant challenge in Kenya. According to Gichubi et al. (2024), more than 60% of Kenyan organizations utilizing cloud services experienced at least one cloud-related security incident, with weak access controls and system misconfigurations accounting for approximately one-quarter of all reported incidents. Similarly, Wachanga & Ndiege (2018) identified inadequate cybersecurity infrastructure, limited technical expertise, and concerns over data security as major barriers to cloud adoption within Kenya's public sector. While previous studies have examined cloud computing adoption in private organizations and developed economies, limited empirical evidence exists regarding how technological security capability influences secure cloud adoption among Kenyan state corporations operating under unique regulatory requirements, governance structures, and public accountability obligations. This knowledge gap necessitated the present study, which sought to examine the effect of technological security capability on secure cloud adoption among Kenyan state corporations and generate evidence to support cybersecurity policy, institutional capacity building, and implementation of Kenya's cloud-first digital transformation agenda.

1.2 Statement of the Problem

Kenya's state corporations are at varying stages of cloud adoption, with 79.5% of surveyed institutions reporting active use of cloud services for either core or non-core functions (Communications Authority of Kenya, 2023). However, adoption has not been uniformly secure. The Communications Authority of Kenya reported a dramatic escalation in cyber threat events across the public sector, and state corporations have been among the most frequently targeted entities. Incidents involving data breaches, ransomware, and unauthorised access to government cloud environments have raised serious questions about the adequacy of the technical security controls that state corporations have in place. While the government has introduced regulatory frameworks — including the Computer Misuse and Cybercrimes Act of 2018, the Data Protection Act of 2019, and the Kenya Cloud Policy of 2025 to guide secure adoption, compliance with these frameworks does not automatically guarantee the presence of effective technical security controls. Studies in comparable contexts suggest that organisations may satisfy regulatory documentation requirements without implementing the substantive technical measures that underpin genuine cloud security (Alreemy et al., 2024). It is therefore unclear whether the technological security capabilities of Kenyan state corporations are sufficient to support secure cloud adoption, and whether the level of technical security capability an institution possesses meaningfully predicts the extent of its secure cloud adoption. This study was designed to generate quantitative empirical evidence to address this question.

1.3 Purpose of the Study

The purpose of this study was to examine the effect of technological security capability on secure cloud adoption among Kenyan state corporations.

1.4 Research Hypothesis

$H0_1$: Technological security capability does not have a statistically significant effect on secure cloud adoption among Kenyan state corporations.

2. LITERATURE REVIEW

2.1 Theoretical Framework: Technology–Organisation–Environment (TOE) Framework

This study is grounded in the Technology–Organisation–Environment (TOE) framework, originally developed by Tornatzky and Fleischer (1990). The framework categorises the determinants of technology adoption into three contextual pillars: the technological context, referring to the internal and external technologies available to an organization and their characteristics; the organizational context, encompassing a firm's internal characteristics including

leadership, culture, and human capital; and the environmental context, which includes the industry structure, regulatory environment, and competitive pressures within which an organization operates. The TOE framework is well suited to this study for several reasons. It has been extensively validated in information systems research and cloud computing adoption studies across diverse sectors and geographies (Amini & Imani, 2021; Oliveira et al., 2014). Its technological pillar directly accommodates the concept of technological security capability as a driver of cloud adoption decisions. Critically, while TOE identifies the categories of adoption determinants, it does not explain how individual perceptions of specific technology attributes shape adoption behaviour, necessitating theoretical supplementation. For this study, TOE serves as the overarching analytical structure within which technological security capability is examined as the primary predictor of secure cloud adoption.

2.2 Technological Security Capability and Secure Cloud Adoption

Technological security capability refers to an organisation's ability to implement, manage, and sustain the technical controls required to protect data and systems within cloud environments. Kshetri (2013) identified encryption, identity and access management (IAM), and audit logging as central security enablers in cloud environments. More recent scholarship confirms that these technical controls remain foundational but that their effectiveness depends critically on how well they are configured, monitored, and maintained over time (Alreemy et al., 2024).

Armbrust et al. (2010) highlighted technical scalability and security architecture as primary enablers of cloud migration, while subsequent literature has focused more specifically on the governance and operational challenges of maintaining security in multi-cloud and hybrid cloud environments. Reece et al. (2023) identified the multi-cloud environment as a particular security challenge, noting that expanding cloud footprints increases the attack surface through credential stealing, privilege escalation, and man-in-the-middle attacks. These findings suggest that technological security capability must be understood not merely as the presence of specific tools but as the organisation's demonstrated operational proficiency in deploying and sustaining those tools across dynamic cloud environments.

In the Kenyan context, Gichubi et al. (2024) reported that over 60% of Kenyan enterprises adopting cloud services had experienced security incidents, with weak access controls and system misconfigurations being the leading vulnerability categories. Wachanga & Ndiege (2018) argued that inadequate technical infrastructure remains the primary barrier to secure cloud adoption in Kenya, while Zwilling et al. (2022) contended that human and governance factors outweigh technical limitations in many developing country contexts. This divergence in findings supports the present study's examination of technological security capability as a distinct variable, allowing its independent contribution to adoption outcomes to be isolated and assessed.

A significant concern identified in the Kenyan public sector literature is the misperception of the shared responsibility model. Chigada and Madzinga (2021) found that end-users in Kenya's public sector tend to assign full security responsibility to cloud service providers rather than recognising their own organisational obligations under the shared responsibility framework. This misperception compounds existing technical vulnerabilities by reducing the organisational attention given to configuring and maintaining the security controls that fall within the client's responsibility domain, including access management, data classification, and configuration monitoring. Addressing this gap requires not only awareness-raising but the institutionalisation of technical security competencies within the state corporation's ICT function.

3. RESEARCH METHODOLOGY

This This study adopted a pragmatist research philosophy and a quantitative cross-sectional survey correlational design to examine the effect of technological security capability on secure cloud adoption among Kenyan State Corporations. The target population comprised ICT-enabled state corporations with active or planned cloud adoption initiatives, focusing on Chief Information Officers, Information Security Officers, ICT Managers, and Data Protection Officers. Stratified purposive sampling was employed to select 100–150 respondents from 40–60 state corporations, guided by power analysis for Partial Least Squares Structural Equation Modelling (PLS-SEM). Primary data were collected using a structured self-administered questionnaire developed from validated scales and refined through expert review, cognitive pretesting, and pilot testing to ensure validity and reliability. Data were analysed using SPSS Version 29 for descriptive statistics and SmartPLS 4 for measurement and structural model assessment. The analysis evaluated the direct effect of technological security capability on secure cloud adoption using bootstrapping techniques and path coefficients. Diagnostic tests, including reliability, validity, multicollinearity, normality, and common method bias, were conducted before hypothesis testing.

4. RESEARCH FINDINGS AND DISCUSSION

4.1 Introduction

This chapter presents the results and analysis of the empirical data collected from ICT-enabled Kenyan state corporations to examine the effect of technological security capability on secure cloud adoption. The chapter is organized as follows: it begins with the response rate and sample characteristics, followed by descriptive statistics for the technological security capability measurement items, the measurement model assessment covering reliability and validity, diagnostic tests, the structural model results addressing the study hypothesis, and a discussion of the findings within the theoretical framework. Only data and analysis directly pertaining to the

relationship between technological security capability and secure cloud adoption are presented in this chapter.

4.2 Response Rate and Sample Characteristics

A total of 150 structured questionnaires were distributed to ICT decision-makers across 47 ICT-enabled Kenyan state corporations. Of these, 126 questionnaires were returned, representing an overall response rate of 84.0%. Following data cleaning and the removal of incomplete responses with more than 10% missing values or evidence of straight-line responding, 112 valid responses were retained for analysis, yielding a usable response rate of 74.7%. This sample size exceeds the minimum of 98 respondents determined through a priori power analysis using G*Power 3.1 (Faul, Erdfelder, Buchner, & Lang, 2009) and satisfies the sample size requirements for PLS-SEM analysis (Hair et al., 2022). The respondent profile is presented in Table 1 below.

Table 1: Respondent Demographic Profile

Characteristic / Category	Frequency (n = 112)	Percentage (%)
Role		
Chief Information Officer (CIO)	28	25.0
Chief Information Security Officer (CISO)	31	27.7
ICT Manager	34	30.4
Data Protection / Compliance Officer	19	17.0
Years of Experience		
Less than 2 years	8	7.1
2 – 5 years	29	25.9
6 – 10 years	42	37.5
More than 10 years	33	29.5
Corporation Type		
Commercial / Revenue-Generating	38	33.9
Regulatory Body with Digital Mandate	32	28.6
Service Delivery Parastatal	42	37.5
Cloud Adoption Status		
Core business operations	41	36.6
Limited / non-core functions	48	42.9
Planned within 12 months	15	13.4
Not currently planned	8	7.1

Source: Survey Data (2025)

The respondent profile indicates that the majority of participants 67.0% possessed six or more years of experience in ICT, information security, or data protection and compliance, confirming

that respondents held sufficient domain expertise to provide reliable assessments of their organisations' cloud security posture and technological security practices. The distribution across corporation types was reasonably balanced, with commercial or revenue-generating parastatals representing 33.9%, regulatory bodies 28.6%, and service delivery institutions 37.5%, ensuring that findings reflect a cross-section of the Kenyan state corporation sector. Notably, 79.5% of respondents indicated that their organisations were actively using cloud services for either core operations or limited functions, confirming that cloud adoption is an operational reality for the large majority of ICT-enabled state corporations and that technological security capability is a practically relevant concern for the study population.

4.3 Descriptive Statistics for Technological Security Capability

Technological security capability (TSC) was measured using five items on a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). The items assessed respondents' perceptions of their organisations' proficiency in identity and access management, data encryption, security logging and monitoring, cyber incident response readiness, and vulnerability assessment and auditing. Table 2 presents the descriptive statistics for each TSC item and the composite TSC index.

Table 2: Descriptive Statistics for Technological Security Capability Items

Item	Mean	Median	Std. Dev.	Skewness	Kurtosis
TSC1 – Identity and Access Management controls	3.964	4.000	0.972	-0.460	-0.923
TSC2 – Data encryption standards	4.277	5.000	0.868	-0.905	-0.222
TSC3 – Security logging and monitoring	3.938	4.000	0.985	-0.442	-0.947
TSC4 – Cyber incident response readiness	3.911	4.000	0.969	-0.416	-0.898
TSC5 – Vulnerability assessment and auditing	4.000	4.000	0.982	-0.516	-0.913
Composite TSC Index	**4.018**	**4.000**	**0.955**	**-0.548**	**-0.781**

Source: Survey Data (2025)

The mean scores for TSC items ranged from 3.911 (TSC4: Cyber incident response readiness) to 4.277 (TSC2: Data encryption standards), indicating that respondents perceived their organisations as having moderate to moderately high levels of technological security capability across all five dimensions. The highest mean score was recorded for data encryption (M = 4.277, SD = 0.868),

suggesting that encryption is the most consistently implemented technical control across the sampled state corporations. This finding is consistent with the emphasis that Kenya's Data Protection Act of 2019 places on data protection measures, which has led many institutions to prioritise encryption as a visible compliance measure (Alreemy et al., 2024). The lowest mean score among TSC items was recorded for cyber incident response readiness (TSC4: M = 3.911, SD = 0.969), indicating that while respondents perceived their organisations as having some incident response capability, this dimension was rated comparatively lower than other security controls. This finding is practically significant because incident response readiness is a critical determinant of an organisation's ability to limit the damage caused by security breaches, and lower readiness scores suggest that state corporations may be better equipped to prevent some attacks than to effectively respond once an incident has occurred. The negative skewness values across all TSC items (ranging from -0.460 to -0.905) indicate that responses were skewed toward agreement, and kurtosis values within acceptable ranges (|<| 2) confirm approximate univariate normality, supporting the use of PLS-SEM.

4.4 Measurement Model Assessment

Before evaluating the structural model, the measurement model was assessed to confirm the reliability and validity of the TSC and SCA constructs. The assessment followed the two-step approach recommended by Anderson and Gerbing (1988) and Hair et al. (2022), examining indicator reliability, internal consistency reliability, convergent validity, and discriminant validity.

4.4.1 Indicator Reliability and Internal Consistency

Indicator reliability was assessed by examining the outer loadings of each TSC item on the construct. Table 3 presents the outer loadings for all five TSC items. All items exceeded the recommended threshold of 0.70 (Hair et al., 2022), with loadings ranging from 0.912 to 0.950. These values confirm that each item shares a substantial proportion of variance with the TSC construct, establishing adequate indicator reliability.

Table 3: TSC Indicator Outer Loadings

Item	Outer Loading
TSC1 – Identity and Access Management controls	0.913
TSC2 – Data encryption standards	0.912
TSC3 – Security logging and monitoring	0.950
TSC4 – Cyber incident response readiness	0.912
TSC5 – Vulnerability assessment and auditing	0.946

Source: SmartPLS 4 Output (2025)

Internal consistency reliability and convergent validity for both the TSC and SCA constructs are presented in Table 4. Cronbach's Alpha for TSC was 0.957 and Composite Reliability (rho_c) was 0.967, both substantially exceeding the recommended threshold of 0.70 (Nunnally & Bernstein, 1994; Hair et al., 2022). The Average Variance Extracted (AVE) for TSC was 0.854, well above the 0.50 threshold required to confirm convergent validity (Fornell & Larcker, 1981), indicating that TSC explains over 85% of the variance in its five measurement items.

Table 4: Internal Consistency Reliability and Convergent Validity

Construct	Cronbach's Alpha	Composite Reliability (rho_c)	Average Variance Extracted (AVE)	Outer Loadings Range
Technological Security Capability (TSC)	0.957	0.967	0.854	0.912 – 0.950
Secure Cloud Adoption (SCA)	0.961	0.968	0.836	0.824 – 0.973

Source: SmartPLS 4 Output (2025)

The measurement model results confirm that the TSC construct is both reliably measured and sufficiently distinct from measurement error to support meaningful structural model testing. The high reliability and convergent validity coefficients also confirm that the five-item TSC scale developed for this study constitutes a robust and internally consistent measure of technological security capability in the Kenyan state corporation context.

4.4.2 Common Method Bias and Multicollinearity

Since all data were collected from a single respondent group through a single questionnaire administration, common method bias (CMB) was assessed using Harman's single-factor test in SPSS. All 27 measurement items across the full study instrument were entered into an exploratory factor analysis with a single factor extracted. The single factor explained 39.2% of the total variance, which is below the 50% threshold that indicates problematic CMB (Podsakoff et al., 2003). In addition, procedural design remedies were implemented, including the separation of predictor and criterion variable items across distinct questionnaire sections and the assurance of complete respondent anonymity. These combined procedural and statistical assessments confirm that common method bias does not pose a meaningful threat to the validity of the study's findings.

Multicollinearity was assessed using Variance Inflation Factor (VIF) values computed in SmartPLS 4. The VIF value for the TSC construct as a predictor of SCA was 1.000, which is

substantially below the conservative threshold of 3.3 recommended by Hair et al. (2022), confirming that multicollinearity does not affect the reliability of the structural model results.

4.5 Structural Model Assessment: Effect of Technological Security Capability on Secure Cloud Adoption

Following confirmation of the measurement model's adequacy, the structural model was evaluated to test Hypothesis 1, which predicted that technological security capability positively and significantly influences secure cloud adoption among Kenyan state corporations. The structural model was assessed using path coefficients (β), t-statistics generated through bootstrapping with 5,000 resamples, p-values, and effect sizes (f^2). The results are presented in Table 5.

Table 5: Structural Model Result – Effect of TSC on Secure Cloud Adoption

Hypothesis / Relationship	Path Coefficient (β)	t-statistic	p-value	Effect Size (f^2)	Decision
H1: TSC → SCA	0.303	1.587	0.057	0.091	Not Supported (p > 0.05)

Source: SmartPLS 4 Bootstrapping Output (2025);

Significance assessed at $p < 0.05$

The path coefficient for TSC → SCA was β = 0.303 with a t-statistic of 1.587 and a p-value of 0.057. While the direction of the effect was positive and consistent with the theoretical expectation that greater technological security capability should facilitate greater secure cloud adoption, the coefficient did not reach the conventional threshold for statistical significance at $p < 0.05$. The null hypothesis (H01) is therefore not rejected. The effect size $f^2 = 0.091$ falls within the small-to-medium range according to the classification proposed by Cohen (1988) as adapted for PLS-SEM by Hair et al. (2022), indicating that TSC has a practically meaningful but context-conditioned relationship with SCA. The overall explanatory power of the model, represented by the R^2 value for SCA, was 0.990, indicating that the integrated set of predictors explains 99.0% of the variance in secure cloud adoption, and the predictive relevance (Q^2) was 0.981, confirming the model's strong predictive capacity. These values are presented in Table 6.

Table 6: Model Explanatory Power and Predictive Relevance

Dependent Variable	R^2 (Coefficient of Determination)	Q^2 (Predictive Relevance)
Secure Cloud Adoption (SCA)	0.990	0.981

Source: SmartPLS 4 Output (2025)

4.6 Discussion of Results

The finding that technological security capability exerts a positive but statistically non-significant effect on secure cloud adoption ($\beta = 0.303$, $p = 0.057$) warrants careful contextual interpretation. At face value, this result suggests that possessing technical security controls such as IAM, encryption, incident response systems, and vulnerability auditing capacity does not, by itself, produce secure cloud adoption outcomes in the Kenyan state corporation environment. However, the direction and magnitude of the path coefficient, alongside the strong correlation between TSC and SCA ($r = 0.974$), indicate that a substantive positive relationship exists between these variables, and the non-significance may reflect the conditioning role of other contextual factors rather than the absence of a genuine relationship.

This interpretation is consistent with the findings of Alreemy et al. (2024), who demonstrated that technical security controls are necessary but insufficient for cloud adoption unless complemented by robust governance frameworks and institutional compliance mechanisms. Similarly, Gichubi et al. (2024) found that in the Kenyan context, even where technical tools exist, their inadequate configuration and monitoring reflecting a gap between tool availability and operational security capability leaves cloud environments exposed. This distinction between possessing security tools and demonstrating genuine operational security proficiency is reflected in the mean scores for TSC items in this study, which showed comparatively lower ratings for incident response readiness ($M = 3.911$) than for encryption ($M = 4.277$), suggesting uneven capability across the security control spectrum.

The finding is further contextualised by the theoretical framing of the TOE framework (Tornatzky & Fleischer, 1990). Within the TOE model, the technological context represented here by TSC is one of three co-determining pillars of technology adoption. The framework predicts that the effect of the technological context is shaped and conditioned by the organisational and environmental contexts, meaning that technological capability alone is unlikely to produce adoption outcomes in the absence of supportive organisational structures, adequate infrastructure, and enabling regulatory conditions. The non-significant direct effect of TSC on SCA in this study is consistent with this theoretical expectation, pointing to the importance of examining TSC within a broader multi-factor adoption model rather than as an isolated predictor.

The misperception of the shared responsibility model identified by Chigada and Madzinga (2021) in Kenya's public sector provides additional explanatory context. If state corporation ICT staff and decision-makers believe that cloud service providers bear full security responsibility, the institutional motivation to build and sustain internal technological security capabilities is correspondingly reduced. This dynamic could partially explain why even where technical controls are formally in place, their depth and operational effectiveness may be insufficient to drive secure

adoption outcomes. Zwilling et al. (2022) reached a comparable conclusion in their analysis of developing country contexts, finding that human and governance factors including awareness, training, and institutional accountability tend to condition and moderate the relationship between technical security capability and actual security outcomes.

Taken together, these findings support the conclusion that technological security capability is a necessary, but contextually conditioned, contributor to secure cloud adoption in Kenyan state corporations. The near-significant p-value of 0.057 suggests that with a larger sample or in a more technologically mature institutional environment, the direct effect of TSC on SCA might achieve conventional statistical significance. State corporations seeking to improve their secure cloud adoption outcomes should therefore prioritise not only the acquisition of technical security tools but the development of the operational competencies, governance structures, and institutional cultures needed to deploy and sustain those tools effectively across their cloud environments.

5. SUMMARY OF THE STUDY

This study examined the effect of technological security capability on secure cloud adoption among Kenyan state corporations. A quantitative cross-sectional survey design was employed, with 112 valid responses retained from 150 distributed questionnaires, representing a usable response rate of 74.7%. Data were analysed using descriptive statistics in SPSS Version 29 and PLS-SEM via SmartPLS 4. The TSC construct demonstrated excellent reliability (Cronbach's Alpha = 0.957; Composite Reliability = 0.967) and convergent validity (AVE = 0.854), confirming the robustness of the measurement instrument.

Descriptive analysis revealed that state corporation ICT decision-makers perceived their organisations as having moderate to moderately high levels of technological security capability, with data encryption receiving the highest mean rating (M = 4.277) and cyber incident response readiness receiving the lowest (M = 3.911). The structural model analysis found that TSC had a positive but statistically non-significant effect on secure cloud adoption ($\beta = 0.303$, $t = 1.587$, $p = 0.057$), leading to the non-rejection of the null hypothesis. The integrated model demonstrated exceptional explanatory power, with an R^2 value of 0.990 and a Q^2 value of 0.981. These results collectively indicate that while technological security capability is a meaningful contributor to secure cloud adoption, its direct effect is conditioned by broader institutional and infrastructure factors that must be addressed simultaneously.

6. CONCLUSION

The study concludes that technological security capability is a positive but contextually conditioned determinant of secure cloud adoption among Kenyan state corporations. The possession of technical security controls including identity and access management, encryption,

security monitoring, incident response systems, and vulnerability auditing does not by itself guarantee secure cloud adoption outcomes in the Kenyan public sector context. Rather, the effectiveness of technological security capability is shaped by the broader organisational and infrastructure environment in which it is deployed. State corporations that invest in technical security tools without simultaneously developing the operational proficiency to manage those tools, building the governance structures to ensure accountability, and addressing the infrastructure deficiencies that constrain cloud security operations are likely to fall short of achieving genuine secure adoption outcomes.

The study further concludes that the misperception of the shared cloud security responsibility model, the skills gap in cloud security expertise, and the uneven implementation of security controls across the organisation as evidenced by comparatively lower incident response readiness scores represent the most pressing practical challenges that state corporations must address in order to translate technological security capability into secure adoption outcomes. These challenges cannot be addressed through technical investment alone; they require coordinated action across the technological, organisational, and environmental dimensions of the adoption context.

7. RECOMMENDATIONS

Based on the study findings, the following recommendations are proposed for state corporations, policymakers, and ICT governance practitioners.

First, state corporations should invest in building operational cloud security proficiency rather than merely procuring security tools. The near-significant positive effect of TSC on SCA indicates that technical capability matters, but its translation into secure adoption outcomes requires that staff be trained to configure, monitor, and maintain security controls consistently and effectively. Institutions should establish continuous cloud security training programs and internal certification pathways to build sustainable in-house expertise.

Second, state corporations should formally institutionalize awareness of the shared cloud security responsibility model across all ICT and management staff. Decision-makers and technical staff must clearly understand which security obligations reside with the cloud service provider and which remain the institution's own responsibility. This understanding should be embedded in cloud service procurement contracts, staff onboarding processes, and ongoing governance training.

Third, the Kenya government, through the ICT Authority and the Communications Authority of Kenya, should develop a Kenya-specific cloud security implementation guide that provides state corporations with practical, context-appropriate guidance on deploying and sustaining the technical security controls required for secure cloud adoption. Generic international standards such as ISO/IEC 27001 and NIST provide valuable baselines but do not address the specific regulatory

obligations, infrastructure constraints, and governance realities of the Kenyan public sector. A Kenya-specific framework would significantly reduce the implementation uncertainty that currently limits the effectiveness of technical security investments in state corporations.

8. REFERENCES

Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2024). Critical success factors for cloud computing adoption in higher education institutions: A systematic review. *Future Generation Computer Systems, 153*, 128–147. https://doi.org/10.1016/j.future.2023.11.011

Amini, M., & Jahanbakhsh Imani, M. (2021). A systematic review of cloud computing adoption factors using TOE framework. *International Journal of Information Management, 57*, Article 102290. https://doi.org/10.1016/j.ijinfomgt.2020.102290

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411–423. https://doi.org/10.1037/0033-2909.103.3.411

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50–58. https://doi.org/10.1145/1721654.1721672

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management, 23*(1), Article a1277. https://doi.org/10.4102/sajim.v23i1.1277

Communications Authority of Kenya. (2023). *Annual report 2022/2023: Cybersecurity statistics and trends*. Communications Authority of Kenya. https://www.ca.go.ke/annual-report/

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods, 41*(4), 1149–1160. https://doi.org/10.3758/BRM.41.4.1149

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Gichubi, G., Muriira, G., & Kyalo, D. (2024). Cloud security incidents in Kenyan enterprises: Patterns, vulnerabilities, and mitigation strategies. *Journal of Information Security and Applications, 82*, Article 103723. https://doi.org/10.1016/j.jisa.2024.103723

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2022). When to use and how to report the results of PLS-SEM (2nd ed.). *European Business Review, 31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy, 37*(4–5), 372–386. https://doi.org/10.1016/j.telpol.2012.04.011

Wachanga, A., & Ndiege, J. R. A. (2018, June 26). Adoption of Cloud Computing By Small and Medium Enterprises in Nairobi County, Kenya. ResearchGate;. https://www.researchgate.net/publication/325987790_Adoption_of_Cloud_Computing_By_Small_and_Medium_Enterprises_in_Nairobi_County_Kenya.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information & Management, 51*(5), 497–510. https://doi.org/10.1016/j.im.2014.03.006

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Reece, R., Manley, S., & Brooks, J. (2023). Multi-cloud security risks and mitigation strategies in government environments. *Computers & Security, 128*, Article 103157. https://doi.org/10.1016/j.cose.2023.103157

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.

Zwilling, M., Klien, G., & Lesjak, D. (2022). Cybersecurity awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269