Cybersecurity Threats in Cloud Accounting: A Case Study of Microfinance Banks in Anambra State Using NAMBUIT Banking Software

***Arinze E. Anaege[1], Onyinye M. Eneh[2], Onyekachi A. Inweregbu[1], Sopuruchukwu P. Okwuego[1]**

[1]Department of Accounting, Kingsley Ozumba Mbadiwe University, Ideato, Nigeria

[2]Department of Accountancy, Nnamdi Azikiwe University, Awka, Nigeria

DOI: https://doi.org/10.51584/IJRIAS.2025.10030021

Received: 25 February 2025; Accepted: 01 March 2025; Published: 02 April 2025

ABSTRACT

This study investigates the effect of cybersecurity threats on the operational efficiency and regulatory compliance of microfinance banks (MFBs) in Anambra State, Nigeria, with a particular focus on MFBs that use the National Association of Microfinance Banks Unified Information Technology (NAMBUIT) cloud accounting platform. As cloud accounting becomes increasingly vital for MFBs due to its benefits, such as real-time data access and reduced IT costs, it also brings heightened cybersecurity risks that can disrupt daily operations and erode customer trust. Through a combination of quantitative analysis and literature review, the study reveals that while current cybersecurity measures provide some level of protection, they are not sufficient to fully mitigate the threats faced by these institutions. The research underscores the need for more robust cybersecurity frameworks, continuous employee training, and stronger regulatory compliance to safeguard the financial operations of MFBs. The findings suggest that balancing the adoption of innovative cloud technologies with enhanced cybersecurity practices is essential for the sustained growth and security of the microfinance sector in Nigeria. Recommendations for improving cybersecurity measures and ensuring better alignment with regulatory standards are provided.

Keywords: Cybersecurity, Cloud Accounting, Microfinance Banks, NAMBUIT, Disruptive Technologies

INTRODUCTION

Background

In recent years, cloud accounting has become increasingly integral to the financial sector, offering scalable, cost-effective, and accessible solutions for managing financial data. Cloud accounting allows businesses to store their financial information on remote servers, enabling real-time access and collaboration across different geographical locations (Saad et al., 2022). This technological shift has been particularly beneficial for small and medium-sized enterprises (SMEs) and Microfinance Banks (MFBs) in emerging economies like Nigeria, where resource constraints often limit the adoption of traditional, on-premise accounting software (Aladejebi, 2019). The National Association of Microfinance Banks Unified Information Technology (NAMBUIT) is a cloud-based accounting and banking solution developed by INLAKS with the support of the Central Bank of Nigeria (CBN) and widely adopted by MFBs in Nigeria. NAMBUIT is designed to cater to the specific needs of MFBs, providing functionalities such as core banking, loan management, and regulatory reporting (INLAKS, 2018). The software's relevance in the Nigerian context is underscored by its alignment with the country's regulatory requirements and its support for the Central Bank of Nigeria's initiatives to enhance financial inclusion through microfinance institutions. As the digital transformation of the microfinance sector continues, the adoption of NAMBUIT has significantly improved operational efficiency and service delivery among MFBs in Nigeria (INLAKS, 2020).

The adoption of cloud accounting has revolutionized financial management in microfinance banks (MFBs), offering benefits such as real-time access to financial data, reduced IT infrastructure costs, and improved

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

operational efficiency (Saad et al., 2022). However, the increasing reliance on cloud-based solutions also exposes these institutions to heightened cybersecurity risks, including data breaches, unauthorized access, malware attacks, and regulatory compliance challenges (Dawood et al., 2023). Microfinance banks in Nigeria have increasingly adopted cloud-based banking and accounting software. While this platform enhances financial inclusion and digital transformation, the level of cybersecurity resilience among MFBs using NAMBUIT remains uncertain. Existing literature on cybersecurity threats in cloud accounting has largely focused on broader financial institutions (Abioye et al., 2021; Akintoye et al., 2022), with limited research addressing the specific vulnerabilities faced by microfinance banks in Nigeria. Moreover, the effectiveness of current cybersecurity measures implemented by these institutions has not been comprehensively evaluated. The unique environment of Nigerian MFBs, characterized by varying levels of digital literacy and cybersecurity infrastructure, exacerbates these risks, making it imperative to investigate the specific challenges they face (Soetan & Mogaji, 2024).

Without a clear understanding of the cybersecurity threats and mitigation strategies within the context of cloud-based microfinance operations, MFBs risk operational disruptions, financial losses, regulatory penalties, and loss of customer trust. This study seeks to bridge this gap by investigating the cybersecurity threats faced by MFBs in Anambra State using NAMBUIT software, assessing the impact on operational efficiency and regulatory compliance, and evaluating the adequacy of existing cybersecurity measures. The findings will provide insights for strengthening cybersecurity frameworks and ensuring regulatory alignment in Nigeria's microfinance sector.

Research Objectives

The objective of the study is to explore the cybersecurity challenges associated with cloud accounting, focusing on Microfinance Banks (MFBs) in Anambra State that use the NAMBUIT banking software.

Specifically, this study will achieve the following objectives:

1. To investigate the cybersecurity threats faced by Microfinance Banks in Anambra State that use NAMBUIT banking software.

2. To evaluate the effect of these cybersecurity threats on the operations and regulatory compliance of the selected banks.

3. To identify the measures currently in place to mitigate these cybersecurity threats, and how effective they are.

Research Questions

The study seeks to answer the following research questions:

1. What are the most common cybersecurity threats encountered by Microfinance Banks using NAMBUIT in Anambra State?

2. How do these cybersecurity threats affect the operational efficiency and compliance of the selected banks?

3. What measures are currently in place to mitigate these cybersecurity threats, and how effective are they?

Significance of the Study

The significance of this study lies in its potential contributions to the accounting profession, the microfinance sector, and regulatory bodies in Nigeria. For the accounting profession, understanding the cybersecurity challenges associated with cloud accounting is crucial for developing best practices and guidelines that ensure data integrity and security. The findings of this study will provide valuable insights for MFBs, particularly in Anambra State, enabling them to enhance their cybersecurity frameworks and safeguard their operations against potential threats. Moreover, the study will offer recommendations for policymakers and regulators to strengthen

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

the cybersecurity infrastructure within the Nigerian financial sector, ensuring that the benefits of digital transformation are not undermined by security vulnerabilities.

LITERATURE REVIEW

Conceptual Review

Cloud Accounting in the Financial Sector

Cloud accounting refers to the use of cloud-based technology to manage, process, and store financial data (Coman et al., 2022). Unlike traditional accounting systems that require software installation on local computers or servers, cloud accounting solutions operate on remote servers, allowing users to access financial data from anywhere with an internet connection (Saad et al., 2022). This flexibility is one of the key advantages of cloud accounting, making it particularly valuable for businesses that need to access financial data across multiple locations or by various stakeholders (Chauhan & Shiaeles, 2023).

The importance of cloud accounting in the financial sector is profound. First, it reduces the need for significant upfront investment in IT infrastructure, as the cloud provider typically manages the hardware and software. This is particularly beneficial for small and medium-sized enterprises (SMEs) and startups that may have limited resources. Additionally, cloud accounting solutions often come with regular updates and maintenance provided by the service provider, ensuring that businesses are always using the latest technology without needing in-house IT support (Petcu, Sobolevschi-David, & Curea, 2024).

Another critical aspect of cloud accounting is the real-time access to financial data it provides. Coman et al. (2022) noted that this real-time capability allows for up-to-date financial reporting and decision-making, which is crucial in today's fast-paced business environment. It also facilitates better collaboration, as multiple users can access and work on the same data simultaneously, streamlining workflows and improving efficiency. Moreover, cloud accounting enhances data security through features such as encryption, automated backups, and disaster recovery options, which are often more robust than those found in traditional accounting systems (Dawood et al., 2023).

Adoption of Cloud Accounting in the Nigerian Microfinance Sector

The Nigerian microfinance sector plays a pivotal role in promoting financial inclusion, particularly for underserved populations such as low-income individuals and small businesses. In recent years, there has been a growing trend toward the adoption of cloud accounting solutions within this sector. This shift has been driven by the need to improve operational efficiency, reduce costs, and enhance service delivery (Zheng, Huang, Wang, & Li, 2023). Cloud accounting offers numerous advantages for Microfinance Banks (MFBs) in Nigeria. These institutions often operate with limited resources, and cloud-based solutions provide a cost-effective alternative to traditional accounting software. Additionally, the ability to access financial data from anywhere is particularly useful for MFBs that serve clients in remote or rural areas, allowing for more timely and accurate financial management (Isern et al., 2009).

Despite the benefits, the adoption of cloud accounting in the Nigerian microfinance sector is not without challenges. One significant barrier is the limited access to reliable internet, particularly in rural areas (Mhlongo et al., 2024). Additionally, there is a level of apprehension regarding data security and privacy, which has slowed adoption rates among some MFBs (Dahiru & Abubakar, 2018). However, as digital infrastructure improves and awareness of cloud accounting's benefits grows, more MFBs are expected to adopt these solutions. The use of platforms like NAMBUIT, a cloud-based software tailored for Nigerian MFBs, exemplifies this growing trend and highlights the potential for cloud accounting to transform the microfinance sector in Nigeria.

Cloud Accounting as a Disruptive Technologies

Disruptive technologies continue to reshape traditional accounting practices and have seen the introduction of new methods, tools, and paradigms that are redefining the profession. Technologies such as artificial intelligence (AI), blockchain, robotic process automation (RPA), and cloud computing have significantly transformed the

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

way accounting tasks are performed, leading to greater efficiency, accuracy, and real-time decision-making (Hashid & Almaqtari, 2024).

Cloud computing has revolutionized how accounting data is stored, accessed, and processed (Akpan, 2024). Moving accounting systems to the cloud allows organizations to access financial information from any location, collaborate in real-time, and scale their operations without the need for extensive IT infrastructure (Akpan, 2024). This has been especially beneficial for small and medium-sized enterprises (SMEs) and microfinance institutions, which often have limited resources and cannot afford expensive on-site IT infrastructure (Pramuka & Pinasti, 2020). Cloud-based systems also enhance data accessibility and enable multiple stakeholders to work on the same financial data simultaneously, streamlining workflows and increasing productivity (Pramuka & Pinasti, 2020).

However, while disruptive technologies such as cloud computing offer many advantages, they also pose challenges. There is a growing need for accountants to upskill and adapt to new tools and processes, and organizations must invest in training to ensure employees can utilize these technologies effectively (Pramuka & Pinasti, 2020). Additionally, data security concerns remain a key issue as financial information stored in the cloud is more vulnerable to cyber threats (Dawood et al., 2023). The rise of automation also raises concerns over job displacement, as many routine accounting tasks are now performed by machines, potentially reducing the demand for traditional roles in the accounting profession (Dawood et al., 2023). Despite these challenges, the benefits of automation, transparency, and accessibility continue to drive the adoption of disruptive technologies in accounting practices.

Overview and Functionality of NAMBUIT in the Context of MFBs

NAMBUIT is a cloud-based core banking and accounting software solution specifically designed to meet the needs of microfinance banks (MFBs) in Nigeria (INLAKS, 2020). It was developed with a focus on addressing the unique challenges faced by MFBs, which often operate with limited resources, infrastructure, and access to technology. The platform integrates essential banking operations with advanced accounting functionalities within a secure cloud environment, offering a solution that is both scalable and cost-effective for financial institutions operating in underserved areas. One of the main advantages of NAMBUIT is its modular design, which allows MFBs to manage various aspects of their operations seamlessly (INLAKS, 2020). These modules include loan management, savings accounts, customer relationship management (CRM), and regulatory reporting, which ensure that MFBs can deliver a full range of financial services to their clients (INLAKS, 2020). The loan management module is particularly useful for microfinance institutions, as it enables banks to track loan performance, manage repayments, and assess borrower creditworthiness. This ensures better loan portfolio management and helps reduce default rates (INLAKS, 2020).

Another important feature of NAMBUIT is its multi-branch support. Due to the fact that many MFBs in Nigeria have branches in rural areas with limited banking infrastructure, the software allows these institutions to manage their operations across multiple locations from a single platform. This centralized management system facilitates smoother coordination between branches and ensures that financial data is readily accessible, regardless of location (Dahiru & Abubakar, 2018). The software also offers real-time data processing and reporting, a feature critical for microfinance institutions that need to generate accurate financial statements and meet regulatory requirements efficiently. With real-time access to financial data, MFBs can ensure timely reporting and better decision-making. This also supports compliance with regulatory frameworks such as the Central Bank of Nigeria's (CBN) guidelines, as MFBs are required to submit regular reports to maintain operational licenses (INLAKS, 2020).

Security is a significant concern for MFBs, particularly when dealing with sensitive customer data. NAMBUIT addresses this by incorporating robust security measures, including data encryption, secure access protocols, and automated backups (INLAKS, 2020). The cloud-based nature of the software ensures that data is stored securely and can be easily recovered in the event of system failures or cyber threats, reducing the risk of data loss (Reis et al., 2024). The adoption of NAMBUIT among Nigerian MFBs has been growing steadily, with more institutions recognizing the advantages of integrating their core banking and accounting operations into a single, streamlined system. Its ability to enhance operational efficiency, reduce costs, and improve service delivery has

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

made it a popular choice for MFBs seeking to expand their reach to underserved populations in Nigeria (INLAKS, 2018).

Banks Regulatory Framework in Relation to Cybersecurity

Nigeria's regulatory framework concerning cybersecurity in financial institutions has evolved in response to the increasing reliance on digital and cloud-based technologies within the sector (Reis, Oliha, Osasona, & Obi, 2024). The primary regulatory body overseeing cybersecurity in the financial sector is the Central Bank of Nigeria (CBN), which has issued several guidelines and frameworks to ensure the security and integrity of financial data and systems. One of the key regulations is the CBN's Risk-Based Cybersecurity Framework, issued in 2022, which mandates financial institutions, including microfinance banks, to implement robust cybersecurity measures (CBN, 2022). This framework requires institutions to conduct regular risk assessments, develop comprehensive cybersecurity policies, and ensure that their systems are resilient against cyber threats. Additionally, the CBN emphasizes the importance of incident response plans, which are critical for mitigating the effect of cyberattacks and ensuring business continuity (CBN, 2022).

Another significant regulation is the Nigeria Data Protection Regulation (NDPR), introduced by the National Information Technology Development Agency (NITDA) in 2019 (NITDA, 2019). The NDPR aims to protect personal data and ensure that financial institutions handle customer information securely. Compliance with the NDPR is crucial for MFBs using cloud-based systems like NAMBUIT, as it governs how data is stored, processed, and transferred, particularly in a cloud environment (NITDA, 2019). These regulatory frameworks highlight Nigeria's commitment to enhancing cybersecurity in the financial sector, ensuring that institutions, including MFBs, are equipped to handle the risks associated with digital transformation.

Hypotheses Development

The growing reliance on cloud accounting in microfinance banks has introduced significant cybersecurity challenges (Dawood et al., 2023). Studies have shown that cloud-based financial systems are vulnerable to data breaches, malware attacks, and unauthorized access, which can compromise operational efficiency and regulatory compliance (Chauhan & Shiaeles, 2023). In the Nigerian microfinance sector, cybersecurity concerns are heightened due to variations in digital literacy, inadequate security infrastructure, and evolving cyber threats (Soetan & Mogaji, 2024). Prior research suggests that while cybersecurity frameworks exist, their effectiveness in mitigating threats remains a subject of debate (Mhlongo et al., 2024). Therefore, this study tests the following hypotheses:

H_{o1}: Cybersecurity threats do not significantly affect the operations of Microfinance Banks in Anambra State using NAMBUIT.

H_{o2}: Cybersecurity threats do not significantly affect the operational efficiency and regulatory compliance of the selected banks.

H_{o3}: The current cybersecurity measures implemented by these banks are insufficient in mitigating the identified threats.

RESEARCH METHODOLOGY

Research Design

The research adopts a descriptive and exploratory approach to investigate the cybersecurity threats associated with the use of cloud accounting systems, specifically NAMBUIT, in microfinance banks (MFBs) within Anambra State. A descriptive design is appropriate for this study as it allows for a detailed examination of the current state of cybersecurity threats faced by these institutions. The exploratory aspect enabled the identification of potential risks and vulnerabilities that may not have been fully explored in previous studies. This dual approach provides a comprehensive understanding of the cybersecurity landscape as it pertains to cloud accounting in the microfinance sector. The descriptive component focused on quantifying the extent of

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

cybersecurity threats and their effect on MFB operations, while the exploratory component delved into the specific types of threats and the effectiveness of existing mitigation strategies.

Population

The study's population consisted of the managing directors, heads of operations, and internal auditors from the six MFBs in Anambra State that are currently using NAMBUIT software. These individuals are considered key informants due to their direct involvement in the management, operational oversight, and audit functions within their respective banks. The total population for this study is therefore 18 respondents, comprising 6 managing directors, 6 heads of operations, and 6 internal auditors. The sample for this study was drawn from this entire population, ensuring that all relevant stakeholders are included in the research. The decision to include all members of this population is driven by the relatively small number of MFBs using NAMBUIT in Anambra State and the need to gather comprehensive insights from all the key decision-makers within these institutions.

The selection criteria for respondents are based on their roles within the MFBs, as these positions are most likely to have direct knowledge of the cybersecurity measures in place, the challenges encountered, and the effect of these challenges on the banks' operations. The managing directors are responsible for overall governance, the heads of operations oversee daily activities including the use of accounting systems, and the internal auditors ensure compliance with regulatory standards and internal controls.

Data Collection Method

Data was collected using structured questionnaires designed to capture both the breadth and depth of information required for this study. The questionnaire includeD closed-ended questions, which will provide quantifiable data on the frequency and types of cybersecurity threats encountered. The questionnaire was divided into several sections, including demographic information, the extent of NAMBUIT usage, types of cybersecurity threats encountered, measures in place to combat these threats, and the perceived effectiveness of these measures. The design of the questionnaire was informed by existing literature on cybersecurity in cloud computing and tailored to the specific context of microfinance banks in Nigeria.

Ethical considerations will be of paramount importance in this study. All participants were informed of the purpose of the research, the voluntary nature of their participation, and their right to withdraw at any time without consequence. Informed consent was obtained from all respondents prior to their participation. The confidentiality of respondents was maintained by ensuring that data is anonymized and securely stored. No identifying information was disclosed in the reporting of the study's findings, and data was used solely for academic purposes.

Data Analysis Techniques

The collected data was analyzed using a combination of descriptive statistics, frequency analysis, and a one-sample t-test. Descriptive statistics was used to summarize the demographic characteristics of the respondents, the extent of NAMBUIT usage, and the frequency and types of cybersecurity threats reported. This include measures such as mean, median, mode, and standard deviation to provide a clear picture of the central tendencies and dispersion of the data.

Frequency analysis was employed to identify the most common cybersecurity threats faced by the MFBs, as well as the most frequently used mitigation strategies. This helped in understanding the prevalence of different types of threats and the extent to which certain measures are being implemented across the sampled banks.

A one-sample t-test was conducted to determine whether the cybersecurity measures in place at the MFBs are statistically significant in mitigating the threats identified. This test compared the mean effectiveness score of the cybersecurity measures against a hypothesized population mean to ascertain whether the measures are effective enough to protect the banks' operations. The t-test provided insights into the reliability of the current cybersecurity strategies and whether they require further enhancement.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

Limitations of the Study

While this study provides comprehensive insights into cybersecurity threats in cloud accounting within microfinance banks in Anambra State, it is important to acknowledge certain limitations.

Firstly, the study is limited to MFBs using NAMBUIT software in a single state (Anambra), which may affect the generalizability of the findings to other regions or financial institutions using different cloud accounting systems. The focus on one software solution may also limit the applicability of the findings to other cloud-based accounting platforms with different security architectures.

Secondly, the reliance on self-reported data from the managing directors, heads of operations, and internal auditors may introduce response bias, as respondents may underreport the extent of cybersecurity threats or overstate the effectiveness of their mitigation strategies due to concerns about reputational risk or regulatory scrutiny.

Lastly, the study's cross-sectional design, which captures data at a single point in time, may not fully account for the dynamic nature of cybersecurity threats, which evolve rapidly. This limitation may affect the study's ability to capture emerging threats that have not yet been widely recognized or reported by the respondents.

Despite these limitations, the study's findings will provide valuable insights into the current state of cybersecurity in cloud accounting within the Nigerian microfinance sector, offering a foundation for future research and the development of more robust security measures.

Data Analysis

Descriptive Statistics

Table 1: Cybersecurity Threat

Cybersecurity Threat	Mean	Std	Min	Max
Malware Attacks	1.67	0.49	1	2
Phishing Attacks	1.44	0.51	1	2
Insider Threats	4.44	0.51	4	5
Ransomware Attacks	1.72	0.46	1	2
Data Breaches	3.39	0.50	3	4
Denial of Service Attacks	1.67	0.49	1	2
Cyber Espionage	1.56	0.51	1	2
System Vulnerabilities	3.61	0.50	3	4

Table 1 reveals varying perceptions of cybersecurity threats among Microfinance Banks using NAMBUIT software in Anambra State. Insider threats stand out with the highest mean of 4.44, indicating they are perceived as the most significant risk, with respondents consistently rating this threat between 4 and 5. System vulnerabilities and data breaches also show moderate concern, with means of 3.61 and 3.39, respectively, reflecting a perceived likelihood of occurrence. In contrast, threats like malware attacks, phishing, ransomware, denial of service, and cyber espionage are considered unlikely, with low mean scores ranging between 1.44 and 1.72. The low standard deviations for these threats indicate that respondents' perceptions were relatively consistent.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

Table 2: Adverse Effect of Cybersecurity Threat

Adverse Effect of Cybersecurity Threat	Mean	SD	Min	Max
Effect on Daily Banking Operations	3.45	0.55	3	4
Effect on Customer Trust and Satisfaction	3.30	0.47	3	4
Effect on Financial Losses	2.75	0.44	2	3
Effect on Data Integrity and Confidentiality	3.20	0.60	3	4
Effect on Regulatory Compliance	3.55	0.50	3	4
Effect on Business Continuity	2.85	0.49	2	3
Effect on Overall Risk Management Practices	3.35	0.52	3	4

The table highlights the perceived adverse effects of cybersecurity threats on various aspects of Microfinance Banks' operations. The most significant concern is the effect on regulatory compliance, with the highest mean score of 3.55, suggesting that cybersecurity threats pose a notable risk to adherence to regulations. The effect on daily banking operations and overall risk management practices also scores high with means of 3.45 and 3.35, respectively, indicating moderate to significant adverse effects. On the other hand, financial losses and business continuity show lower concern, with mean scores of 2.75 and 2.85, reflecting minimal to moderate perceived effect. The consistent standard deviations suggest a shared perception among respondents.

Table 3: Measures to Mitigate Cybersecurity Threats

Measures to Mitigate Cybersecurity Threats	Mean	SD	Min	Max
Extent of Employee Training Programs	3.60	0.52	3	4
Effectiveness of Firewalls and Intrusion Detection Systems	3.80	0.45	3	4
Implementation of Data Encryption Techniques	3.30	0.50	3	4
Effectiveness of Access Control Mechanisms	3.45	0.55	3	4
Regularity of Security Audits and Assessments	3.25	0.60	3	4
Extent of Incident Response and Recovery Plans	2.90	0.48	2	3
Effectiveness of Security Awareness Campaigns	2.75	0.44	2	3

The table highlights the perceived adverse effects of cybersecurity threats on various aspects of Microfinance Banks' operations. The most significant concern is the effect on regulatory compliance, with the highest mean score of 3.55, suggesting that cybersecurity threats pose a notable risk to adherence to regulations. The effect on daily banking operations and overall risk management practices also scores high with means of 3.45 and 3.35, respectively, indicating moderate to significant adverse effects. On the other hand, financial losses and business continuity show lower concern, with mean scores of 2.75 and 2.85, reflecting minimal to moderate perceived effect. The consistent standard deviations suggest a shared perception among respondents.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

Test of Hypotheses

H_{o1}: Cybersecurity threats do not significantly affect the operations of Microfinance Banks in Anambra State using NAMBUIT.

Table 4: One-Sample t-Test Table

Cybersecurity Threats	**Mean**	**Std**	**Test Value (μ_0)**	**t-Statistic**	**p-Value**
All Identified Threats	2.44	0.49	3	-3.22	0.014

Table 4 shows that the mean score for all identified threats is 2.44, which is below the test value of 3. The negative t-statistic of -3.22 and the p-value of 0.014, which is less than the standard significance level of 0.05, indicate that the difference is statistically significant. Given these results, we reject the null hypothesis that Microfinance Banks in Anambra State using NAMBUIT do not face significant cybersecurity threats. This suggests that these banks do experience cybersecurity threats, but they are perceived as less significant in adversely affecting their operations.

H_{o2}: Cybersecurity threats do not significantly affect the operational efficiency and compliance of the selected banks.

Table 5: One-Sample t-Test Table

Operational Efficiency & Compliance	Mean	Std	Test Value (μ_0)	t-Statistic	p-Value
All Identified Effects	3.21	0.51	3	1.05	0.33

The mean score for all identified effects is 3.21, slightly above the test value of 3, suggesting a moderate perceived effect. The t-statistic of 1.05 is positive but relatively low, and the p-value of 0.33 is well above the standard significance level of 0.05. Given these results, we fail to reject the null hypothesis, meaning that the data does not provide sufficient evidence to conclude that cybersecurity threats significantly affect the operational efficiency and compliance of the selected banks. While the threats are acknowledged, their effect on operations and compliance is not seen as highly significant according to the respondents.

H_{o3}: The current cybersecurity measures implemented by these banks are not adequate in mitigating the identified threats.

Table 6: One-Sample t-Test Table

Cybersecurity Measures Aggregate	Mean	Std	Test Value (μ_0)	t-Statistic	p-Value
All Identified Measures	3.29	0.50	3	1.53	0.17

The mean score for all identified measures is 3.29, slightly above the test value of 3, suggesting that the respondents perceive the measures as somewhat effective. The t-statistic of 1.53 indicates a positive but modest deviation from the test value, and the p-value of 0.17 is greater than the standard significance level of 0.05. As a result, we fail to reject the null hypothesis, meaning there is insufficient evidence to conclude that the existing cybersecurity measures are significantly effective. While the measures are viewed as more than adequate, they are not perceived as overwhelmingly effective, indicating potential areas for improvement in the security strategies employed by these banks.

DISCUSSION OF FINDINGS

The findings from this study emphasize the dual nature of cloud accounting in the Nigerian microfinance sector—while it offers significant operational benefits, it also introduces cybersecurity challenges that must be

carefully managed. The study's results reveal that cybersecurity threats, such as data breaches and system vulnerabilities, significantly affect daily banking operations, customer trust, and regulatory compliance. This aligns with the observations of Zheng et al. (2023), who noted that the adoption of cloud accounting in Nigeria has been driven by the need to improve operational efficiency and service delivery. However, the apprehension regarding data security and privacy, as highlighted by Dahiru and Abubakar (2018), is evident in the study's findings. The findings from daily operations and regulatory compliance underscore the importance of robust cybersecurity measures, consistent with the CBN's Risk-Based Cybersecurity Framework (CBN, 2022).

The study's findings corroborate the literature on the importance of cloud accounting in providing real-time access to financial data, as emphasized by Coman et al. (2022). However, the study also reveals that the current cybersecurity measures, while generally effective, may not be entirely sufficient. This finding contrasts with Dawood et al. (2023), who highlighted the enhanced security features of cloud accounting systems, such as encryption and automated backups. The need for continuous improvement in cybersecurity practices, particularly in environments where regulatory compliance is critical, is a key takeaway from this study. This suggests that while platforms like NAMBUIT offer valuable benefits, microfinance banks must remain vigilant and proactive in addressing cybersecurity risks to fully leverage the advantages of cloud accounting.

CONCLUSION

This study explored the effect of cybersecurity threats on the operational efficiency and regulatory compliance of microfinance banks (MFBs) in Anambra State, Nigeria, particularly those using the NAMBUIT cloud accounting platform. The findings indicate that while cloud accounting provides significant benefits, such as improved data accessibility and operational efficiency, it also introduces cybersecurity risks that can adversely affect daily operations, customer trust, and regulatory compliance. The study highlighted that current cybersecurity measures, though effective to some extent, require further enhancement to address these emerging threats adequately. Overall, the study underscores the importance of balancing the adoption of innovative technologies with robust cybersecurity practices to safeguard the integrity and continuity of financial operations in the microfinance sector.

RECOMMENDATIONS

Based on the study's findings, the following recommendations are proposed:

1. Enhance Cybersecurity Measures: MFBs should implement AI-driven threat detection, real-time monitoring, and regular security audits. Stronger access controls and multi-factor authentication (MFA) should be enforced to prevent unauthorized access.

2. Improve Employee Awareness and Training: Regular cybersecurity training should be conducted to address insider threats, phishing, and password security. Simulated phishing tests can help assess staff preparedness and reduce human error risks.

3. Strengthen Regulatory Compliance and Data Protection: MFBs must ensure strict compliance with CBN's cybersecurity framework and NDPR by adopting data encryption, routine security audits, and incident response plans to minimize risks and ensure business continuity.

REFERENCES

1. Abioye, T., Arogundade, O., Misra, S., Adesemowo, K., & Damaševičius, R. (2021). Cloud-Based Business Process Security Risk Management: A Systematic Review, Taxonomy, and Future Directions. Computers, 10(12), 160. https://doi.org/10.3390/computers10120160
2. Akintoye, R., Ogunode, O., Ajayi, M., & Joshua, A. A. (2022). Cyber Security and Financial Innovation of Selected Deposit Money Banks in Nigeria. Universal Journal of Accounting and Finance, 10(2), 643–652. https://doi.org/10.13189/ujaf.2022.100302
3. Akpan, M. (2024). Cloud Computing: Transforming Accounting in the Digital Age. Emerald Publishing Limited EBooks, 23–29. https://doi.org/10.1108/978-1-83797-819-920241004

4. Aladejebi, O. (2019). The Impact of Microfinance Banks on the Growth of Small and Medium Enterprises in Lagos Metropolis. European Journal of Sustainable Development, 8(3), 261. https://doi.org/10.14207/ejsd.2019.v8n3p261
5. Central Bank of Nigeria (CBN). (2022). Risk-based Cybersecurity Framework and Guidelines. Central Bank of Nigeria.
6. Chauhan, M., & Shiaeles, S. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. Network, 3(3), 422–450. https://doi.org/10.3390/network3030018
7. Coman, D. M., Ionescu, C. A., Duică, A., Coman, M. D., Uzlau, M. C., Stanescu, S. G., & State, V. (2022). Digitization of Accounting: The Premise of the Paradigm Shift of Role of the Professional Accountant. Applied Sciences, 12(7), 3359. https://doi.org/10.3390/app12073359
8. Dahiru, A. A., & Abubakar, H. (2018). Cloud Computing Adoption: A Cross-Continent Overview of Challenges. Nigerian Journal of Basic and Applied Sciences, 25(1), 23. https://doi.org/10.4314/njbas.v25i1.4
9. Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and Security of Cloud Computing: A Complete Guideline. Symmetry, 15(11), 1981. mdpi. https://doi.org/10.3390/sym15111981
10. Hashid, A., & Almaqtari, F. A. (2024). The Impact of Artificial Intelligence and Industry 4.0 on Transforming Accounting and Auditing Practices. Journal of Open Innovation: Technology, Market, and Complexity, 10(1), 100218. https://doi.org/10.1016/j.joitmc.2024.100218
11. INLAKS. (2018, May 30). Inlaks, CBN to Provide Solution for All Microfinance Banks (Demo). Retrieved August 22, 2024, from Inlaks | Information Technology Systems Integrator website: https://www.inlaks.com/inlaks-cbn-to-provide-solution-for-all-microfinance-banks-3/
12. INLAKS. (2020, January 24). About Us - INLAKS-NAMBUIT. Integrated Banking Platform for Nigerian Microfinance Banks. Retrieved August 22, 2024, from INLAKS-NAMBUIT website: https://www.inlaks-nambuit.com/about-us/
13. Isern, J., Agbakoba, A., Flaming, M., Mantilla, J., Pellegrini, G., & Tarazi, M. (2009). Access to Finance in Nigeria: Microfinance, Branchless Banking, and SME Finance. Retrieved from https://www.cgap.org/sites/default/files/CGAP-Access-to-Finance-in-Nigeria-Microfinance-Branchless-Banking-and-SME-Finance-Jan-2009.pdf
14. Mhlongo, N. Z., Usman, F. O., Odeyemi, O., Ike, C. U., Elufioye, O. A., & Daraojimba, A. I. (2024). Reviewing the impact of cloud computing on small and medium enterprises in Africa. International Journal of Science and Research Archive, 11(1), 1444–1451. https://doi.org/10.30574/ijsra.2024.11.1.0236
15. NITDA. (2019). Nigeria Data Protection Regulation (NDPR). National Information Technology Development Agency.
16. Petcu, M. A., Sobolevschi-David, M.-I., & Curea, S. C. (2024). Integrating Digital Technologies in Sustainability Accounting and Reporting: Perceptions of Professional Cloud Computing Users. Electronics, 13(14), 2684. https://doi.org/10.3390/electronics13142684
17. Pramuka, B. A., & Pinasti, M. (2020). Does Cloud-Based Accounting Information System Harmonize the Small Business Needs? Journal of Information and Organizational Sciences, 44(1), 141–156. https://doi.org/10.31341/jios.44.1.6
18. Reis, O., Oliha, J. S., Osasona, F., & Obi, O. C. (2024). Cybersecurity dynamics in Nigerian banking: Trends and Strategies Review. Computer Science & IT Research Journal, 5(2), 336–364. https://doi.org/10.51594/csitrj.v5i2.761
19. Saad, M., Lutfi, A., Almaiah, M., Alshira'h, A., Alshirah, M., Alqudah, H., … Abdelmaksoud, O. (2022). Assessing the Intention to Adopt Cloud Accounting during COVID-19. Electronics, 11(24), 4092. https://doi.org/10.3390/electronics11244092
20. Soetan, T. O., & Mogaji, E. (2024). Financial Services in Nigeria. In Sustainable development goals series. Springer International Publishing. https://doi.org/10.1007/978-3-031-62340-0
21. Zheng, M., Huang, R., Wang, X., & Li, X. (2023). Do firms adopting cloud computing technology exhibit higher future performance? A textual analysis approach. International Review of Financial Analysis, 90, 102866. https://doi.org/10.1016/j.irfa.2023.102866