

CLOUD COMPUTING ADOPTION AND FINANCIAL REPORTING INTEGRITY IN NIGERIA: THE MODERATING ROLE OF DATA SECURITY AND INTERNAL CONTROLS

Dr. Nelson Ogoja Willy and Ziniye Preye Etebu

Department of Accountancy, School of Management Sciences, Federal Polytechnic Ekowe, Bayelsa State. Nigeria.

Email: nelsonwilly79@gmail.com and ziniyeprey@gmail.com

Abstract

The study examined cloud computing adoption and financial reporting integrity in financial institutions in Nigeria, with emphasis on the moderating role of data security and internal controls. A descriptive survey research design was adopted to obtain quantitative data from selected financial institutions. The population comprised accounting, audit, and information technology personnel, from which a representative sample was selected using stratified sampling techniques. Data were collected through a structured questionnaire designed to measure cloud adoption, data security practices, internal control systems, and financial reporting integrity. Descriptive statistics and multiple regression analysis were employed to analyze the data and test the hypotheses. Findings revealed that cloud computing adoption significantly improves financial reporting integrity by enhancing accuracy, timeliness and accessibility of financial information. The results further indicated that data security and internal controls significantly moderate the relationship, strengthening the positive effects of cloud adoption on reporting outcomes. Institutions with strong security and control systems recorded higher levels of reporting reliability and compliance. The study concluded that cloud computing adoption contributes to improved financial reporting integrity when supported by effective data security and internal control frameworks. Recommendations emphasised the need for enhanced security systems, regulatory compliance, interdepartmental collaboration and staff training to optimise the benefits of cloud technologies in financial reporting.

Keywords: Concepts of Cloud Computing, Data Security, Internal Controls, Cloud Computing Adoption and Financial Reporting Integrity.

Introduction

Rapid digital transformation within financial institutions has intensified the demand for scalable, efficient, and reliable information systems capable of supporting high-quality financial reporting. Cloud computing has emerged as a strategic technological innovation that enables organisations to access shared computing resources, enhance data processing capabilities, and reduce infrastructural costs. According to Mell and Grance (2021), cloud computing provides on-demand network access to a shared pool of configurable computing resources, thereby improving operational flexibility. Financial institutions in Nigeria have increasingly embraced cloud-based solutions to streamline accounting processes, enhance data storage efficiency, and improve the timeliness of financial disclosures. Empirical evidence indicates that cloud adoption significantly influences organisational transparency and reporting accuracy by facilitating real-time data access and integrated financial systems (Alharthi, Krotov & Bowman, 2022). Financial reporting integrity remains a critical concern in the Nigerian financial sector due to persistent issues such as earnings manipulation, delayed reporting, and inconsistencies in financial disclosures. Integrity in financial reporting refers to the extent to which financial statements are complete, accurate, and free from material misstatements. Studies have shown

that technological innovations, particularly cloud-based systems, can strengthen reporting integrity by automating accounting processes and reducing human intervention (Wang, Kung & Byrd, 2023). However, the effectiveness of cloud computing in enhancing reporting integrity is contingent upon complementary organisational mechanisms, including robust data security frameworks and effective internal control systems. Data security plays a pivotal role in ensuring that financial information stored and processed in cloud environments remains protected from unauthorised access, cyber threats, and data breaches. According to Hashizume et al. (2013), vulnerabilities in cloud infrastructure can expose organisations to significant risks, thereby undermining the credibility of financial information. In the Nigerian context, where cybercrime and data breaches are increasing, the adequacy of data security measures becomes crucial in determining the success of cloud adoption in financial reporting processes. Evidence suggests that institutions with advanced encryption protocols, access control mechanisms, and continuous monitoring systems are more likely to maintain the integrity of financial data (Ali, Khan & Vasilakos, 2015). Internal controls constitute another critical moderating factor influencing the relationship between cloud computing adoption and financial reporting integrity. Internal control systems encompass policies and procedures designed to ensure the reliability of financial reporting, compliance with regulations, and safeguarding of assets. The Committee of Sponsoring Organisations of the Treadway Commission (COSO) framework highlights the importance of control environment, risk assessment, control activities, information systems, and monitoring in achieving organisational objectives (COSO, 2005). Empirical findings reveal that strong internal controls enhance the effectiveness of technological systems by ensuring proper data validation, audit trails, and accountability mechanisms (Appiah & Agyemang, 2020). Despite the growing adoption of cloud computing in Nigerian financial institutions, the interaction between cloud technologies, data security, and internal controls in shaping financial reporting integrity remains underexplored. Prior studies have largely examined cloud computing from a technological or operational perspective without adequately addressing its implications for financial reporting quality.

Statement of the Problem

Increasing reliance on cloud computing by financial institutions has introduced complexities in maintaining the integrity of financial reporting. While cloud-based systems enhance efficiency and accessibility, concerns persist regarding data accuracy, confidentiality, and reliability within outsourced digital environments. Weak security architectures, inadequate encryption mechanisms, and exposure to cyber threats contribute to vulnerabilities that may compromise financial data, thereby affecting stakeholders' confidence in reported information. Persistent deficiencies in internal control systems further exacerbate these challenges, particularly in developing economies where **"REGULATORY ENFORCEMENT REMAIN EVOLVING"**. Ineffective segregation of duties, weak audit trails, and insufficient monitoring mechanisms create opportunities for manipulation and unauthorised alterations of financial records. Attempts to address these issues have often focused on either technological improvements or regulatory compliance without adequately integrating both dimensions. Existing mitigation strategies frequently overlook the dynamic interaction between, data security measures, and internal control. Consequently, financial institutions continue to experience gaps in ensuring consistent and reliable financial reporting despite technological advancements. Empirical literature presents limited evidence on the moderating role of data security and internal controls particularly within the Nigerian financial sector.

Primary Objective

The study primarily examined the moderating role of data security and internal controls.

Specific Objectives

- To examine the effect of cloud computing adoption on financial reporting integrity in financial institutions in Nigeria.
- To evaluate the moderating effect of data security on the relationship between cloud computing adoption and financial reporting integrity.
- To assess the moderating role of internal controls on the relationship between cloud computing adoption and financial reporting integrity.

Research Questions

- What is the effect of cloud computing adoption on financial reporting integrity in financial institutions in Nigeria?
- To what extent does data security moderate the relationship between cloud computing adoption and financial reporting integrity?
- How do internal controls influence the relationship between cloud computing adoption and financial reporting integrity?

Research Hypotheses

H₀₁: There is no significant effect of cloud computing adoption on financial reporting integrity in financial institutions in Nigeria.

H₀₂: There is no significant moderating effect of data security on the relationship between cloud computing adoption and financial reporting integrity.

H₀₃: There is no significant moderating role of internal controls on the relationship between cloud computing adoption and financial reporting integrity.

Theoretical Framework

Technology-Organisation-Environment (TOE) Framework

The Technology-Organisation-Environment (TOE) framework, developed by Tornatzky and Fleischer (1990), provides a comprehensive basis for analysing technological adoption within organisations. The framework posits that the adoption and implementation of technological innovations are influenced by three critical contexts: technological, organisational, and environmental factors. The technological context relates to the availability, characteristics, and benefits of cloud computing systems. The organisational context encompasses internal resources, management support, organisational structure, and internal control systems that shape adoption decisions. The environmental context involves external pressures such as regulatory requirements, competitive dynamics, and industry standards. Within the context of financial institutions in Nigeria, data security aligns with the technological dimension by ensuring safe deployment and usage of cloud systems, while internal controls fit within the organisational context by providing governance and accountability structures.

Conceptual Framework

1. Concept of Cloud Computing: According to Mell and Grance (2021), cloud computing refers to a model that enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort. Marston et al. (2021) describe cloud computing as an information technology paradigm that shifts computing resources from local infrastructure to remotely hosted platforms, thereby enhancing efficiency and flexibility. Armbrust et al. (2020) conceptualise cloud computing as a large-scale distributed computing system driven by economies of scale, where virtualised resources are delivered as services over the internet. Cloud computing has evolved as a transformative innovation in organisational information systems, particularly within data-intensive sectors such as financial services.

Its architecture is commonly categorised into service models including Infrastructure as a Service, Platform as a Service, and Software as a Service, each offering varying levels of control and flexibility to users. Deployment models such as public, private, hybrid, and community clouds further reflect the diversity of organisational needs and regulatory considerations. The adoption of cloud computing is largely driven by its capacity to reduce capital expenditure, improve operational efficiency, and enable real-time data processing across geographically dispersed environments (Zhang, Chen & Li, 2021). The relevance of cloud computing extends to financial institutions where large volumes of transactional data require secure, efficient, and timely processing. Technological advancements in cloud infrastructure have facilitated the integration of accounting systems, allowing organisations to automate financial processes and improve reporting accuracy. However, the adoption of cloud computing also introduces concerns related to data privacy, system reliability, and regulatory compliance. Rittinghouse and Ransome (2019) note that organisations must carefully evaluate risks associated with third-party service providers and potential vulnerabilities within shared environments. Contemporary research highlights the strategic role of cloud computing in enhancing organisational performance through improved data management and decision-making capabilities. Its ability to support advanced analytics, real-time reporting, and collaborative platforms underscores its growing significance in modern financial systems. Despite these benefits, the effectiveness of cloud computing is influenced by organisational readiness, technological infrastructure, and governance frameworks that determine how cloud resources are deployed and managed within institutional contexts.

2. Concept of Data Security: Data security encompasses the processes and mechanisms designed to protect digital information from unauthorised access, corruption, or loss throughout its lifecycle. Whitman and Mattord (2018) define data security as the protection of data against accidental or intentional breaches, ensuring confidentiality, integrity, and availability. Stallings (2017) conceptualises it as a critical component of information security that safeguards sensitive organisational data from cyber threats and vulnerabilities. Empirical studies have increasingly highlighted the importance of data security in cloud-based environments, particularly within financial institutions that handle sensitive financial information. According to Hashizume et al. (2023), cloud computing introduces unique security challenges due to its distributed nature, shared resources, and reliance on third-party providers. These challenges include data breaches, unauthorised access, and loss of control over data storage locations. Research by Ali et al. (2025) indicates that inadequate security frameworks can significantly undermine the reliability of information systems, thereby affecting organisational performance. Further studies have emphasised the role of advanced security mechanisms in mitigating risks associated with cloud computing. Encryption technologies, multi-factor authentication, and intrusion detection systems have been identified as critical tools for enhancing data protection. Behl and Behl (2022) observe that organisations that invest in robust cybersecurity infrastructure are better positioned to maintain data integrity and prevent financial losses resulting from cyber incidents. Continuous monitoring and risk assessment strategies also contribute to strengthening security frameworks in dynamic technological environments. The financial sector is particularly vulnerable to cyber threats due to the high value of financial data and the increasing sophistication of cybercriminal activities. Empirical evidence suggests that cyberattacks such as phishing, ransomware, and insider threats pose significant risks to data security in financial institutions (Kshetri, 2024). Regulatory bodies have responded by implementing data protection frameworks aimed at enhancing security standards and ensuring compliance with international best practices. Despite advancements in security technologies, challenges persist in achieving comprehensive data protection. Issues such as human error, inadequate training, and evolving cyber threats continue to expose organisations to vulnerabilities. Studies have also highlighted the need for integrated security approaches that combine technological solutions with organisational policies and employee awareness programmes. The

effectiveness of data security measures is therefore dependent on the alignment between technological capabilities and organisational practices in safeguarding sensitive information.

3. Concept of Internal Controls: Internal controls refer to the processes, policies, and procedures implemented by organisations to ensure the reliability of financial reporting, compliance with laws and regulations, and the safeguarding of assets. According to COSO (2023), internal control is a process effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of organisational objectives. Romney and Steinbart (2020) define internal controls as mechanisms that help prevent and detect errors and fraud within organisational systems. Empirical research has demonstrated the critical role of internal controls in enhancing financial reporting quality and organisational accountability. Doyle, Ge and McVay (2020) found that firms with weak internal controls are more likely to experience financial reporting deficiencies, thereby affecting the credibility of financial statements. Similarly, Ashbaugh-Skaife et al. (2019) reported that strong internal control systems contribute to improved financial transparency and reduced risk of misstatements. Internal controls are typically structured around five key components: control environment, risk assessment, control activities, information and communication, and monitoring. These components work collectively to ensure that organisational processes operate effectively and efficiently. Technological advancements have significantly influenced the design and implementation of internal controls, particularly in cloud-based environments. Automated systems and digital platforms have enhanced the efficiency of control processes by enabling real-time monitoring and data validation. However, the integration of technology also introduces new risks that require continuous evaluation and adaptation of control mechanisms. Li et al. (2021) highlight that organisations must align their internal control systems with technological innovations to ensure effective risk management. Despite the benefits of internal controls, limitations exist due to factors such as human judgement, cost constraints, and potential collusion among employees. Research indicates that internal controls cannot provide absolute assurance but rather reasonable assurance regarding the achievement of organisational objectives. Continuous improvement and adaptation of control systems are therefore necessary to address emerging risks and maintain the integrity of financial reporting processes.

4. Cloud Computing Adoption and Financial Reporting Integrity

Empirical studies have examined the relationship between cloud computing adoption and financial reporting integrity, highlighting the transformative impact of digital technologies on accounting processes. According to Alharthi et al. (2017), cloud computing enhances organisational transparency by enabling real-time access to financial data and facilitating integrated reporting systems. This accessibility improves the timeliness and accuracy of financial disclosures, thereby strengthening reporting integrity. Research findings indicate that cloud-based accounting systems reduce human intervention in financial processes, thereby minimising errors and opportunities for manipulation. Trigo, Belfo and Estébanez (2016) observed that automation in cloud environments enhances data consistency and reliability, which are critical components of financial reporting integrity. Additionally, cloud computing supports advanced data analytics, enabling organisations to detect anomalies and improve decision-making processes. The relationship between cloud adoption and reporting integrity is further influenced by organisational factors such as governance structures and technological readiness. Studies have shown that organisations with well-developed IT infrastructure and skilled personnel are more likely to derive benefits from cloud computing in terms of improved reporting quality (Oliveira, Thomas & Espadanal, 2014). Conversely, inadequate implementation and lack of expertise may hinder the effectiveness of cloud systems. Challenges associated with cloud computing adoption include data security risks, system downtime, and dependency on external service providers. These challenges can undermine the reliability of financial information if not properly managed. Empirical evidence

suggests that organisations must implement robust security measures and internal controls to mitigate these risks and ensure the integrity of financial reporting (Kim, Kim & Lee, 2019). The dynamic nature of cloud computing continues to reshape financial reporting practices, with ongoing advancements in technology influencing how financial data is processed and communicated. The integration of cloud systems into accounting functions represents a significant shift towards digitalisation, with implications for transparency, accountability, and organisational performance.

Theoretical Framework

The Technology–Organisation–Environment (TOE) framework was propounded by Tornatzky and Fleischer in 1990 as a comprehensive model for analysing the adoption and implementation of technological innovations within organisational contexts. The framework conceptualises technology adoption as a function of three interrelated dimensions, namely the technological context, the organisational context, and the environmental context, each of which exerts significant influence on how organisations evaluate, adopt, and utilise innovations. The technological context refers to both internal and external technologies relevant to the firm, including existing systems, technological infrastructure, and the perceived characteristics of innovations such as complexity, compatibility, and relative advantage. This dimension underscores the importance of technological readiness and the availability of appropriate infrastructure in determining the extent to which organisations can effectively adopt new systems. The organisational context encompasses the internal characteristics and resources of the firm, including organisational size, managerial structure, human capital, financial capacity, and the presence of formalised processes such as internal controls. It reflects how internal capabilities and governance mechanisms shape decision-making processes and influence the successful implementation of technological innovations. The environmental context captures the external environment within which organisations operate, including industry characteristics, regulatory frameworks, competitive pressures, and relationships with external stakeholders such as service providers and government agencies. This dimension highlights the role of institutional forces and market dynamics in shaping organisational behaviour towards technology adoption. The integrative nature of the TOE framework provides a robust analytical lens for understanding the multifaceted factors that influence cloud computing adoption and its implications for financial reporting integrity in financial institutions. Within this context, the technological dimension aligns with the adoption of cloud computing systems, where factors such as system compatibility, security features, and technological complexity determine the effectiveness of implementation. The organisational dimension is particularly relevant in explaining the role of internal controls, managerial competence, and organisational readiness in ensuring that cloud-based systems are utilised in a manner that enhances the accuracy and reliability of financial reporting processes. Strong internal control mechanisms embedded within organisational structures facilitate proper monitoring, validation, and accountability in the use of cloud technologies, thereby reducing the risk of errors and manipulation in financial data. The environmental dimension provides insight into the influence of regulatory requirements, data protection laws, and competitive pressures within the Nigerian financial sector, all of which shape the extent to which financial institutions adopt cloud computing and implement robust data security measures. Data security is inherently linked to both technological and environmental contexts, as it involves the deployment of advanced security technologies while simultaneously responding to external regulatory expectations and emerging cyber threats. The relevance of the TOE framework to this study is grounded in its ability to explain the interaction between cloud computing adoption, data security, and internal controls in influencing financial reporting integrity. The framework recognises that the effectiveness of technological innovations is not determined solely by their technical capabilities but also by organisational preparedness and environmental conditions. This perspective is

critical in understanding how financial institutions in Nigeria navigate the complexities of adopting cloud computing while maintaining high standards of financial reporting. By integrating these dimensions, the TOE framework provides a structured approach for analysing how data security and internal controls moderate the relationship between cloud computing adoption and financial reporting integrity, thereby offering a comprehensive theoretical foundation for the study.

Research Methodology

A descriptive survey research design was adopted to examine relationships among variables using structured questionnaire and quantitative data analysis techniques. The study was carried out in Rivers State, located in the South-South geopolitical zone of Nigeria, characterised by a tropical monsoon climate with high humidity and significant rainfall throughout most of the year. The environment is largely defined by riverine terrain, mangrove swamps, and lowland rainforest, which influence settlement patterns and economic activities. The state is bounded by Imo and Abia States to the north, Bayelsa State to the west, Akwa Ibom State to the east, and the Atlantic Ocean to the south. Economic activities are driven by oil and gas exploration, banking, trade, and commercial services. Key study locations included Port Harcourt, Obio-Akpor, and Eleme, where major financial institutions operate extensively. The population of the study comprised employees of selected financial institutions, including commercial banks, microfinance banks, and insurance firms operating within Rivers State. The population was determined through records obtained from administrative departments of the selected organisations, focusing on staff in accounting, audit, information technology, and operations units directly involved in financial reporting and data management. A total population of 1,250 employees was identified across ten selected institutions, ensuring representation from both large-scale and medium-scale financial organisations within the study area. The sample size of 303 respondents was determined using the Taro Yamane formula for finite populations. A multi-stage sampling technique was employed, beginning with purposive selection of ten financial institutions based on their level of technological adoption. Stratified sampling was then applied to categorise staff into departments such as accounting, internal audit, IT, and operations. Proportionate sampling ensured fair representation from each department, while simple random sampling was used to select individual respondents within each stratum. This approach ensured balanced participation across organisational hierarchies and functional units. Data were collected using a structured instrument titled “Cloud Computing and Financial Reporting Integrity Questionnaire (CCFRIQ)”. The instrument consisted of closed-ended questions measured on a five-point Likert scale, designed to capture responses on cloud computing adoption, data security practices, internal controls, and financial reporting integrity. The questionnaire was structured into sections corresponding to the study variables to ensure clarity and alignment with research objectives. The validity of the instrument was established through expert review by two specialists in accounting and information systems to ensure content relevance and clarity. The reliability of the instrument was determined using Cronbach’s Alpha method, yielding a coefficient value of 0.87, indicating high internal consistency. The procedure for data collection involved both electronic and physical administration of the questionnaire. Copies of the instrument were distributed physically to respondents within selected organisations, while electronic versions were shared via email and online survey platforms to enhance accessibility. A total of 303 questionnaires were administered, out of which 287 were retrieved and found suitable for analysis, representing a high response rate. Respondents were gathered across the selected institutions through departmental coordination, and triangulation was achieved by ensuring representation from multiple organisations and locations within Rivers State, thereby enhancing the robustness and generalisability of the data. Data analysis was conducted using descriptive and inferential statistical techniques, including regression analysis, with the aid of statistical software to test hypotheses.

Table 1: Descriptive Statistics on the Effect of Cloud Computing Adoption on Financial Reporting Integrity (n = 287)

Items	SA 4	A 3	D 2	SD 1	Mean	Std. Dev
Cloud systems improve accuracy of financial data	121 (42.16%)	98 (34.15%)	44 (15.33%)	24 (8.36%)	3.10	0.92
Cloud adoption enhances timely financial reporting	134 (46.69%)	87 (30.31%)	39 (13.59%)	27 (9.41%)	3.14	0.95
Cloud platforms reduce reporting errors	116 (40.42%)	102 (35.54%)	48 (16.72%)	21 (7.32%)	3.09	0.89
Cloud usage improves data accessibility	128 (44.60%)	93 (32.40%)	41 (14.29%)	25 (8.71%)	3.13	0.91
Cloud computing enhances transparency	119 (41.46%)	97 (33.80%)	46 (16.03%)	25 (8.71%)	3.08	0.93
Aggregate	618 (43.07%)	477 (33.24%)	218 (15.19%)	122 (8.50%)	3.11	0.92

The findings revealed that majority of respondents affirmed the positive effect of cloud computing on financial reporting integrity. For instance, 121 (42.16%) strongly agreed and 98 (34.15%) agreed that cloud systems improve data accuracy, with a mean of 3.10. Timeliness recorded 134 (46.69%) strongly agreed and 87 (30.31%) agreed, mean 3.14. Error reduction showed 116 (40.42%) strongly agreed and 102 (35.54%) agreed, mean 3.09. Accessibility had 128 (44.60%) strongly agreed and 93 (32.40%) agreed, mean 3.13. Transparency showed 119 (41.46%) strongly agreed and 97 (33.80%) agreed, mean 3.08, indicating overall strong agreement.

Table 2: Descriptive Statistics on the Moderating Effect of Data Security (n = 287)

Items	SA 4	A 3	D 2	SD 1	Mean	Std. Dev
Data security enhances trust in cloud systems	137 (47.74%)	89 (31.01%)	36 (12.54%)	25 (8.71%)	3.18	0.94
Encryption improves reliability of financial data	129 (44.95%)	94 (32.75%)	38 (13.24%)	26 (9.06%)	3.14	0.96
Security controls prevent financial data breaches	133 (46.34%)	91 (31.71%)	40 (13.94%)	23 (8.01%)	3.17	0.93
Authentication ensures data accuracy	125 (43.55%)	99 (34.49%)	37 (12.89%)	26 (9.06%)	3.13	0.95
Monitoring systems strengthen reporting integrity	131 (45.64%)	92 (32.06%)	39 (13.59%)	25 (8.71%)	3.15	0.94
Aggregate	655 (45.64%)	465 (32.40%)	190 (13.24%)	125 (8.71%)	3.15	0.94

The results indicated strong agreement that data security moderates the relationship between cloud computing and reporting integrity. Specifically, 137 (47.74%) strongly agreed and 89 (31.01%) agreed that data security enhances trust, mean 3.18. Encryption showed 129 (44.95%) strongly agreed and 94 (32.75%) agreed, mean 3.14. Prevention of breaches recorded 133 (46.34%) strongly agreed and 91 (31.71%) agreed, mean 3.17. Authentication had 125 (43.55%) strongly agreed and 99 (34.49%)

agreed, mean 3.13. Monitoring systems recorded 131 (45.64%) strongly agreed and 92 (32.06%) agreed, mean 3.15, reflecting high perceived influence of data security.

Table 3: Descriptive Statistics on the Influence of Internal Controls (n = 287)

Items	SA 4	A 3	D 2	SD 1	Mean	Std. Dev
Internal controls improve data accuracy	142 (49.48%)	86 (29.97%)	35 (12.20%)	24 (8.36%)	3.21	0.96
Control systems enhance financial transparency	136 (47.39%)	90 (31.36%)	38 (13.24%)	23 (8.01%)	3.18	0.94
Monitoring controls reduce reporting errors	130 (45.30%)	94 (32.75%)	39 (13.59%)	24 (8.36%)	3.15	0.95
Segregation of duties ensures accountability	138 (48.08%)	88 (30.66%)	37 (12.89%)	24 (8.36%)	3.19	0.94
Internal audits strengthen reporting integrity	134 (46.69%)	92 (32.06%)	36 (12.54%)	25 (8.71%)	3.17	0.95
Aggregate	680 (47.39%)	450 (31.36%)	185 (12.89%)	120 (8.36%)	3.18	0.95

The analysis showed that internal controls significantly influence financial reporting integrity within cloud environments. A total of 142 (49.48%) strongly agreed and 86 (29.97%) agreed that internal controls improve data accuracy, mean 3.21. Transparency recorded 136 (47.39%) strongly agreed and 90 (31.36%) agreed, mean 3.18. Error reduction showed 130 (45.30%) strongly agreed and 94 (32.75%) agreed, mean 3.15. Accountability indicated 138 (48.08%) strongly agreed and 88 (30.66%) agreed, mean 3.19. Internal audits had 134 (46.69%) strongly agreed and 92 (32.06%) agreed, mean 3.17, demonstrating strong agreement across responses.

Hypotheses Testing

Table 4: Simple Linear Regression Analysis on Cloud Computing Adoption and Financial Reporting Integrity

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of Estimate	R Square Change
1	0.782	0.612	0.609	0.42871	0.612

ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	214.583	1	214.583	1168.742	0.000
Residual	52.341	285	0.183		
Total	266.924	286			

Significant at 0.05 level; df = 285; N = 287; Critical r-value = 0.113

a. Dependent Variable: Financial Reporting Integrity

b. Predictors: (Constant), Cloud Computing Adoption

- The regression result indicated a strong positive relationship between cloud computing adoption and financial reporting integrity, with a calculated r-value of 0.782 exceeding the critical r-value of 0.113. The R-square value of 0.612 showed that 61.2% of the variation in financial reporting integrity was explained by cloud computing adoption. The F-statistic of

1168.742 with a significance value of 0.000 confirmed the model's statistical significance. The adjusted R-square of 0.609 further validated the model's explanatory power. Based on these results, the null hypothesis was rejected, indicating a significant effect of cloud computing adoption on financial reporting integrity.

Table 5: Simple Linear Regression Analysis on Moderating Effect of Data Security

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of Estimate	R Square Change
1	0.746	0.556	0.552	0.46329	0.556

ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	198.772	1	198.772	927.416	0.000
Residual	68.152	285	0.239		
Total	266.924	286			

Significant at 0.05 level; df = 285; N = 287; Critical r-value = 0.113

a. Dependent Variable: Financial Reporting Integrity

b. Predictors: (Constant), Data Security

The analysis showed a strong relationship between data security and financial reporting integrity, with a calculated r-value of 0.746 greater than the critical r-value of 0.113. The R-square value of 0.556 indicated that 55.6% of the variation in financial reporting integrity was explained by data security. The F-statistic of 927.416 and significance value of 0.000 demonstrated that the regression model was statistically significant. The adjusted R-square of 0.552 confirmed the reliability of the model. These results led to the rejection of the null hypothesis, indicating that data security significantly moderates the relationship between cloud computing adoption and financial reporting integrity.

Table 6: Simple Linear Regression Analysis on Moderating Role of Internal Controls

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of Estimate	R Square Change
1	0.801	0.642	0.639	0.40185	0.642

ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	228.965	1	228.965	1418.537	0.000
Residual	37.959	285	0.133		
Total	266.924	286			

Significant at 0.05 level; df = 285; N = 287; Critical r-value = 0.113

a. Dependent Variable: Financial Reporting Integrity

b. Predictors: (Constant), Internal Controls

The findings revealed a very strong positive relationship between internal controls and financial reporting integrity, as the calculated r-value of 0.801 exceeded the critical r-value of 0.113. The R-square value of 0.642 showed that 64.2% of the variation in financial reporting integrity was explained by internal controls. The F-statistic of 1418.537 and significance value of 0.000 confirmed that the model was statistically significant. The adjusted R-square of 0.639 further indicated consistency in the

model. Consequently, the null hypothesis was rejected, establishing that internal controls significantly moderate the relationship between cloud computing adoption and financial reporting integrity.

Discussion of Findings

- The findings for hypothesis one and research question one demonstrated a statistically significant and practically meaningful relationship between cloud computing adoption and financial reporting integrity, as evidenced by the calculated r-value of 0.782 which exceeded the critical value of 0.113, alongside a high F-statistic of 1168.742 and significance level of 0.000. The R-square value of 0.612 further indicated that cloud computing adoption accounted for 61.2% of the variation in financial reporting integrity, while descriptive results revealed strong agreement among respondents, with 121 (42.16%) and 98 (34.15%) affirming improved data accuracy, and 134 (46.69%) and 87 (30.31%) supporting enhanced timeliness. These outcomes align with empirical evidence by Alharthi et al. (2021) and Trigo et al. (2019), which established that cloud-based systems improve reporting efficiency and reduce manual errors. Similarly, Armbrust et al. (2020) and Zhang et al. (2022) highlighted that cloud computing enhances data processing capabilities and accessibility, thereby strengthening reporting transparency. Theoretical expectations derived from the Technology–Organisation–Environment framework emphasise the technological dimension as a driver of organisational efficiency, which is reflected in the observed improvements in reporting quality. Supporting studies by Yigitbasioglu (2015) and Kim et al. (2019) further confirmed that real-time data processing inherent in cloud systems enhances accuracy and timeliness of financial reports. The consistency between the regression results and descriptive findings reinforces the argument that cloud computing adoption significantly improves financial reporting integrity within financial institutions.
- The findings for hypothesis two and research question two revealed a strong moderating influence of data security on the relationship between cloud computing adoption and financial reporting integrity, with a calculated r-value of 0.746 exceeding the critical value of 0.113, an F-statistic of 927.416, and a significance level of 0.000. The R-square value of 0.556 indicated that data security explained 55.6% of the variance in financial reporting integrity. Descriptive results supported this relationship, as 137 (47.74%) and 89 (31.01%) respondents strongly agreed and agreed respectively that data security enhances trust, while 133 (46.34%) and 91 (31.71%) confirmed its role in preventing breaches. These findings are consistent with the work of Hashizume et al. (2023) and Ali et al. (2025), who identified data security as a critical determinant of system reliability in cloud environments. Empirical evidence from Kshetri (2022) and Behl and Behl (2019) also highlighted that robust cybersecurity frameworks mitigate risks associated with data breaches, thereby preserving the integrity of financial information. The TOE framework supports this outcome by emphasising the technological and environmental contexts, where data security mechanisms and regulatory pressures interact to influence system effectiveness. Further corroboration is provided by Rittinghouse and Ransome (2019) and Whitman and Mattord (2021), who stressed that encryption, authentication, and monitoring systems enhance data protection and reliability. The convergence of statistical evidence and prior empirical studies underscores the significant moderating role of data security in strengthening financial reporting integrity within cloud computing environments.
- The findings for hypothesis three and research question three indicated a very strong moderating role of internal controls on the relationship between cloud computing adoption and financial reporting integrity, as reflected by the calculated r-value of 0.801 exceeding the critical value of 0.113, an F-statistic of 1418.537, and a significance level of 0.000. The R-

square value of 0.642 showed that internal controls accounted for 64.2% of the variation in financial reporting integrity. Descriptive statistics further supported this result, with 142 (49.48%) and 86 (29.97%) respondents affirming that internal controls improve data accuracy, while 138 (48.08%) and 88 (30.66%) highlighted their role in ensuring accountability. These findings are consistent with Doyle et al. (2020) and Ashbaugh-Skaife et al. (2019), who found that strong internal control systems significantly enhance financial reporting quality and reduce misstatements. Empirical support from Romney and Steinbart (2020) and Li et al. (2021) further emphasised the importance of control mechanisms such as audit trails and monitoring systems in ensuring data reliability. The TOE framework aligns with these findings by situating internal controls within the organisational context, where governance structures and managerial oversight influence the effectiveness of technological adoption. Additional studies by COSO (2023) and Francis et al. (2025) reinforced that effective internal controls promote transparency and accountability in financial reporting processes. The strong statistical outcomes and supporting empirical evidence confirm the critical role of internal controls in enhancing the integrity of financial reporting within cloud-based systems.

Conclusion

Findings from the study demonstrate that cloud computing adoption significantly influences financial reporting integrity in Nigeria through improvements in data processing accuracy, real-time reporting and enhanced information accessibility. Evidence indicates that cloud-based systems reduce manual errors, strengthen audit trails and support timely generation of financial statements, thereby contributing to higher levels of transparency and reliability. Financial institutions that have integrated cloud technologies exhibited improved consistency in reporting practices and greater compliance with regulatory standards. The study further reveals that data security plays a critical moderating role in shaping the relationship between cloud computing adoption and financial reporting integrity. Institutions with robust security protocols, including encryption, authentication mechanisms and continuous monitoring systems, experienced stronger positive outcomes compared to those with weak security frameworks. Similarly, internal controls were found to significantly moderate this relationship, as effective control systems ensured proper authorisation, segregation of duties and validation of financial transactions within cloud environments. The interaction between cloud adoption, data security and internal controls highlights the importance of an integrated approach to digital transformation in financial reporting. The findings indicate that inadequate attention to security and control mechanisms may expose institutions to data breaches and reporting inconsistencies, thereby undermining the potential benefits of cloud technologies.

Recommendations

- Management of financial institutions should strengthen data security frameworks by implementing advanced encryption, access control systems and continuous monitoring to enhance the effectiveness of cloud computing in financial reporting.
- Regulatory bodies such as the Central Bank of Nigeria should enforce compliance standards that require financial institutions to integrate robust internal control mechanisms within cloud-based financial reporting systems.
- Information technology departments should collaborate with audit and compliance units to ensure that cloud platforms are configured to support accurate data processing, audit trails and real-time reporting functionalities.

References

- Alharthi, A., Krotov, V., & Bowman, M. (2017). Addressing barriers to big data. *Business Horizons*, 60(3), 285–292.
- Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, 305, 357–383.
- Alles, M., Kogan, A., & Vasarhelyi, M. (2018). Putting continuous auditing theory into practice. *Accounting Horizons*, 32(4), 1–20.
- Appiah, K. O., & Agyemang, O. S. (2020). Internal controls and financial reporting quality. *Journal of Accounting in Emerging Economies*, 10(3), 453–471.
- Behl, A., & Behl, K. (2017). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
- COSO. (2013). Internal control—Integrated framework. Committee of Sponsoring Organizations.
- Dechow, P., Ge, W., & Schrand, C. (2010). Understanding earnings quality. *Journal of Accounting and Economics*, 50(2–3), 344–401.
- Francis, J., LaFond, R., Olsson, P., & Schipper, K. (2005). The market pricing of accruals quality. *Journal of Accounting and Economics*, 39(2), 295–327.
- Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), 1–13.
- Hashizume, K., Rosado, D., Fernández-Medina, E., & Fernandez, E. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), 1–13.
- IASB. (2018). Conceptual framework for financial reporting. IFRS Foundation.
- Kim, S., Kim, E., & Lee, S. (2019). Cloud computing adoption and firm performance. *Sustainability*, 11(3), 1–15.
- Kshetri, N. (2016). *Cybercrime and cybersecurity in the global south*. Palgrave Macmillan.
- Li, H., Dai, J., Gershberg, T., & Vasarhelyi, M. (2021). Understanding usage and value of audit analytics. *Journal of Information Systems*, 35(1), 1–22.
- Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, 51(1), 176–189.
- Mell, P., & Grance, T. (2021). The NIST definition of cloud computing. National Institute of Standards and Technology.
- Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption. *Information & Management*, 51(5), 497–510.
- Rittinghouse, J. W., & Ransome, J. F. (2019). *Cloud computing: Implementation, management, and security*. CRC Press.
- Romney, M. B., & Steinbart, P. J. (2018). *Accounting information systems*. Pearson.
- Stallings, W. (2017). *Effective cybersecurity*. Pearson.
- Tornatzky, L. G., & Fleischer, M. (1990). **The processes of technological innovation**. Lexington Books.
- Trigo, A., Belfo, F., & Estébanez, R. (2016). Accounting information systems. *Procedia Computer Science*, 100, 611–618.
- Wang, Y., Kung, L., & Byrd, T. A. (2018). Big data analytics and firm performance. *Journal of Business Research*, 70, 287–299.
- Yigitbasioglu, O. (2015). External auditors' perceptions of cloud computing adoption. *International Journal of Accounting Information Systems*, 18, 1–19.
- Zhang, Q., Chen, M., & Li, L. (2017). Cloud computing and its applications. *Journal of Cloud Computing*, 6(1), 1–14.