World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Evaluation of cloud based computing in security accounting information system

Sanusi I. [1,*], Sanusi A.R. [2], Shamwill A.K. [2], Yinusa S.[2] and Iliyasu R. [2]

[1] *Department of Statistics, University of Ibadan, Ibadan, Oyo State, Nigeria.*
[2] *Institute of Governance and Development Studies, Nasarawa State University, Keffi, Nasarawa State, Nigeria.*

World Journal of Advanced Research and Reviews, 2025, 25(03), 1073-1086

Publication history: Received on 26 January 2025; revised on 11 March 2025 accepted on 13 March 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.3.0734

Abstract

The increasing reliance on cloud-based accounting information systems (AIS) has heightened concerns about data security, necessitating the adoption of effective protective measures. This study examines the impact of security mechanisms, including data encryption, access control, backup and recovery procedures, compliance with security standards, and user awareness and training, on the security of cloud-based AIS. A quantitative research design was employed, utilizing a structured questionnaire to collect data from 384 respondents in organizations that use cloud-based AIS. Multiple regression analysis was conducted to assess the relationship between the independent security measures and the dependent variable—system security. Additionally, an Artificial Neural Network (ANN) model was used to determine the relative importance of each security measure in enhancing AIS security. The model's validity was confirmed through diagnostic tests, including collinearity assessment and error evaluation. The findings revealed that data encryption, access control mechanisms, backup and recovery procedures, and compliance with security standards significantly enhance AIS security, while user awareness and training had an insignificant effect. Data encryption emerged as the most critical factor, followed by access control and compliance. The ANN model reinforced these findings, indicating that technical security measures play a more dominant role in safeguarding cloud-based AIS. The study concludes that robust encryption, strict access control, and regulatory compliance are essential for strengthening cloud security. The study recommends that organizations should prioritize implementing advanced encryption techniques, enforcing stringent access control policies, and ensuring compliance with established security standards. While user training remains important, technical security measures should be the primary focus for securing cloud-based accounting information systems effectively.

Keywords: Access Control Mechanism; Backup and Recovery Procedures; Compliance with Security Standards; Data Encryption; Security of Cloud-Based AIS; User Awareness and Training

1. Introduction

The rapid evolution of technology has significantly transformed accounting processes worldwide. Cloud-based accounting systems represent a major advancement, offering benefits such as scalability, cost-effectiveness, and real-time access to financial data (Smith & Rupp, 2021). These systems provide organizations with the ability to manage accounting information online, enhancing operational efficiency beyond traditional on-premises systems (Jones, 2020). Due to their ability to optimize financial processes, reduce IT infrastructure costs, and facilitate collaboration, cloud-based accounting solutions have gained popularity among businesses of all sizes (Brown & Thompson, 2022). According to Grand View Research (2022), the global market for cloud accounting software is projected to reach $7.9 billion by 2025, reflecting the increasing reliance on cloud technology in financial management. Since accounting information systems (AIS) handle sensitive financial data, they are prime targets for cyber threats.

* Corresponding author: Sanusi Ibraheem.

Data breaches and cyber-attacks have underscored the need for robust security protocols to protect cloud-based accounting systems (Kumar & Kaur, 2021). In 2021, over 1,200 data breaches were recorded in the United States, many of which involved cloud environments (Verizon Data Breach Investigations Report, 2022). Such breaches can lead to financial losses, legal liabilities, and reputational damage (Wang, Li & Kim, 2021). To mitigate these risks, organizations must implement a combination of technical measures and organizational strategies. Encryption, access control mechanisms, and regular security audits are key methods for enhancing the security of cloud-based AIS (Gupta & Sharman, 2021). Encryption ensures that intercepted data remains unreadable without a decryption key, preserving confidentiality (Mell & Grance, 2021). Additionally, multi-factor authentication (MFA) prevents unauthorized access by requiring identity verification before granting access (Johnson, Jones & Wang, 2021).

Backup and recovery strategies are critical components of a secure cloud-based AIS, ensuring data restoration in the event of a security breach or system failure (Smith, Wang & Patel, 2021). Compliance with international security standards such as ISO 27001 and SOC 2 is vital in safeguarding cloud-based accounting systems (Rouse, 2021). These frameworks help organizations establish, implement, and manage security controls while ensuring adherence to regulatory requirements (Jensen & Meckling, 2020). Moreover, human factors play a significant role in the security of cloud-based accounting systems. Employee training and awareness programs are essential in preventing security breaches, as human error often contributes to security incidents (Sommestad et al., 2021). Educating employees on security best practices can reduce the likelihood of breaches caused by negligence or lack of awareness (Huang & Pearlson, 2021).

The adoption of cloud-based accounting solutions has been driven by advancements in information technology, revolutionizing traditional accounting practices. Previously, organizations relied on on-premises software, requiring substantial investment in hardware, software, and IT personnel. Cloud-based solutions have disrupted this model by providing accounting software as a service (SaaS), enabling organizations to pay only for the services they use, resulting in cost savings and improved efficiency (Tahmid, 2023). These systems are hosted on remote servers managed by cloud service providers, allowing users to access their accounting data from any internet-enabled device (Tahmid, 2023). The flexibility and scalability of cloud-based solutions benefit small and medium-sized enterprises (SMEs), which may lack the resources to invest in complex IT infrastructure. By leveraging cloud-based systems, SMEs can compete with larger firms, utilizing advanced accounting features and real-time data analytics to make informed financial decisions (Castellani, Mariotti, & Piscitello, 2022). These systems also improve collaboration by allowing multiple users to simultaneously access and update financial records, enhancing efficiency and reducing reporting time (Castellani et al., 2022).

A key security measure for cloud-based accounting systems is data encryption, which ensures that unauthorized individuals cannot interpret information without a decryption key. Advanced Encryption Standards (AES) and Secure Socket Layer (SSL) encryption are commonly employed to protect data in transit and at rest, providing an additional security layer (Hassan et al., 2022). Role-based access control (RBAC) further enhances security by restricting access to sensitive information based on user roles within an organization (Marquis, 2024). Additionally, implementing robust backup and recovery protocols is crucial for minimizing data loss in the event of cyber-attacks, system failures, or natural disasters. Regular data backups ensure business continuity by restoring lost information, reducing downtime, and mitigating breach impacts (Kesa, 2023). Organizations should establish comprehensive backup plans, including regular backups, secure storage, and periodic recovery tests to ensure data integrity (Kritikos & Skrzypek, 2022).

Compliance with security regulations is essential in strengthening the security of cloud-based accounting systems. Adhering to frameworks such as the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States demonstrates organizational commitment to data security and legal compliance (Isibor, 2024). Many cloud service providers undergo third-party audits to verify compliance, assuring clients that their data is securely managed (Solms & Niekerk, 2021). Furthermore, employee training and security awareness programs form an integral part of a holistic security strategy. A significant number of security breaches result from human errors, such as weak passwords, phishing scams, or accidental data leaks (Bhadouria, 2022). Organizations must invest in continuous security awareness training to educate employees on modern security threats and best practices for data protection (Bhadouria, 2022).

1.1. Statement of Problem

The adoption of cloud-based accounting systems has transformed financial management by enhancing accessibility, reducing operational costs, and streamlining accounting processes (Smith & Rupp, 2021). Despite the numerous advantages of cloud-based accounting systems, including cost-effectiveness, scalability, and real-time financial data access, concerns regarding their security remain a critical issue for organizations. The increasing reliance on cloud

technology has exposed accounting information systems (AIS) to cyber threats, data breaches, and unauthorized access, which can compromise financial integrity and lead to significant economic losses. Many organizations lack robust security frameworks, leaving sensive financial data vulnerable to cyber-attacks such as hacking, phishing, and ransomware. Additionally, compliance with global data protection regulations, such as the General Data Protection Regulation (GDPR) and the International Organization for Standardization (ISO) security standards, presents challenges for businesses operating across multiple jurisdictions. Weak encryption protocols, inadequate authentication measures, and human-related security lapses further exacerbate these vulnerabilities. As financial data forms the backbone of corporate decision-making, any compromise in the security of cloud-based accounting systems could undermine business sustainability, stakeholder confidence, and regulatory compliance. Thus, addressing these security concerns is imperative to ensuring the continued adoption and effectiveness of cloud-based accounting in modern financial management.

1.2. Research Gap

Existing studies on cloud-based accounting systems have extensively explored their benefits, including cost efficiency, scalability, and real-time financial data access (Smith & Rupp, 2021; Brown & Thompson, 2022). However, a critical gap remains in addressing the security vulnerabilities associated with these systems, particularly in relation to evolving cyber threats and the adequacy of current security measures. While previous research has examined encryption protocols, access control mechanisms, and compliance with global data protection regulations, limited empirical studies assess the effectiveness of these security strategies in mitigating risks specific to cloud-based accounting (Gupta & Sharman, 2021). Furthermore, much of the existing literature focuses on developed economies, where regulatory frameworks and technological infrastructure are more advanced, leaving a gap in understanding the security challenges faced by organizations in emerging markets (Jensen & Meckling, 2020). Additionally, while studies recognize the role of human factors in cybersecurity, there is insufficient research on how employee awareness and training impact the security of cloud-based accounting systems (Huang & Pearlson, 2021). Addressing these gaps is essential for developing more effective security frameworks that enhance the reliability and adoption of cloud-based accounting systems across diverse business environments.

1.3. Theoretical Underpinning

1.3.1. Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM), developed by Davis (1989), explains technology adoption based on two key factors: perceived ease of use and perceived usefulness. In the context of cloud-based accounting systems, perceived ease of use refers to the system's intuitiveness, while perceived usefulness relates to its ability to enhance efficiency and performance. Research by Amron & Noh (2021) highlighted TAM's relevance in cloud computing, emphasizing its role in evaluating user perceptions and optimizing system design. Organizations can improve adoption rates by enhancing usability through user-friendly interfaces and support systems while demonstrating the tangible benefits of cloud-based accounting. Lun et al. (2024) reinforced that these factors significantly influence user acceptance, confirming TAM's ongoing relevance in the evolving digital landscape.

1.3.2. Diffusion of Innovation (DOI) Theory

The Diffusion of Innovation (DOI) Theory, introduced by Rogers (2003), elucidates the process through which new technologies and practices disseminate within a social system over time. This theory identifies five critical attributes influencing the adoption of innovations: relative advantage, compatibility, complexity, trialability, and observability. In the realm of cloud-based accounting, relative advantage pertains to the benefits these systems offer over traditional methods, such as enhanced efficiency, cost savings, and real-time data access. Compatibility refers to the alignment of cloud accounting solutions with existing business processes and technological infrastructures, which can significantly impact adoption rates. Complexity involves the perceived difficulty in understanding and utilizing the new system; a more user-friendly interface can lead to higher adoption rates. Trialability allows potential adopters to experiment with the system on a limited basis, reducing uncertainty and fostering acceptance. Observability relates to the visibility of the system's benefits to others; when organizations observe peers successfully implementing cloud-based accounting, they are more inclined to adopt it themselves. Empirical studies have applied DOI theory to cloud computing adoption. For instance, Onayemi et al. (2022) examined how SMEs in Kampala, Uganda, adopt cloud computing technologies, revealing that factors such as perceived complexity and lack of trialability hinder adoption. Similarly, Sastararuji and Hoonsopon (2020) integrated DOI with other frameworks to study cloud accounting adoption in SMEs, highlighting the importance of relative advantage and compatibility in the decision-making process. These studies underscore the relevance of DOI theory in understanding the dynamics of cloud-based accounting adoption, emphasizing the need for strategic implementation that addresses these key attributes to facilitate widespread acceptance.

2. Literature Review

Akanbi & Akanbi (2022) analyzed cloud computing adoption in Nigeria, focusing on the barriers and future prospects. The study highlighted significant challenges such as inadequate technological infrastructure, regulatory uncertainties, and resistance to change among organizations. Through a survey of businesses and IT professionals, the authors recommended enhancing the technological infrastructure, streamlining regulatory policies, and fostering a culture of innovation to support cloud adoption. Their findings emphasize the need for a strategic approach to overcoming adoption barriers and leveraging cloud computing benefits for organizational growth. Olokunde & Adekola (2022) explored the challenges of cloud computing adoption in Nigeria, identifying issues such as data sovereignty, security vulnerabilities, and limited technical expertise. The study utilized qualitative data from interviews and surveys to provide a comprehensive analysis of these challenges. The authors recommended implementing robust security measures, adopting best practices in data protection, and investing in technical training to address these challenges effectively. Their recommendations aim to enhance the security and efficiency of cloud computing systems in Nigerian organizations.

Ofoegbu & Olawale (2021) investigated the use of cloud-based accounting systems by SMEs in Nigeria. The study found that while cloud accounting systems offer benefits such as cost savings and improved accessibility, they also present challenges related to data security and system reliability. Through a survey of SMEs, the authors recommended investing in secure and reliable cloud solutions, as well as providing training for staff to maximize the benefits of cloud accounting systems. Their findings highlight the need for a balanced approach to adopting cloud technologies in small and medium enterprises. Alshamaileh, Papagiannidis & Li, (2018) explored the effectiveness of cloud-based financial management systems in Nigerian SMEs. The study identified benefits such as enhanced financial management and accurate reporting but also pointed out challenges such as system integration issues and cybersecurity concerns. The authors recommended adopting hybrid cloud solutions to balance cost and security and investing in training for staff to ensure effective use of cloud-based financial systems. Adeoye & Alhassan (2021) analyzed cybersecurity threats in cloud computing within Nigerian financial institutions. The study found that while cloud computing offers numerous benefits, it also exposes institutions to various cyber threats, including data breaches and ransomware attacks. Recommendations included enhancing cybersecurity measures, investing in advanced threat detection technologies, and implementing regular security audits to protect sensitive data.

Ojedokun (2022) reviewed data protection regulations and compliance in Nigeria, highlighting the challenges organizations face in adhering to data protection laws, particularly in cloud environments. The study emphasized the need for improved regulatory enforcement and better guidance for compliance, recommending that organizations adopt best practices for data protection and work closely with regulatory bodies to ensure compliance. Okere & Asika (2021) examined the impact of cloud computing on the financial performance of Nigerian businesses. The study used financial performance indicators to assess the benefits of cloud adoption, finding positive impacts on efficiency and cost savings. However, it also identified risks related to data security and regulatory compliance. Recommendations included investing in secure cloud solutions and ensuring adherence to regulatory standards to mitigate risks and enhance financial performance. The Technology Acceptance Model (TAM), Diffusion of Innovation (DOI) Theory and the study's empirical data led to the creation of the following hypothesis, which asserts that:

H_1: Data encryption significantly enhances the security of cloud-based accounting information systems.
H_2: Effective access control mechanisms positively impact the security of cloud-based accounting systems.
H_3: Robust backup and recovery procedures contribute significantly to improved security of accounting information in the cloud.
H_4: Compliance with security standards has a significant effect on the security of cloud-based accounting information systems.
H_5: Higher levels of user awareness and training have a significant impact on security of cloud-based accounting systems.

3. Methodology

3.1. Research Design

The study adopts a descriptive research design, which is suitable for collecting information that describes the characteristics of the variables of interest. This design is selected because it allows for a detailed analysis of the current practices, challenges, and perceptions regarding cloud-based accounting systems and their impact on accounting

security. By using a structured questionnaire, the research aims to gather quantitative data that can be analyzed to draw meaningful conclusions about the effectiveness and security implications of cloud-based accounting systems.

3.2. Population of the Study

The population for this study comprises accounting professionals, IT personnel, and management staff from various organizations that utilize cloud-based accounting systems. The inclusion of these groups is essential because they are directly involved in the adoption, implementation, and use of cloud-based accounting systems. Their insights are valuable in understanding the security concerns and effectiveness of these systems in practice. The population spans across small, medium, and large enterprises within Abuja metropolis.

3.3. Sampling Technique and Sample Size

A stratified random sampling technique was employed to ensure representation across different categories of organizations (small, medium, and large enterprises). This approach helps to capture diverse perspectives on cloud-based accounting systems (Maelah, Al Lami, & Ghas, 2021). The sample size will be determined using a sample size formula that ensures statistical significance and representation. The sample size was calculated using the formula for estimating sample sizes for proportions, proposed by Cochran (1977):

$$n = \frac{Z^2 * p * (1 - p)}{e^2}$$

Where
n = sample size
p = estimated proportion (0.5, assuming maximum variability)
Z = Z-score (1.96 at 95% confidence level)
e = margin of error (0.05)

$$n = \frac{1.96^2 * 0.5 * (1 - 0.5)}{0.05^2}$$

$$n = 384$$

3.4. Sources

The study employed primary data collection methods to gather relevant information on the security of cloud-based accounting systems. Primary data, obtained directly from respondents, is advantageous in this context as it provides current, specific insights tailored to the research objectives (Jones, Gwynn, & Teeter, 2019). Collecting firsthand data allows for a more accurate understanding of the factors influencing the security of cloud-based accounting systems, such as data encryption, access control, backup and recovery procedures, compliance with security standards, and user awareness and training.

3.5. Methods of Data Collection

The primary data was collected through the use of a structured questionnaire, a common and effective tool for gathering large amounts of data efficiently. The questionnaire will be designed to cover all aspects of the study's objectives and to address the research questions comprehensively. It includes a mix of closed-ended and Likert scale questions, allowing respondents to express their level of agreement or disagreement with various statements related to cloud-based accounting security. The use of a Likert scale is particularly useful for quantifying attitudes and perceptions, enabling the study to measure the degree of importance respondents attach to different security measures. This approach ensures that responses can be systematically analyzed and statistically interpreted to draw meaningful conclusions (Ho, 2017).

The questionnaire was carefully structured to ensure clarity and relevance, minimizing the potential for bias or misunderstanding. Each question aligned with the study's objectives to ensure that the data collected is directly applicable to the research hypotheses. For instance, questions on data encryption will assess how respondents perceive its effectiveness in safeguarding sensitive financial information. Similarly, questions on access control mechanisms will evaluate the perceived adequacy of these controls in preventing unauthorized access to accounting systems. Moreover, questions related to backup and recovery will gauge the preparedness of organizations to handle data loss incidents. Compliance-related questions will examine the level of adherence to security standards, while those on user awareness will measure the effectiveness of training programs in preventing security breaches.

3.6. Validity and Reliability

To ensure the validity of the research instrument, content validity was employed. The questionnaire undergo a rigorous review process, including a pilot test with a small group of respondents who are representative of the study population. Feedback from the pilot test was used to refine the questionnaire, ensuring that it accurately captures the concepts being studied. Reliability was assessed using Cronbach's alpha, a statistical measure that evaluates the internal consistency of the questionnaire. A Cronbach's alpha value of 0.7 or higher was considered acceptable, indicating that the questionnaire reliably measures the intended variables.

3.7. Technique of Data Analysis

The data collected from the questionnaires was analyzed using quantitative data analysis techniques. Descriptive statistics such as frequency, percentage, mean and standard deviation was used to summarize the data and provide an overview of the responses. To enable regression analysis and examine relationships between variables, the categorical data collected through the Likert-scale responses were converted into continuous variables by computing the average scores of grouped questions.

Inferential statistical methods such as regression analysis and machine learning approach (Artificial Neural Network) was employed to test hypotheses and examine relationships between variables. The use of SPSS version 27, facilitate the analysis process, ensuring accuracy and efficiency in interpreting the results. This approach help to draw meaningful conclusions and provide actionable insights into the effectiveness and security of cloud-based accounting systems.

3.7.1. Regression Analysis

Regression analysis was employed to investigate the linear relationships between the independent variables (predictors) and the dependent variable (outcome). The study will utilize multiple linear regression analysis, which is appropriate for modeling the relationship between one dependent variable and two or more independent variables. The multiple regression model is specified as follows:

$$SAIS = \alpha_0 + \alpha_1(DE) + \alpha_2(ACM) + \alpha_3(BRP) + \alpha_4(CSS) + \alpha_5(UAT) + \varepsilon$$

Where
β_0 is the intercept
$\beta_1, \ldots, \beta_5$ are the coefficients of the independent variables.
ε is the error term.

Dependent Variable

SAIS = Security of Accounting Information Systems (AIS)

Independent Variables:

DE = Data Encryption
ACM = Access Control Mechanisms
BRP = Backup and Recovery Procedures
CSS = Compliance with Security Standards
UAT= User Awareness and Training

3.7.2. Artificial Neural Network

Artificial Neural Network (ANN) is a machine learning technique modeled after the human brain's neural structure, designed to recognize patterns and improve decision-making processes (Goel, Goel & Kumar, 2023). ANN is particularly useful in financial and accounting systems, where it enhances predictive analytics, anomaly detection, and data security (Sarker, 2023). They are widely used for complex pattern recognition, prediction, and classification tasks, making them suitable for financial data analysis, including cloud-based accounting security and risk assessment. An ANN consists of multiple layers of interconnected nodes (neurons), including an input layer, one or more hidden layers, and an output layer. Each neuron receives weighted inputs, applies an activation function, and transmits the output to the next layer. The network is trained using an optimization algorithm such as backpropagation to minimize the error between predicted and actual values. ANN can be expressed as follows:

For a given neuron j in the hidden or output layer, the activation function is defined as:

$$z_j = \sum_{i=1}^{n} w_{ji} x_i + b_j$$

where:
z_j = weighted sum of inputs for neuron j,
x_i = input from neuron iii in the previous layer,
w_{ji} = weight associated with the connection between neuron i and neuron j,
b_j = bias term for neuron j,
n = number of input neurons.

The output of neuron j is computed using an activation function $f(z_j)$, such as the sigmoid, ReLU, or tanh function:

$$y_j = f(z_j)$$

For example, the sigmoid activation function is defined as:

$$f(z) = \frac{1}{1 + e^{-z}}$$

where e is Euler's number.

During training, ANN adjusts the weights and biases using gradient descent and backpropagation, where the error E is minimized using the loss function:

$$E = \frac{1}{2} \sum (y_{actual} - y_{predicted})^2$$

The weights are updated using the gradient of the error with respect to each weight:

$$w_{ji} = w_{ji} - \eta \frac{\partial E}{\partial w_{ji}}$$

where η is the learning rate.

By iterating through multiple training cycles (epochs), the ANN progressively improves its predictions, making it a powerful tool for detecting anomalies, predicting financial risks, and optimizing security protocols in cloud-based accounting systems.

4. Result

4.1. Descriptive Statistics

Table 1 Summary Statistics

Variables	Mean	Std. Deviation
Security of AIS	4.44	0.582
Data Encryption	3.14	0.815
Access Control Mechanisms	3.10	0.814
Backup and Recovery Procedures	3.04	0.735
Compliance with Security Standards	3.08	0.775
User Awareness and Training	3.08	0.739

Table 1 presents the summary statistics of variables used in the study. The mean value of 4.44 for security of AIS suggests that respondents generally perceive the system as secure, with a relatively low standard deviation of 0.582, indicating a high level of agreement among responses. Data encryption, which is crucial for protecting sensitive financial information, has a mean of 3.14 with a standard deviation of 0.815, suggesting moderate effectiveness but some variability in perception. Similarly, access control mechanisms and compliance with security standards exhibit mean values of 3.10 and 3.08, respectively, with standard deviations of 0.814 and 0.775, reflecting moderate implementation with slight differences in responses. The mean score for backup and recovery procedures is 3.04 (SD = 0.735), indicating that while backup protocols are in place, their effectiveness vary. Lastly, user awareness and training, which plays a crucial role in mitigating security risks, also has a mean of 3.08 (SD = 0.739), suggesting that while training programs exist, they may not be uniformly effective across all users.

4.2. OLS Regression Techniques

Table 2 Model Summary

R	R Square	Adjusted R Square	Std. Error	Durbin-Watson
0.744	0.554	0.548	0.391	1.927

Table 2 presents the model summary, which evaluates the strength and explanatory power of the regression model. The R-value of 0.744 indicates a strong positive correlation between the independent variables and the dependent variable, suggesting a substantial relationship. The R Square (0.554) shows that approximately 55.4% of the variation in the dependent variable is explained by the independent variables, demonstrating a moderate to high level of explanatory power. The Adjusted R Square (0.548), which accounts for the number of predictors in the model, is slightly lower than the R Square, indicating that the model remains robust even after adjusting for potential overfitting. The standard error of 0.391 suggests the extent of deviation in the observed values from the predicted values, implying a reasonably good fit of the model. Lastly, the Durbin-Watson statistic of 1.927 is close to the ideal value of 2, signifying that there is no significant autocorrelation in the residuals, confirming the reliability of the model's estimations.

Table 3 ANOVA

Source of Variation	Sum of Squares	df	Mean Square	F	P-value
Regression	65.787	5	13.157	85.961	0.000
Residual	52.96	346	0.153		
Total	118.747	351			

Table 3 presents the ANOVA results to determine the statistical significance of the regression model. The **p-value of 0.000** indicates that the model is statistically significant at 5% level. This suggests that the model is fit which implies that there is linear relationship between the dependent variable and the independent variables.

Table 4 Coefficients

Security of AIS	B	Std. Error	t-statistic	P-value
(Constant)	1.148	0.191	6.023	0.000
Data Encryption	0.36	0.026	13.963	0.000
Access Control Mechanisms	0.323	0.026	12.538	0.000
Backup and Recovery Procedures	0.198	0.029	6.924	0.000
Compliance with Security Standards	0.164	0.027	6.075	0.000
User Awareness and Training	0.017	0.028	0.591	0.555

Table 4 presents the regression coefficients assessing the impact of various security measures on the security of cloud-based accounting information systems. The results show that data encryption (B = 0.36, p = 0.000) significantly enhances security of AIS, supporting H1 and confirming its critical role in safeguarding cloud-based accounting systems.

Similarly, access control mechanisms (B = 0.323, p = 0.000) have a positive and significant impact on the security of AIS, validating H2 and emphasizing their necessity in restricting unauthorized access. Backup and recovery procedures (B = 0.198, p = 0.000) are also significantly associated with improved security of AIS, confirming H3, as effective data recovery minimizes risks of data loss. Additionally, compliance with security standards (B = 0.164, p = 0.000) has a statistically significant effect on security of AIS, supporting H4 by reinforcing the importance of regulatory adherence in enhancing system security. However, user awareness and training (B = 0.017, p = 0.555) does not significantly influence security, leading to the rejection of H5, suggesting that while awareness programs are essential, their direct effect on security might be limited compared to technical controls.

Table 5 Collinearity Statistics

Tolerance	VIF
0.989	1.011
0.993	1.007
0.987	1.013
0.995	1.005
0.995	1.005

Table 5 presents the collinearity statistics, specifically Tolerance and the Variance Inflation Factor (VIF), which assess the presence of multicollinearity among the independent variables. The Tolerance values range from 0.987 to 0.995, while the VIF values remain between 1.005 and 1.013, indicating an absence of significant multicollinearity. Since VIF values below 10 and Tolerance values above 0.1 suggest that predictor variables are not highly correlated, the results confirm that the independent variables used in this study—data encryption, access control mechanisms, backup and recovery procedures, compliance with security standards, and user awareness and training—are sufficiently independent of each other. This implies that the regression model is well-specified, and the estimated coefficients are reliable for interpretation without concerns of multicollinearity bias.

4.3. Artificial Neural Network

Table 6 Variable Importance

Variables	Importance	Normalized Importance
Data Encryption	0.292	100.00%
Access Control Mechanisms	0.27	92.60%
Backup and Recovery Procedures	0.175	59.80%
Compliance with Security Standards	0.212	72.50%
User Awareness and Training	0.051	17.40%

Training Relative Error: 0.456; Testing Relative Error: 0.459

Table 6 presents the variable importance analysis in the Artificial Neural Network (ANN) model, highlighting the relative contributions of each predictor to the security of cloud-based accounting information systems. Data encryption emerges as the most influential factor, with an importance score of 0.292 and a normalized importance of 100%, indicating its critical role in enhancing system security. Access control mechanisms follow closely with an importance of 0.27 (92.60%), suggesting that effective authentication and authorization protocols significantly impact system protection. Compliance with security standards (0.212, 72.50%) and backup and recovery procedures (0.175, 59.80%) also play substantial roles, underscoring the need for adherence to regulatory frameworks and data redundancy measures. However, user awareness and training exhibit the lowest importance (0.051, 17.40%), implying a relatively weaker influence on system security compared to technical safeguards. The training and testing relative errors of 0.456 and 0.459, respectively, indicate a well-fitted ANN model with minimal error, confirming the reliability of these findings in predicting security effectiveness in cloud-based accounting systems.

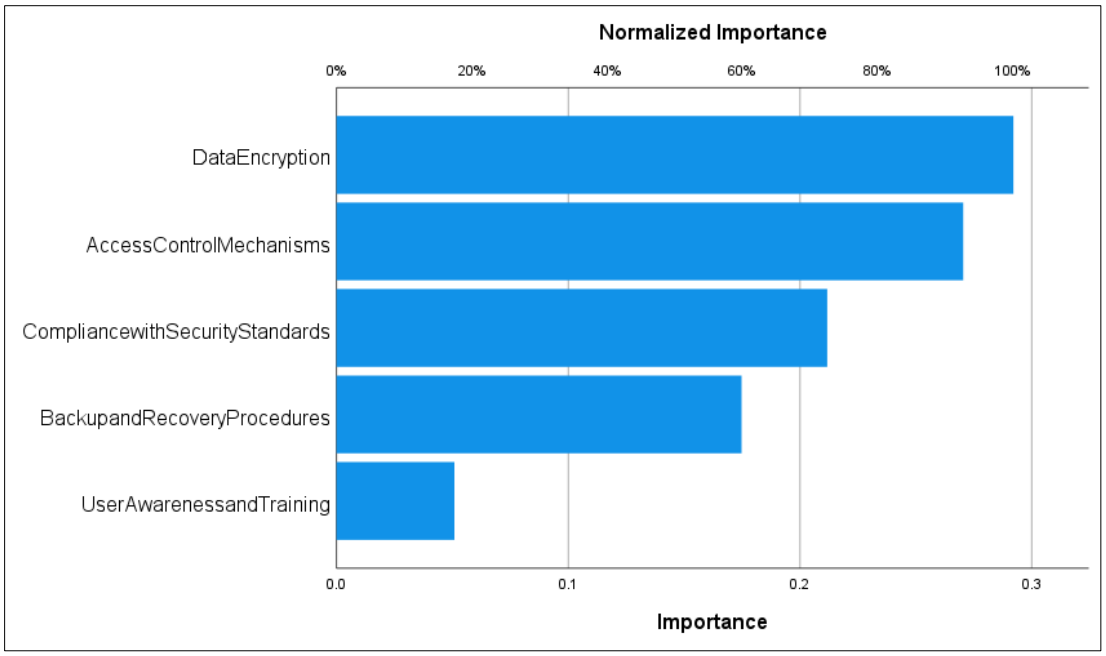

Figure 1 Independent Variable Importance Plot

Figure 1 presents the Independent Variable Importance Plot, visually depicting the relative contributions of different security measures to the protection of cloud-based accounting information systems. Data encryption emerges as the most critical factor, with the highest importance score, reinforcing its role in safeguarding sensitive financial data. Access control mechanisms follow closely, indicating the significance of authentication and authorization in preventing unauthorized access. Compliance with security standards and backup and recovery procedures also play substantial roles, highlighting the need for regulatory adherence and data redundancy strategies in mitigating security risks. However, user awareness and training exhibit the lowest importance, suggesting that while essential, human factors may have a lesser direct impact compared to technical security measures. This visualization aligns with the statistical findings, emphasizing the necessity of robust encryption, stringent access control, and compliance enforcement to enhance the security of cloud-based accounting information systems.

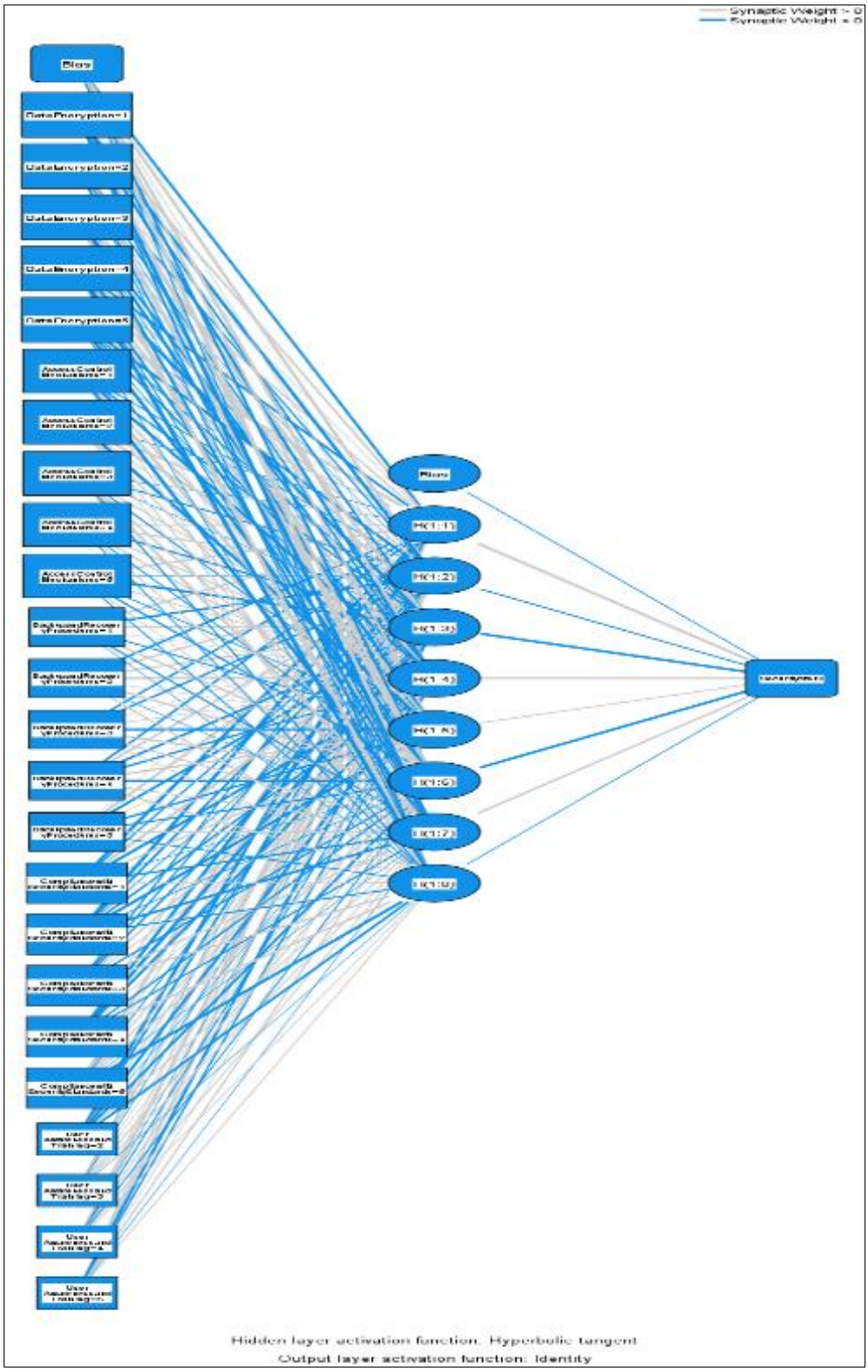

Figure 2 Artificial Neural Network Diagram

Figure 2 presents an Artificial Neural Network (ANN) Diagram, illustrating the complex relationships between input variables and the predicted security effectiveness of cloud-based accounting systems. The network comprises multiple input nodes representing security measures such as data encryption, access control mechanisms, backup and recovery procedures, compliance with security standards, and user awareness and training. These inputs are processed through a hidden layer consisting of eight neurons (H(1:1) to H(1:8)), where weighted connections apply transformations using a hyperbolic tangent activation function to model non-linear relationships. The synaptic weights, represented by blue

and gray lines, indicate the strength and direction of influence between variables. Finally, the output node represents the predicted security effectiveness, employing an identity activation function to generate a continuous output. The diagram highlights the ANN's ability to capture complex interactions among security factors, reinforcing the importance of technical and compliance-based security strategies in safeguarding cloud-based accounting information systems.

5. Discussion of Findings

The findings of this study provide a comprehensive understanding of the factors influencing the security of cloud-based accounting information systems, integrating both regression and artificial neural network (ANN) analyses to validate the significance of key security measures. The regression results indicate that data encryption, access control mechanisms, backup and recovery procedures, and compliance with security standards significantly enhance security, whereas user awareness and training do not have a statistically significant effect. The ANN model further corroborates these findings, ranking data encryption as the most critical factor, followed by access control mechanisms, compliance with security standards, and backup and recovery procedures, while user awareness and training exhibit the least importance. The model summary confirms the robustness of the regression model, with an R-squared value of 55.4%, indicating that more than half of the variation in security effectiveness is explained by the independent variables. Additionally, the absence of multicollinearity ensures the reliability of the results, while the ANN model's low training and testing errors further validate the predictive accuracy of the findings. The findings of this study align with existing literature (such as Akanbi & Akanbi (2022); Olokunde & Adekola (2022); Ofoegbu & Olawale (2021)) on cloud-based accounting information system security, reinforcing the significance of technical safeguards in mitigating cyber threats.

6. Conclusion

The study concludes that the security of cloud-based accounting information systems is predominantly influenced by technical security measures, with data encryption, access control mechanisms, compliance with security standards, and backup and recovery procedures playing significant roles in enhancing system protection. The regression analysis establishes a strong positive correlation between these factors and security effectiveness, while the artificial neural network (ANN) model further confirms their relative importance, ranking data encryption as the most critical safeguard. The absence of multicollinearity in the regression model ensures the reliability of the findings, and the ANN model's minimal error rates validate the robustness of the predictive analysis. Notably, user awareness and training do not exhibit a statistically significant impact, suggesting that while essential, human interventions alone may not be sufficient in mitigating security risks without strong technical defenses.

6.1. Recommendations

Based on the findings of this study, the following recommendations are proposed:

- Organizations should prioritize strong encryption protocols to safeguard sensitive financial data stored in cloud-based accounting information systems.
- Multi-factor authentication, role-based access control, and strict authorization policies should be enforced to prevent unauthorized access to accounting information.
- Regular automated backups and well-defined disaster recovery plans should be established to minimize data loss and ensure business continuity.
- Regular security evaluations should be conducted to identify vulnerabilities and strengthen system defenses against emerging cyber threats.

Compliance with ethical standards

Disclosure of conflict of interest

The author declares that there is no conflict of interest related to this research between the authors.

References

[1] Adeoye, S., & Alhassan, F. (2021). Cybersecurity Threats in Cloud Computing: Implications for Nigerian Financial Institutions. Journal of Information Systems, 35(2), 233-248.

[2] Akanbi, O. M., & Akanbi, C. O. (2022). Cloud Computing in Nigeria: Adoption, Challenges, and Future Directions. International Journal of Technology Management and Information Systems, 7(1), 112-125.

[3] Alshamaileh, Y., Papagiannidis, S., & Li, F. (2018). Cloud Computing Adoption by SMEs in the UAE: Influencing Factors and Challenges. Journal of Enterprise Information Management, 31(2), 210-235.

[4] Amron, M. T., & Noh, N. M. (2021). Technology acceptance model (TAM) for analysing cloud computing acceptance in higher education institution (HEI). In IOP Conference Series: Materials Science and Engineering (Vol. 1176, No. 1, p. 012036). IOP Publishing.

[5] Bhadouria, A. S. (2022). Study of: impact of malicious attacks and data breach on the growth and performance of the company and few of the world's biggest data breaches. International Journal of Scientific and Research Publications, 10(10), 1-11.

[6] Brown, C., & Thompson, J. (2022). The Future of Cloud Accounting: Trends and Innovations. Journal of Financial Innovation, 18(2), 123-135.

[7] Castellani, D., Mariotti, S., & Piscitello, L. (2022). SMEs and cloud-based financial management systems. Small Business Economics, 58(2), 215-233.

[8] Davis, F. D. (1989). Technology acceptance model: TAM. Al-Suqri, MN, Al-Aufi, AS: Information Seeking Behavior and Technology Adoption, 205(219), 5.

[9] Goel, A., Goel, A. K., & Kumar, A. (2023). The role of artificial neural network and machine learning in utilizing spatial information. Spatial Information Research, 31(3), 275-285.

[10] Grand View Research. (2022). Cloud Accounting Software Market Size, Share & Trends Analysis Report By Deployment (Public, Private, Hybrid), By Application (SMEs, Large Enterprises), By End-use (BFSI, IT & Telecom, Retail), And Segment Forecasts, 2022 - 2028. Retrieved from https://www.grandviewresearch.com

[11] Gupta, A., & Sharman, R. (2021). Enhancing Cloud Security: Technologies and Strategies. Journal of Information Systems Security, 28(4), 456-478.

[12] Hassan, R., Ali, K., & Noor, S. (2022). Data encryption techniques in cloud-based accounting. Cloud Security Journal, 15(4), 233-248.

[13] Ho, G. W. (2017). Examining perceptions and attitudes: A review of Likert-type scales versus Q-methodology. *Western journal of nursing research*, *39*(5), 674-689.

[14] Huang, Y., & Pearlson, K. (2021). Understanding the Human Factor in Cybersecurity: A Conceptual Framework for Managing User Behavior. Journal of Cybersecurity Research, 5(1), 33-49.

[15] Isibor, E. (2024). Regulation of Healthcare Data Security: Legal Obligations in A Digital Age. Available at SSRN 4957244.

[16] Jensen, M. C., & Meckling, W. H. (2020). Theory of the Firm: Managerial Behavior, Agency Costs, and Ownership Structure. Journal of Financial Economics, 3(4), 305-360.

[17] Johnson, R., Jones, M., & Wang, T. (2021). Multi-Factor Authentication: Enhancing Security in the Cloud. Cybersecurity Journal, 9(2), 101-115.

[18] Jones, A. (2020). The Rise of Cloud-Based Accounting Systems: An Overview. Journal of Modern Accounting, 14(1), 21-34.

[19] Jones, K. R., Gwynn, E. P., & Teeter, A. (2019). Quantitative or qualitative: Selecting the right methodological approach for credible evidence. *Journal of Human Sciences and Extension*, *7*(2), 5.

[20] Kesa, D. M. (2023). Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations. World Journal of Advanced Research and Reviews, 18(3), 970-992.

[21] Kumar, R., & Kaur, J. (2021). Data Breaches in Cloud Computing: A Review and Future Research Directions. International Journal of Cloud Computing, 19(3), 205-220.

[22] Lun, L., Zetian, D., Hoe, T. W., Juan, X., Jiaxin, D., & Fulai, W. (2024). Factors influencing user intentions on interactive websites: Insights from the technology acceptance model. IEEE Access.

[23] Marquis, Y. A. (2024). From theory to practice: Implementing effective role-based access control strategies to mitigate insider risks in diverse organizational contexts. Journal of Engineering Research and Reports, 26(5), 138-154.

[24] Maelah, R., Al Lami, M. F. F., & Ghas, G. (2021). Usefulness of management accounting information in decision making among SMEs: the moderating role of cloud computing. *Asia-Pasific Management Accounting Journal*, *16*(1), 59-92.

[25] Mell, P., & Grance, T. (2021). The NIST Definition of Cloud Computing. National Institute of Standards and Technology. Retrieved from https://www.nist.gov

[26] Ofoegbu, G. N., & Olawale, Y. T. (2021). Adoption of Cloud Computing Accounting Systems by SMEs in Nigeria: A Survey of Challenges and Benefits. International Journal of Cloud Applications and Computing, 11(2), 45-61.

[27] Ojedokun, A. (2022). Data Protection Regulations and Compliance in Nigeria: An Overview of NDPR. Journal of Privacy and Data Protection, 6(4), 191-207.

[28] Okere, I., & Asika, N. (2021). The Impact of Cloud Computing on Nigerian Businesses: An Empirical Study. Journal of Information Technology and Business Management, 12(1), 89-103.

[29] Olokunde, E., & Adekola, P. (2022). Challenges of Cloud Computing Adoption in Nigeria. International Journal of Cloud Computing and Services Science, 11(1), 23-30.

[30] Onayemi, A., Mugabe, R., & Turyakira, P. (2022). Factors influencing cloud computing adoption among SMEs in Kampala, Uganda: A diffusion of innovation perspective. African Journal of Business Technology, 8(2), 45–61.

[31] Rogers, E. M. (2003). Diffusion of innovations (5th ed.). Free Press.

[32] Rouse, M. (2021). Understanding Compliance Standards for Cloud Security. TechTarget. Retrieved from https://www.techtarget.com

[33] Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. Annals of Data Science, 10(6), 1473-1498.

[34] Sastararuji, D., & Hoonsopon, D. (2020). The impact of diffusion of innovation factors on cloud accounting adoption among SMEs: An integrated model. International Journal of Business Innovation and Research, 23(1), 112–134.

[35] Smith, A., & Rupp, W. (2021). Benefits and Risks of Cloud-Based Accounting: A Review. Journal of Business and Technology, 25(4), 341-355.

[36] Smith, R., Wang, J., & Patel, N. (2021). Effective Backup Strategies for Cloud-Based Systems. Journal of Information Technology, 19(2), 221-238.

[37] Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2021). User Awareness and its Impact on Cybersecurity: A Review of the Literature. Journal of Cybersecurity, 7(1), 1-12.

[38] Tahmid, M. (2023). Accounting in the cloud: a new era of streamlining accounting with cloud technology. Journal of Cloud Computing, 1, 1-14.

[39] Verizon Data Breach Investigations Report. (2022). 2022 Data Breach Investigations Report. Verizon Enterprise Solutions. Retrieved from https://www.verizon.com

[40] Wang, T., Li, X., & Kim, J. (2021). Impact of Data Breaches on Financial Performance of Companies. Journal of Information Systems, 35(1), 1-18.