Journal of Business Systems Innovation and Management Science

INFLUENCE OF CLOUD SECURITY MANAGEMENT ON SERVICE DELIVERY IN NAIROBI CITY COUNTY E-SERVICES

Rose Naomi Ong'ayo and **Dr. Godfrey Makau, PhD**

Journal of Business Systems Innovation and Management Science
ISSN: 1849-5419
Vol.3, Issue.No.1, 2026

Influence of Cloud Security Management On Service Delivery in Nairobi City County E-Services

Rose Naomi Ong'ayo

Researcher, Jomo Kenyatta University of Agriculture and Technology

Dr. Godfrey Makau, PhD

Lecturer, Entrepreneurship and Procurement Department, School of Business and Entrepreneurship, Jomo Kenyatta University of Agriculture and Technology

Article History:
***Published on**:* 3/6/2026

DOI:
https://doi.org/10.5281/zenodo.20524062

***How to Cite**:* Ong'ayo, R. N., & Makau, G. (2026). Influence of Cloud Security Management On Service Delivery in Nairobi City County E-Services. *Journal of Business Systems Innovation and Management Science*, 3(1), 1-20. **https://doi.org/10.5281/zenodo.20524062**

Abstract:

Purpose of the Study: This study examined the influence of Cloud Security Management on service delivery in Nairobi City County e-services. Guided by Information Security Theory, the research sought to determine how cloud security practices, particularly confidentiality, integrity, and availability, affect the efficiency, reliability, accessibility, and trustworthiness of public digital services.

Methodology: The study adopted a mixed-methods design combining descriptive and exploratory approaches. A sample of 177 employees was selected from a target population of 316 using Slovin's formula and stratified random sampling. Data were collected through questionnaires and interviews and analyzed using descriptive statistics, correlation, regression, and thematic analysis.

Findings: The study achieved a 91% response rate, with 161 respondents participating. Results indicated that Cloud Security Management positively influenced service delivery, recording an overall mean score of 3.73 (SD = 0.90). Citizen trust (Mean = 4.21) and data protection (Mean = 4.15) emerged as the strongest indicators of effective service delivery. Regression analysis established a statistically significant positive relationship between Cloud Security Management and service delivery performance ($\beta = 0.156$, $t = 2.294$, $p = 0.023$). The findings suggest that stronger cloud security measures enhance operational efficiency, service reliability, data protection, and public confidence in county e-services.

Conclusion: The study concludes that effective Cloud Security Management significantly improves service delivery in Nairobi City County e-services. Strengthening security controls enhances reliability, efficiency, and citizen trust. The study recommends continuous staff training, stronger inter-departmental security coordination, and the adoption of user-friendly security mechanisms that balance accessibility with protection.

Keywords: *Cloud Security Management; E-Service Delivery; Information Security Theory; Nairobi City County.*

1. INTRODUCTION

1.1 Background of the Study

The growing adoption of digital technologies in public administration has fundamentally altered the manner in which governments deliver services to citizens. Across the globe, governments are increasingly leveraging cloud computing to enhance the efficiency, accessibility, and transparency of public services (Alkhasawneh et al., 2025). Cloud computing offers scalable infrastructure, cost efficiency, and real-time data processing capabilities, making it an attractive platform for e-government initiatives. In sub-Saharan Africa, this transformation is gaining momentum, with countries such as Kenya, Rwanda, and South Africa embedding cloud-based systems into their public service frameworks (Sangwa & Mutabazi, 2025).

In Kenya, the national and county governments have made considerable investments in digital infrastructure as part of the broader e-government agenda aligned with Kenya Vision 2030 and the Big Four Agenda. Nairobi City County, as the country's capital and largest urban centre, has deployed cloud-based platforms to support key e-services, including business licensing, land management, health services, and revenue collection (Alkhasawneh et al., 2025). These digital services are intended to reduce bureaucratic delays, minimize physical interaction, and improve service delivery outcomes for approximately four million residents.

However, the deployment of cloud services introduces significant security challenges that, if unaddressed, can undermine service continuity and erode public confidence. Cloud security management encompasses the policies, technologies, and procedures used to protect cloud-hosted data and applications from unauthorized access, breaches, and disruptions (Dawood et al., 2023). In the public sector, where large volumes of sensitive citizen data are processed, the consequences of security failures extend beyond financial losses to include erosion of public trust and breakdown in service delivery (Bodó & Janssen, 2022).

Global evidence indicates that inadequate cloud security remains a persistent challenge. According to the David et al. (2025), nearly 79% of organizations that adopted cloud services experienced at least one security incident within a 12-month period. In developing countries, the risk is compounded by limited cybersecurity expertise, aging infrastructure, and insufficient regulatory frameworks (Avordeh & Boateng, 2026). In the African context, Egwuatu (2025) observed that public sector organizations often lack the financial and technical capacity to implement advanced cloud security protocols, thereby exposing their digital services to significant vulnerabilities.

In Kenya, cybersecurity threats have escalated significantly in recent years, with the Communications Authority of Kenya (2025) reporting over 860 million cyber threat events in 2022, representing a 100% increase from the previous year. These threats disproportionately affect public sector systems, including county-level e-services, where security investment often

lags behind service expansion. Despite these challenges, empirical studies specifically examining the influence of cloud security management on service delivery within Kenyan county governments remain sparse, creating an important knowledge gap that this study seeks to address.

1.2 Statement of the Problem

Nairobi City County has made notable strides in deploying cloud-based e-services to enhance public service delivery. However, the effectiveness of these services is increasingly undermined by security vulnerabilities, inconsistent application of security protocols, and limited staff competence in managing cloud security threats (Sorunke, 2026). Service disruptions attributed to cyber threats, data breaches, and unauthorized access have been reported across various county departments, raising concerns about the reliability and trustworthiness of the digital service infrastructure (Communications Authority of Kenya, 2025).

While studies such as Tanaka and Yamamoto (2021) and Zhang et al. (2022) have examined cloud security in the context of e-government services in Japan and China, respectively, these findings are limited in their applicability to the Kenyan context due to differences in institutional capacity, regulatory frameworks, and digital literacy levels. Similarly, Rupra (2020) provide preliminary insights into cloud security within Nairobi County, but their study did not employ inferential statistics to establish the directional and predictive relationship between cloud security management and specific service delivery outcomes.

The absence of a robust empirical framework linking cloud security management to e-service delivery performance in Nairobi City County means that policymakers and county administrators lack an evidence base to guide investment in security infrastructure. This study therefore sought to fill this gap by empirically examining the influence of Cloud Security Management on service delivery in Nairobi City County e-services.

1.3 Purpose of the Study

The purpose of this study was to determine the influence of Cloud Security Management on service delivery of e-services in Nairobi City County.

1.4 Research Hypothesis

H01: Cloud Security Management does not significantly influence service delivery in Nairobi City County e-services.

2. LITERATURE REVIEW

2.1 Theoretical Framework: Information Security Theory

This study was grounded in the Information Security Theory (IST), originally developed by Dhillon and Backhouse (2001) and further elaborated by Hina and Dominic (2020) as a comprehensive framework for managing information security risks in digital environments. The theory addresses both the technical and socio-organizational dimensions of information security, making it especially relevant for analyzing cloud security management in the public sector.

IST is built on three foundational principles, commonly referred to as the CIA triad: Confidentiality, Integrity, and Availability. Confidentiality ensures that information is accessible only to authorized users, thereby preventing unauthorized access to sensitive citizen data. Integrity guarantees the accuracy and completeness of data by safeguarding it against unauthorized modification. Availability ensures that digital services and the data they rely upon remain accessible when needed, thereby supporting uninterrupted service delivery (Ahmed & Ahmed, 2023). These principles align directly with the operational requirements of Nairobi City County's cloud-based e-services, where secure and consistent access to citizen data is fundamental to service quality.

Bwiino et al. (2026) emphasize that IST advocates for a dual approach to information security, integrating technical controls such as encryption, firewalls, intrusion detection systems, and multi-factor authentication alongside organizational measures including user training, access control policies, and compliance audits. In the context of Nairobi City County, this dual approach is particularly relevant, as the effectiveness of cloud security depends not only on the robustness of technical systems but also on the security awareness and compliance of county employees who interact with these systems daily.

A strength of the Information Security Theory in this context is its holistic orientation, which acknowledges that security threats can arise from both external cyberattacks and internal organizational vulnerabilities (Almindeel & Martins, 2021). This perspective is supported by Ali et al. (2024), who argue that information security is a dynamic and continuous process requiring regular assessments and adaptive responses to emerging threats. This is consistent with the nature of cloud computing environments, where new vulnerabilities continuously emerge as technology evolves.

Despite its relevance, IST has certain limitations when applied to public sector organizations in low-resource environments. Blouin et al. (2025) note that the theory's prescriptions can be resource-intensive, requiring sustained financial and technical investment that may be difficult for county-level governments to maintain. Furthermore, IST's focus on risk management and technical compliance may not fully address the behavioral dimensions of security, such as user resistance to security protocols or the cultural norms that influence compliance (Nurse et al., 2025). Acknowledging these limitations, this study integrates IST as the primary theoretical

lens while contextualizing its application within the institutional realities of Nairobi City County.

2.2 Empirical Review

2.2.1 Cloud Security Management

Satpathy et al. (2024) examined the effect of cloud security on the efficiency of e-government services in India, employing a quantitative survey design among 200 government employees. Their regression analysis found that robust cloud security, particularly measures ensuring data confidentiality and integrity, significantly improved service delivery by reducing breaches and minimizing service delays. The study highlighted, however, that employee awareness of cloud security protocols remained insufficient, suggesting that technical measures alone are inadequate without complementary training programs.

Ito (2024) explored the role of cloud security in Japan's public sector using a mixed-methods approach combining qualitative interviews with 15 IT managers and quantitative surveys with 200 government employees. Their factor analysis revealed that encryption, multi-factor authentication, and secure access protocols were pivotal in improving e-service efficiency and reliability. The study noted a gap in user-centric security solutions and recommended future research on end-user security experiences, particularly concerning phishing and data leakage risks.

Feyisa (2025) conducted a case study in China, interviewing 20 municipal government officials overseeing cloud adoption. Thematic analysis revealed that strong access controls and secure data transmission enhanced the responsiveness of government e-services. However, the study found that legacy IT infrastructure and poor inter-departmental coordination impeded the effective implementation of security measures. The researchers called for a comprehensive evaluation framework tailored to public sector cloud security implementation.

In the African context, David et al. (2026) investigated cloud security's influence on public e-service quality in Nigeria through qualitative interviews with 12 IT managers and cybersecurity specialists. Their thematic findings confirmed that regular vulnerability assessments and secure data storage were critical to service quality. However, implementation was hampered by the scarcity of skilled cybersecurity personnel and insufficient government funding, identifying scalability and workforce development as priority areas for future research.

Mwongera and Nyambega (2026) assessed the effect of cloud security on e-government service delivery in Nairobi County using a survey of 200 employees, analyzed through descriptive statistics and correlation analysis. The study found positive correlations between encryption, multi-factor authentication, and service delivery efficiency. However, the study identified gaps in security policy integration across departments and recommended further investigation into

the relationship between cloud security and public trust in digital services. The present study builds on these findings by employing regression analysis to establish predictive relationships and by incorporating qualitative data to enrich the empirical evidence.

2.2.2 Service Delivery in the Context of Cloud-Based E-Services

Service delivery in cloud-computing environments is broadly understood as the capacity of digital platforms to provide consistent, accessible, and responsive services that meet user expectations (Qazi et al., 2024). Nyachiro et al. (2023) identify four key dimensions of e-service delivery: efficiency, accessibility, user satisfaction, and accountability. Efficiency relates to the speed and reliability of service processing, while accessibility concerns the ease with which citizens can interact with digital services regardless of their location or device. User satisfaction captures the subjective assessment of service quality, and accountability involves transparency in how services are managed and delivered.

In the public sector, service delivery quality is closely tied to citizens' perceptions of security and trustworthiness. Pham et al. (2023) found that citizens' willingness to use digital government services was significantly influenced by their confidence in data protection and system reliability. Axelsson and Eriksson (2022) further demonstrated that positive customer experiences in digital service environments are strongly correlated with the perceived security of the platform. These findings collectively underscore the centrality of cloud security management to service delivery performance in e-government contexts.

Ahmed and Ahmed (2023) established that citizen adoption of e-government services is shaped by perceived ease of use, usefulness, and trust in the security of digital transactions. Building on this, Ali et al. (2024) found that citizens who perceive government digital services as secure are significantly more likely to engage with and derive satisfaction from those services. This body of evidence supports the theoretical contention that cloud security management is not merely a technical concern but a direct determinant of e-service delivery outcomes.

2.3 Conceptual Framework

The conceptual framework of this study positions Cloud Security Management as the independent variable and Service Delivery of e-Services as the dependent variable. Cloud Security Management is operationalized through the following dimensions: data encryption and access controls, multi-factor authentication, employee training on security protocols, frequency of security updates, and management of security breaches. Service delivery is assessed across the dimensions of service accessibility, processing speed, reliability, citizen satisfaction, and feedback mechanisms.

The framework is informed by the Information Security Theory, which posits that effective management of information security—through the integration of technical controls and

organizational policies—leads to improved confidentiality, integrity, and availability of digital systems. These security outcomes, in turn, support consistent and trustworthy service delivery. The conceptual framework therefore anticipates a positive and significant relationship between Cloud Security Management and e-service delivery performance in Nairobi City County.

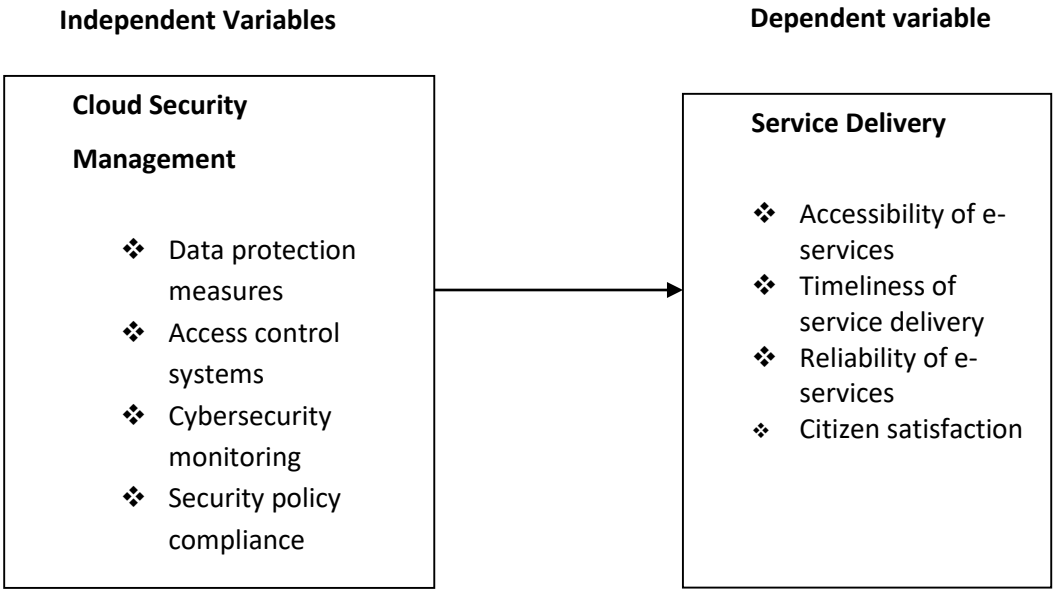

Figure 1: Conceptual Framework

3. RESEARCH METHODOLOGY

This study adopted a mixed-methods research design incorporating descriptive and exploratory approaches to examine the influence of Cloud Security Management on service delivery in Nairobi City County e-services. The mixed-methods design enabled the researcher to capture both the statistical patterns in cloud security and service delivery data and the contextual insights necessary for a nuanced interpretation of findings (Creswell & Creswell, 2022).

The target population comprised 316 employees from three strategic departments of Nairobi City County: the Department of Public Service Management, the Department of Information, Communication and E-Government, and the Department of Water, Energy, Forestry and

Natural Resources. These departments were selected based on their central roles in the deployment and management of cloud-based e-services. A sample size of 177 respondents was determined using Slovin's formula and selected through stratified random sampling to ensure proportional representation across all departments.

Data were collected through structured questionnaires and semi-structured interviews. The questionnaires gathered quantitative data on cloud security management practices and service delivery outcomes, while the interviews provided qualitative insights into implementation experiences, challenges, and perceptions of county employees. A pilot study involving 18 respondents from Machakos County was conducted to test the suitability and reliability of the research instruments prior to the main data collection exercise.

Validity of the instruments was established through expert review by senior academics and practitioners in information systems and public administration, supplemented by exploratory factor analysis to confirm construct validity. Reliability was assessed using Cronbach's Alpha coefficient, with all constructs yielding coefficients above the accepted threshold of 0.70. Quantitative data were analyzed using descriptive statistics, Pearson correlation, and multiple regression with the Statistical Package for Social Sciences (SPSS) version 25. Qualitative data were analyzed thematically, following Braun and Clarke's (2021) six-phase framework. Findings were presented using tables and narrative explanations. All ethical requirements regarding participant confidentiality, informed consent, and voluntary participation were strictly observed throughout the research process.

4. RESEARCH FINDINGS AND DISCUSSION

4.1 Response Rate

The study targeted 177 respondents from three strategic Nairobi City County departments involved in cloud-based service delivery and management. The response rate analysis is presented in Table 4.1 below.

Table 4.1: Response Rate

Category	Frequency	Percentage
Responded	161	91%
Not Responded	16	9%
Total	**177**	**100%**

Source: Researcher (2025)

The study achieved an overall response rate of 91.0%, with 161 out of 177 targeted respondents participating. This exceptional response rate demonstrates strong stakeholder engagement and

interest in cloud resource management initiatives within Nairobi City County. A response rate above 70% is considered excellent for statistical analysis, while Babbie (2010) suggests that response rates above 85% significantly reduce non-response bias and enhance the generalizability of findings. The 91.0% response rate therefore provides confidence that the findings accurately reflect the perspectives of county personnel involved in cloud-based service delivery.

4.2 Descriptive Findings: Cloud Security Management on Service Delivery Efficiency

The study examined the influence of Cloud Security Management on service delivery efficiency in Nairobi City County e-services. The findings are presented in Table 4.9 below.

Table 4.9: Cloud Security Management on Service Delivery Efficiency

Statement	N	Mean	Std Dev
The implementation of strong Cloud Security Management has enhanced the reliability of e-government services in Nairobi City County.	161	3.99	0.88
Cloud security practices have helped reduce the frequency of service disruptions in Nairobi City County e-Services.	161	3.83	1.01
Cloud Security Management has contributed to better protection of sensitive citizen data in Nairobi City County e-Services.	161	4.15	0.79
Security breaches in cloud services have led to delays in the provision of e-government services in Nairobi City County.	161	2.11	1.06
Employee training on cloud security protocols has positively impacted the delivery of e-services in Nairobi City County.	161	3.99	0.87
Cloud Security Management measures are regularly updated in Nairobi City County e-Services to mitigate emerging cyber threats.	161	3.86	0.96
The level of cloud security directly influences the trust that citizens have in Nairobi City County e-Services.	161	4.21	0.76
Overall Mean		**3.73**	**0.90**

Source: Researcher (2025)

The analysis demonstrates strong recognition that Cloud Security Management significantly influences service delivery efficiency, with an overall mean of 3.73 (SD = 0.90), indicating that respondents generally agreed with the statements presented. Respondents most strongly agreed that security influences citizen trust (Mean = 4.21, SD = 0.76) and ensures better protection of sensitive citizen data (Mean = 4.15, SD = 0.79). These findings align with David et al. (2025), who found that enhanced cloud security measures, including encryption and multi-factor authentication, were positively correlated with improved efficiency and reliability in e-service delivery. The strong positive ratings on trust and data protection further support Zaini et al. (2020), who established that citizens' trust in digital government platforms is fundamentally shaped by their perceptions of data security.

The reverse-coded statement regarding security breaches causing service delays yielded a notably low mean of 2.11 (SD = 1.06), indicating strong disagreement. This suggests that current cloud security interventions within Nairobi City County are largely effective in preventing disruptions rather than causing them—a finding that contradicts the common assumption that stringent security measures introduce friction into service processes. This observation is consistent with David et al. (2026) finding that well-implemented security protocols, including multi-factor authentication and access controls, streamline rather than impede e-service operations.

Employee training on cloud security protocols received strong endorsement (Mean = 3.99, SD = 0.87), underscoring the importance of human capital in effective security management. Dawood et al. (2023) similarly emphasized that technical measures alone are insufficient without corresponding investment in staff awareness and competency. Regular security updates also achieved moderate agreement (Mean = 3.86, SD = 0.96), indicating an established but improvable security update culture within the county's ICT departments. The consistency of these findings across quantitative indicators provides robust support for the Information Security Theory's assertion that combining technical controls with organizational policy yields improved security outcomes.

4.3 Qualitative Findings on Cloud Security Management

Security emerged as a central concern across all interviews conducted with ICT managers, department heads, and cloud implementation team leaders. One ICT Manager emphasized the strategic importance of security beyond mere technical configuration, stating that robust security protocols had effectively eliminated the need for manual verification processes, enabling citizens to complete digital transactions with confidence. This qualitative insight reinforces the quantitative finding that cloud security positively influences service efficiency and citizen trust.

Training and capacity building received prominent attention during interviews. A Cloud Implementation Team Leader explained that heightened staff security awareness had fundamentally changed the service delivery culture within the department, with employees recognizing that adherence to security protocols is essential for both citizen protection and operational continuity. However, challenges in balancing security stringency with citizen accessibility also emerged. Respondents highlighted the need to develop user-friendly security interfaces that maintain rigorous protection while remaining accessible to citizens with limited digital literacy a challenge that aligns with Egwuatu (2025) findings on the tension between security robustness and usability in public sector digital services.

4.4 Descriptive Findings: Service Delivery Performance

The study assessed overall service delivery performance in Nairobi City County e-services as the dependent variable. The findings are presented in Table 4.12 below.

Table 4.12: Service Delivery Performance in Nairobi City County e-Services

Statement	N	Mean	Std Dev
The e-services provided by Nairobi City County are always easily accessible to citizens.	161	3.91	0.93
Citizens are satisfied with the responsiveness of Nairobi City County e-Services when they request information or assistance.	161	3.82	0.99
The time it takes to process citizen requests through e-services in Nairobi City County is reasonable.	161	3.97	0.88
The reliability of Nairobi City County e-Services is consistent, with minimal service interruptions.	161	3.77	1.03
Citizens have experienced an improvement in their overall experience with the Nairobi City County e-Services in the past year.	161	3.93	0.91
The Nairobi City County e-Services meet the diverse needs of its citizens, providing services across various sectors.	161	3.76	1.01
There is a sufficient feedback mechanism to assess and improve the quality of e-services provided by Nairobi City County.	161	3.62	1.06
Overall Mean		**3.83**	**0.97**

Source: Researcher (2025)

The findings indicate positive service delivery performance with an overall mean of 3.83 (SD = 0.97), reflecting general agreement that Nairobi City County's e-services perform adequately across the dimensions assessed. Respondents most strongly agreed on reasonable processing times for citizen requests (Mean = 3.97, SD = 0.88) and improvement in overall citizen experience in the past year (Mean = 3.93, SD = 0.91). Service accessibility also received strong endorsement (Mean = 3.91, SD = 0.93), indicating successful implementation of cloud-based infrastructure improvements. These findings are consistent with Feyisa (2025), who established that perceived service quality and accessibility are primary determinants of citizen satisfaction with e-government platforms.

However, the feedback mechanism dimension received the lowest rating (Mean = 3.62, SD = 1.06), indicating that mechanisms for capturing and acting on citizen input require strengthening. This finding resonates with the qualitative evidence gathered in this study, wherein respondents acknowledged that while significant progress had been achieved in service processing and accessibility, systematic feedback collection and analysis remained underdeveloped. Service reliability also achieved a moderate rating (Mean = 3.77, SD = 1.03), suggesting that while the county's cloud infrastructure maintains general stability, there is room for further improvement in minimizing service interruptions.

4.5 Qualitative Findings on Service Delivery Performance

Interview respondents consistently highlighted significant improvements in the pace and accessibility of e-service delivery. One ICT Manager described the transformation as remarkable, noting that processing times that previously extended over several weeks had been reduced to a matter of hours following the deployment of cloud-based systems. Department heads emphasized improvements in citizen satisfaction attributed to reduced waiting times and the availability of multiple digital access channels.

Notwithstanding these advances, respondents identified feedback collection and service improvement processes as areas requiring urgent attention. A Cloud Implementation Team Leader acknowledged that while performance gains had been substantial, the county lacked sophisticated mechanisms to systematically capture citizen feedback and translate it into actionable service improvements. The need for continuous enhancement of service delivery systems was a recurring theme, aligning with Ito (2024) assertion that customer experience management must be iterative and data-driven to remain responsive to evolving citizen needs.

4.6 Inferential Statistics

4.6.1 Regression Model Summary

Inferential statistics were employed to determine the predictive relationship between Cloud Security Management and service delivery performance in Nairobi City County. The regression model summary is presented in Table 4.13 below.

Table 4.13: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of Estimate
1	.651a	.577	.502	.50370

a. Predictors: (Constant), Cloud Security Management

The model summary indicates a correlation coefficient of R = 0.651, reflecting a moderate to strong positive relationship between Cloud Security Management and service delivery performance. The coefficient of determination (R^2 = 0.577) indicates that Cloud Security Management explains 57.7% of the variation in service delivery performance within Nairobi City County e-services. The adjusted R^2 of 0.502 confirms that the model maintains reasonable explanatory power after accounting for the number of predictors. The standard error of estimate of 0.504 indicates that predictions made by the model are relatively precise. These results suggest that Cloud Security Management is a substantively important predictor of service delivery outcomes, consistent with the theoretical expectations of the Information Security Theory.

4.6.2 ANOVA Results

Table 4.14: ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	24.899	4	14.006	58.653	.000b
Residual	69.564	156	.254		
Total	**94.463**	**160**			

a. Dependent Variable: Service Delivery Performance b. Predictors: (Constant), Cloud Security Management

The ANOVA results confirm that the overall regression model is statistically significant (F = 58.653, p < 0.001). This indicates that Cloud Security Management has a significant effect on service delivery performance in Nairobi City County e-services and that the regression model provides a statistically valid fit to the data. These results support the rejection of the null hypothesis that Cloud Security Management does not significantly influence service delivery in Nairobi City County e-services.

4.6.3 Regression Coefficients

Table 4.15: Beta Coefficients for Cloud Security Management

Model	B	Std. Error	Beta	t	Sig.
(Constant)	0.421	0.186		2.263	0.025
Cloud Security Management	0.156	0.068	0.152	2.294	0.023

a. Dependent Variable: Service Delivery Performance

The regression coefficients in Table 4.15 indicate that Cloud Security Management is a statistically significant predictor of service delivery performance ($B = 0.156$, $\beta = 0.152$, $t = 2.294$, $p = 0.023$). This means that a one-unit increase in the quality of Cloud Security Management is associated with a 0.156-unit improvement in service delivery performance. The statistical significance of this relationship ($p = 0.023 < 0.05$) confirms that the effect is not attributable to chance and is consistent across the sample. These findings are consistent with those of Mwongera and Nyambega (2026), who demonstrated positive correlations between cloud security measures and service delivery efficiency in Nairobi County. Similarly, Singh and Nyachiro et al. (2023) found that robust cloud security practices significantly enhanced service responsiveness in Indian e-government settings.

The positive and significant beta coefficient further validates the Information Security Theory's contention that maintaining the availability, confidentiality, and integrity of cloud-hosted information systems directly supports service delivery quality. The finding that a unit improvement in cloud security yields a measurable improvement in service performance provides a compelling evidence base for county policymakers to prioritize investment in cloud security infrastructure.

5. SUMMARY OF THE STUDY

The study examined the influence of Cloud Security Management on service delivery in Nairobi City County e-services. The analysis was guided by the Information Security Theory, which postulates that the confidentiality, integrity, and availability of digital systems are fundamental prerequisites for effective service delivery. The study targeted 316 employees across three county departments, achieving a response rate of 91% from a stratified sample of 177 respondents.

Descriptive findings revealed that Cloud Security Management practices within Nairobi City County are broadly perceived as effective contributors to service delivery quality, particularly in building citizen trust and safeguarding sensitive data. The overall mean score for Cloud Security Management indicators was 3.73 (SD = 0.90), while service delivery performance

achieved a mean of 3.83 (SD = 0.97), reflecting positive perceptions across both constructs. Strong agreement was observed on the role of security in citizen trust (Mean = 4.21), data protection (Mean = 4.15), and employee training (Mean = 3.99). Feedback mechanisms emerged as the weakest dimension of service delivery, suggesting a need for systematic improvements in citizen engagement processes.

Inferential analysis confirmed that Cloud Security Management is a statistically significant predictor of service delivery performance ($\beta = 0.156$, $t = 2.294$, $p = 0.023$), with the regression model explaining 57.7% of the variance in service delivery outcomes ($R^2 = 0.577$). The ANOVA results further validated the overall model fit ($F = 58.653$, $p < 0.001$). These findings collectively support the rejection of the null hypothesis and affirm the centrality of cloud security management to e-service delivery quality in Nairobi City County.

6. CONCLUSIONS

The study concludes that Cloud Security Management exerts a significant and positive influence on service delivery in Nairobi City County e-services. The empirical evidence demonstrates that county departments that invest in comprehensive cloud security practices including data encryption, multi-factor authentication, regular security updates, and staff training achieve measurably better service delivery outcomes in terms of efficiency, reliability, and citizen trust. The significant positive relationship between Cloud Security Management and service delivery performance ($\beta = 0.156$, $p = 0.023$) confirms that security investment in cloud infrastructure is not merely a technical necessity but a strategic driver of public service quality.

The findings further reveal that while Nairobi City County has made commendable progress in deploying cloud-based e-services, significant opportunities remain for strengthening security policy integration across departments, improving the user-friendliness of security interfaces, and developing more robust feedback mechanisms to enable continuous service improvement. The lowest-rated service delivery dimension—feedback mechanisms—indicates a structural gap in the county's approach to citizen-responsive governance that, if addressed, could significantly enhance overall service delivery performance.

The Information Security Theory's emphasis on combining technical controls with organizational policies is validated by both the quantitative and qualitative findings of this study. In Nairobi City County, the effectiveness of cloud security depends equally on the robustness of technical measures and the security awareness and compliance culture among county employees. This dual dimension of security management must be sustained and strengthened to support the long-term success of the county's e-government agenda.

7. RECOMMENDATIONS

Based on the findings of this study, the following recommendations are proposed for Nairobi City County and similar county government administrations in Kenya:

Nairobi City County should establish a dedicated cloud security governance framework with clearly defined policies, roles, and responsibilities for all departments involved in e-service delivery. This framework should incorporate standardized security protocols, regular compliance audits, and inter-departmental coordination mechanisms to ensure uniform application of security measures across all service units. Clear accountability structures will reduce the fragmentation currently observed in the implementation of cloud security policies.

The county government should invest continuously in staff training and capacity building on cloud security protocols. Training programs should be tailored to different employee roles, covering both technical security procedures for ICT staff and awareness-raising for frontline employees who interact with cloud-based systems. Partnerships with academic institutions, cybersecurity firms, and national agencies such as the National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC) can be leveraged to deliver high-quality, cost-effective training at scale.

Given the low rating of feedback mechanisms in the service delivery assessment, the county should develop systematic and accessible channels for capturing citizen feedback on e-service experiences. This could include in-app surveys, automated service rating systems, and periodic citizen satisfaction assessments. Data gathered through these channels should be regularly analyzed and used to inform iterative improvements to cloud security and service delivery processes, creating a citizen-centered cycle of continuous improvement.

The county should adopt user-friendly security interfaces that balance rigorous protection with ease of access, particularly for citizens with limited digital literacy. This requires deliberate investment in user experience design for security features such as authentication processes and data consent mechanisms. Usability testing involving diverse citizen groups can help identify and eliminate barriers that may discourage citizens from engaging with digital services, thereby improving service utilization and overall delivery performance.

8. AREAS FOR FURTHER RESEARCH

The findings of this study open several avenues for further scholarly investigation. Future research should consider longitudinal studies that track the long-term impact of cloud security investments on e-service delivery outcomes within Nairobi City County and other Kenyan county governments. Such studies would provide insights into the sustainability and trajectory of security-driven service improvements over time. Comparative studies examining cloud security management practices across multiple county governments in Kenya would enhance understanding of the contextual factors that moderate the relationship between security

management and service delivery performance. Additionally, future research should explore the role of citizen digital literacy as a moderating variable between cloud security perceptions and e-service adoption, given the growing diversity of digital users in urban Kenya. Studies employing experimental or quasi-experimental designs could also provide stronger causal evidence for the effects identified in this cross-sectional study.

9. REFERENCES

Ahmed, M. M., & Ahmed, A. M. (2023). Citizens' Data Protection in E-government System. *International Journal of Innovative Computing*, *13*(2), 1–9. https://doi.org/10.11113/ijic.v13n2.389

Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2024). Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. *The Journal of Computer Information Systems*, 1–28. https://doi.org/10.1080/08874417.2024.2329985

Alkhasawneh, R., Cob, Z. C., & Latif, A. B. A. (2025). Cloud Computing Adoption in Government Organizations in Developing Countries. *International Journal of Public Administration in the Digital Age*, *12*(1), 1–27. https://doi.org/10.4018/ijpada.368246

Anguche, C., Kimani, H., & Ndururi, J. (2024). E-Government Services and Performance of County Governments in Kenya: The Case of Nairobi City County. *European Journal of Business and Strategic Management*, *9*(3), 1–30. https://doi.org/10.47604/ejbsm.2796

Avordeh, T. K., & Boateng, D. (2026). Identifying and mitigating cybersecurity risks in residential demand response for smart grids in Sub-Saharan Africa. *Utilities Policy*, *101*, 102223. https://doi.org/10.1016/j.jup.2026.102223

Axelsson, M., & Eriksson, O. (2022). *CUSTOMER EXPERIENCE MANAGEMENT IN SOCIAL MEDIA an Empirical Study of How Swedish E-commerce Companies Work with Customer Experience Management in Social Media*. https://www.diva-portal.org/smash/get/diva2:1680497/FULLTEXT01.pdf

Blouin, D., Bissonnette, J.-F., Goyette, J.-O., Cimon-Morin, J., Mendes, P., Torchio, G. M., Gosselin-Tapp, J., & Poulin, M. (2025). Ecosystem services concept: Challenges to its integration in government organizations. *Ecosystem Services*, *71*, 101691. https://doi.org/10.1016/j.ecoser.2024.101691

Bodó, B., & Janssen, H. (2022). Maintaining trust in a technologized public sector. *Policy and Society*, *41*(3), 414–429. https://doi.org/10.1093/polsoc/puac019

Bwiino, K., Mayoka, G. K., Nkamwesiga, L., & Nyamadi, M. (2026). A Systematic Literature Review of Information Security Practices in Higher Education Contexts. *IET Information Security*, *2026*(1). https://doi.org/10.1049/ise2/6324508

Communication Authority of Kenya. (2025). *Cybersecurity Report*.

https://www.ca.go.ke/sites/default/files/2025-10/Cyber%20Security%20Report%20Q1%202025-2026.pdf

Creswell, & Creswell. (2022). *Creswell, J. W., & Creswell, J. D. (2022). Research Design Qualitative, Quantitative, and Mixed Methods Approach. SAGE Publication. - References - Scientific Research Publishing*. Scirp.org. https://www.scirp.org/reference/referencespapers?referenceid=3692984

David, O., Vallabhaneni, R., Harjinder Lallie, Guglielmo, M., & Caporale. (2025, July 5). *Cloud Computing and Cybersecurity: Emerging Threats and Defense Mechanisms*. https://www.researchgate.net/publication/393434987_Cloud_Computing_and_Cybersecurity_Emerging_Threats_and_Defense_Mechanisms

David, S., Offia Anthonia Chioma, & Ekwunife Ebele. (2026). *Cyber Security Threats and Fraud Detection: A Study of Selected Banks in Nigeria*. *11*(11), 2695–2211. https://doi.org/10.56201/jafm.vol.11.no11.2025.pg269.290

Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and Security of Cloud Computing: A Complete Guideline. *Symmetry*, *15*(11), 1–33. mdpi. https://doi.org/10.3390/sym15111981

Egwuatu, O. V. (2025). Cybersecurity Readiness in Developing Countries' Enterprises: A Comparative Multi-Case Analysis. *Magna Scientia Advanced Research and Reviews*, *15*(1), 068–083. https://doi.org/10.30574/msarr.2025.15.1.0110

Feyisa, K. (2025). AI Adoption and Implementation in China's Public Sector: Factors, challenges, and Case Study Insights. *Academic Journal of Politics and Public Administration*, *2*(3). https://doi.org/10.19080/acjpp.2025.02.555586

Ito, S. (2024). Role of Technological Advancements on Customer Satisfaction in Japan's Hospitality. *International Journal of Modern Hospitality and Tourism*, *4*(3), 1–15. https://doi.org/10.47604/ijmht.3062

Mwongera, F., & Nyambega, S. (2026). Effects of Digital Transformation on Public Service Delivery in Nairobi County, Kenya. *International Journal of Innovative Research and Development*. https://doi.org/10.24940/ijird/2025/v14/i12/dec25008

Nurse, J. R. C., Milward, J., & Alashe, O. (2025). From Security Awareness and Training to Human Risk Management in Cybersecurity. *Lecture Notes in Computer Science*, 86–104. https://doi.org/10.1007/978-3-031-92833-8_6

Nyachiro, A., Ondimu, K., & Mafura, G. (2023). Adoption Strategy for Cloud Computing in Research Institutions: A Structured Literature Review. *Journal of Computer and Communications*, *11*(4), 63–78. https://doi.org/10.4236/jcc.2023.114004

Pham, L., Limbu, Y. B., Le, M. T. T., & Nguyen, N. L. (2023). E-government service quality, perceived value, satisfaction, and loyalty: Evidence from a newly emerging country. *Journal of Public Policy*, *43*(4), 812–833. https://doi.org/10.1017/S0143814X23000296

Qazi, F., Kwak, D., Fiaz Gul Khan, Ali, F., & Sami Ullah Khan. (2024). Service Level Agreement in cloud computing: Taxonomy, prospects, and challenges. *Internet of Things (Amsterdam. Online)*, 101126–101126. https://doi.org/10.1016/j.iot.2024.101126

Rupra, Dr. S. S. (2020). A Descriptive Research on the Security Challenges of Cloud Computing Among Selected SMEs in Kenya. *Volume 5 - 2020, Issue 9 - September*, *5*(9), 588–598. https://doi.org/10.38124/ijisrt20sep231

Sangwa, S., & Mutabazi, P. (2025, August 2). *Assessing the Effectiveness of E-Governance in Public Service Delivery: A Comparative Study of Digitization Efforts in Rwanda, Kenya, and Ghana*. https://doi.org/10.5281/zenodo.16723425

Satpathy, A. S., Sahoo, S. K., Mohanty, A., & Mohanty, P. P. (2024). Strategies for enhancements of MSME resilience and sustainability in the post-COVID-19 era. *Social Sciences & Humanities Open*, *11*, 101223. https://doi.org/10.1016/j.ssaho.2024.101223

Sorunke, O. (2026, February 22). *EMERGING CYBER THREATS AND CLOUD SECURITY: AN EMPIRICAL INVESTIGATION*. https://doi.org/10.56726/IRJMETS89197