ISRG Journal of Economics, Business & Management (ISRGJEBM)

ISRG PUBLISHERS

Abbreviated Key Title: Isrg J Econ Bus Manag

ISSN: 2584-0916 (Online)

Journal homepage: https://isrgpublishers.com/isrgjebm/

Volume – IV Issue -II (March–April) 2026

Frequency: Bimonthly

CYBERSECURITY AND CUSTOMER TRUST IN DIGITAL BANKING SERVICES IN SELECTED MICROFINANCE BANKS IN FCT-ABUJA

EDE JULIET NGOZI

Department of business administration, Faculty of management sciences, University of Abuja, Nigeria

| **Received:** 04.03.2026 | **Accepted:** 08.03.2026 | **Published:** 28.04.2026

***Corresponding author:** EDE JULIET NGOZI

Department of business administration, Faculty of management sciences, University of Abuja, Nigeria

Abstract

This study examines the effect of cybersecurity on customer trust in digital banking services within selected microfinance banks in FCT-Abuja, Nigeria. A cross-sectional survey research design was employed, targeting customers of two selected microfinance banks in FCT-Abuja. A structured questionnaire was used to collect primary data from a sample of 338 respondents. Data were analysed using regression analysis with the aid of SPSS v23. Reliability was assessed using Cronbach's alpha, while validity was established through content validation. Results indicate that data privacy and protection significantly influence customers' perceived security in digital banking services. Additionally, fraud prevention has a strong positive effect on customers' perceived reliability in digital banking. These findings highlight the critical role of cybersecurity measures in fostering customer trust. The study recommends the necessity for microfinance banks to enhance their cybersecurity frameworks by strengthening data privacy policies and implementing robust fraud prevention mechanisms. These efforts are essential for improving customer trust and ensuring long-term digital banking adoption. This study contributes to the growing body of knowledge on cybersecurity in digital banking, particularly within the microfinance sector in Nigeria. It provides empirical evidence on the relationship between cybersecurity and customer trust, offering insights that can guide policymakers, financial institutions, and regulators in enhancing digital banking security strategies.

Keywords: Cybersecurity, Customer Trust, Digital Banking, Data Privacy, Fraud Prevention, Microfinance Banks.

DOI: 10.5281/zenodo.19843623

Introduction

In an era where digitalization is reshaping global financial services, cybersecurity has emerged as a critical pillar in securing digital transactions and fostering customer trust (Hidayat & Kassim, 2023). Across the world, financial institutions are increasingly reliant on digital platforms to facilitate seamless banking experiences. However, this digital transformation has also brought about heightened concerns regarding data security, privacy breaches, and cyber fraud (Cele & Kwenda, 2025). The rapid growth of cyber threats has necessitated stringent cybersecurity measures to protect both financial institutions and their customers from financial losses and reputational damage (Nguyen et al., 2024). As digital banking services continue to expand, ensuring robust cybersecurity frameworks remains paramount in safeguarding sensitive customer information and maintaining confidence in the digital banking ecosystem (Gargouri, 2023).

Cybersecurity refers to the set of technologies, processes, and practices designed to protect digital systems, networks, and data from unauthorized access, cyberattacks, and other security threats (Oyewole et al., 2024). Effective cybersecurity measures are crucial for enhancing a firm's operational performance and long-term sustainability by mitigating financial risks, ensuring regulatory compliance, and fostering customer confidence (Nguyen et al., 2024). Scholars have identified two key dimensions of cybersecurity: data privacy and protection, and fraud prevention (Cele & Kwenda, 2025). Data privacy and protection involve safeguarding customers' personal and financial information from unauthorized access, thereby ensuring confidentiality and compliance with legal frameworks (Hidayat & Kassim, 2023). Fraud prevention focuses on implementing mechanisms to detect and prevent fraudulent transactions, reducing financial losses and enhancing transactional integrity (Oyewole et al., 2024). These dimensions are vital for fostering customer trust, as they assure users of the security and reliability of digital banking services (Cardoso et al., 2022).

Customer trust is a fundamental aspect of digital banking adoption and usage (Al-Dwairi et al., 2024). It refers to customers' confidence in the safety, reliability, and integrity of a financial institution's digital banking services (Gargouri, 2023). The dimensions of customer trust in digital banking services include perceived security and reliability. Perceived security relates to customers' beliefs that their financial and personal data are safe from cyber threats, while reliability pertains to the consistency and dependability of digital banking services in processing transactions accurately and efficiently (Hidayat & Kassim, 2023). These dimensions significantly influence customer behavior, determining whether they will continue using digital banking services or revert to traditional banking methods (Cardoso et al., 2022).

The interplay between cybersecurity and customer trust in digital banking services within microfinance banks in FCT-Abuja is a subject of increasing importance (Cele & Kwenda, 2025). While robust cybersecurity measures are expected to enhance customer confidence, the extent to which these measures influence trust levels in microfinance banking remains an area for further exploration (Nguyen et al., 2024). Given the growing prevalence of cyber threats, it is necessary to examine how security practices within microfinance banks impact customer perceptions and trust in digital transactions (Oyewole et al., 2024).

Microfinance banks face significant challenges in building and maintaining customer trust in digital banking services. Customers remain sceptical about the security and reliability of digital banking platforms due to increasing reports of cyber fraud, data breaches, and service failures. Unlike commercial banks with advanced cybersecurity infrastructures, many microfinance banks operate with limited resources, making them more vulnerable to cyber threats. This scepticism has resulted in reduced adoption of digital banking services among microfinance bank customers. Consequently, addressing cybersecurity concerns is crucial for these institutions to remain competitive and sustain customer confidence in their digital offerings.

Given these concerns, this study investigated the relationship between cybersecurity and customer trust in digital banking services among selected microfinance banks in FCT-Abuja. The findings will provide valuable insights for financial institutions, regulators, and policymakers in enhancing digital banking security frameworks and fostering trust among customers.

Statement of the Problem

Digital banking services should be secure, reliable, and trusted by customers, ensuring seamless financial transactions. Cybersecurity measures should be robust enough to prevent unauthorized access, data breaches, and fraudulent activities, fostering confidence in digital banking platforms.

However, in the context of microfinance banks in Nigeria, customers' trust in digital banking services remains a significant challenge. Reports of cyber fraud, data breaches, and service inefficiencies have contributed to growing skepticism among users. According to industry reports, Nigeria experienced over $500 million in cyber-related financial losses in recent years, with microfinance banks being among the most vulnerable institutions. Additionally, the rise of fintech companies offering secure and efficient digital banking alternatives has intensified competition, further challenging microfinance banks' ability to retain digitally inclined customers.

From a theoretical perspective, gaps exist in understanding the direct impact of cybersecurity dimensions—data privacy and protection, and fraud prevention—on customer trust in digital banking. While previous studies have explored cybersecurity in commercial banks, limited research has focused on microfinance institutions, particularly within FCT-Abuja. If these challenges are not addressed, microfinance banks may experience dwindling customer bases, reduced digital banking adoption, and potential financial instability, ultimately undermining their role in financial inclusion. It is on this premise that this study assessed the influence of cybersecurity on customers trust in selected microfinance banks in FCT-Abuja. Hence, the study specific objective were to:

i. examine the extent to which data privacy and protection affect perceived security in digital banking among customers of selected microfinance banks in FCT Abuja.
ii. assess the effect of fraud prevention on the reliability of digital banking services in selected microfinance banks in FCT Abuja.

Literature Review

Conceptual Review

Cybersecurity

Cybersecurity refers to the comprehensive set of practices,

DOI: 10.5281/zenodo.19843623

technologies, and processes designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access (Sekhar & Kumar, 2023). In the context of digital banking, cybersecurity is a cornerstone of operational integrity, as it ensures the protection of sensitive customer information, such as personal identification details, account numbers, and transaction histories. The rise of digital banking has exponentially increased the volume of data exchanged online, making financial institutions prime targets for cybercriminals. Scholarly perspectives emphasize that robust cybersecurity measures are essential for mitigating risks such as data breaches, fraud, and cyberattacks, which can undermine the stability and reputation of financial institutions (Akintoye et al., 2022). For instance, a single data breach can lead to significant financial losses, legal liabilities, and a loss of customer trust, which can take years to rebuild.

The importance of cybersecurity in digital banking extends beyond mere data protection; it also encompasses ensuring the integrity and availability of financial services. Cyberattacks, such as Distributed Denial of Service (DDoS) attacks, can disrupt banking operations, leaving customers unable to access their accounts or complete transactions. This not only causes immediate inconvenience but also erodes confidence in the banking system. Furthermore, as digital banking platforms increasingly integrate advanced technologies like artificial intelligence and blockchain, the complexity of cybersecurity challenges grows. Scholars argue that proactive measures, such as continuous monitoring, threat intelligence, and employee training, are critical for staying ahead of evolving cyber threats (Nguyen et al., 2024). In essence, cybersecurity is not just a technical requirement but a strategic imperative for digital banking, as it directly influences customer trust, regulatory compliance, and the overall sustainability of financial institutions**.**

Data Privacy and Protection

Data privacy and protection is a critical dimension of cybersecurity that focuses on safeguarding sensitive customer information from unauthorized access, breaches, or misuse. This involves implementing robust measures such as encryption, access controls, and secure data storage practices to ensure that personal and financial information remains confidential (Sekhar & Kumar, 2023). In digital banking, data privacy and protection are paramount because customers entrust their sensitive data, including account details, transaction histories, and personal identification information, to the platform. The consequences of failing to protect this data can be severe, ranging from financial losses and legal liabilities to long-term reputational damage for the financial institution. Scholarly perspectives emphasize that breaches in data privacy not only harm customers but also erode trust in the banking system, making it difficult for institutions to retain clients and attract new ones (Akintoye et al., 2022).

To maintain the integrity of digital banking systems, financial institutions must adopt a proactive approach to data privacy and protection. This includes complying with regulatory frameworks such as the General Data Protection Regulation (GDPR) and implementing advanced technologies like end-to-end encryption and blockchain for secure data storage and transmission. Additionally, banks must educate customers about best practices for protecting their data, such as using strong passwords and avoiding phishing scams. By prioritizing data privacy and protection, digital banking platforms can build a secure environment that fosters customer trust and confidence, ultimately contributing to the long-term success of the institution.

Fraud Prevention

Fraud prevention refers to the strategies and technologies employed to detect, mitigate, and prevent fraudulent activities such as identity theft, phishing, and unauthorized transactions (Oyewole et al., 2024). In digital banking, this dimension is vital for protecting customers from financial losses and ensuring the security of their accounts. As digital banking platforms handle large volumes of transactions daily, they become attractive targets for cybercriminals seeking to exploit vulnerabilities. Scholarly definitions highlight that fraud prevention mechanisms, such as real-time transaction monitoring, multi-factor authentication, and behavioural analytics, are critical for reducing vulnerabilities and enhancing the overall security of digital platforms (Cele & Kwenda, 2025). For example, real-time monitoring systems can flag suspicious transactions for further review, while behavioural analytics can identify unusual patterns of activity that may indicate fraud.

Effective fraud prevention not only safeguards customers but also reinforces their confidence in the banking system. When customers feel secure, they are more likely to engage in online transactions and adopt new digital banking services. Financial institutions must also stay ahead of emerging threats by continuously updating their fraud prevention strategies and investing in cutting-edge technologies. For instance, artificial intelligence and machine learning can be used to predict and prevent fraudulent activities before they occur. Additionally, banks should collaborate with industry stakeholders and regulatory bodies to share knowledge and best practices for combating fraud. By prioritizing fraud prevention, digital banking platforms can create a secure and trustworthy environment that supports customer loyalty and business growth.

Customer Trust

Customer trust is the confidence that customers have in a service provider's ability to deliver reliable and secure services (Al-Dwairi et al., 2024). In the context of digital banking, trust is a cornerstone of customer relationships, as users must feel assured that their financial data and transactions are protected. Digital banking platforms handle sensitive information, such as account details, transaction histories, and personal identification data, making trust a critical factor in customer adoption and retention. Scholarly definitions highlight that trust is built through consistent positive experiences, transparency, and the perceived competence of the service provider (Firmansyah & Ali, 2019). For instance, when customers perceive that a bank is transparent about its security measures and consistently delivers error-free services, their confidence in the platform grows.

Without trust, customers may hesitate to adopt or continue using digital banking platforms, making it a critical variable in the study. Trust is particularly important in the digital banking context because customers cannot physically interact with the service provider, relying instead on the platform's interface and reputation to gauge its reliability. Scholars emphasize that trust is not static but evolves over time based on customer experiences and the perceived effectiveness of the bank's security measures (Gogoi, 2021). For example, a single security breach or service outage can significantly erode trust, while consistent performance and proactive communication can strengthen it. Additionally, empirical studies suggest that trust directly influences customer engagement

DOI: 10.5281/zenodo.19843623

and brand loyalty (Agyei et al., 2020). Similarly, research on brand relationships in retail environments highlights that trust and loyalty are essential in sustaining long-term customer connections (Cardoso et al., 2022).

In essence, customer trust is a dynamic and multifaceted construct that plays a pivotal role in the success of digital banking services. Ensuring security, transparency, and consistent service quality are essential strategies for maintaining and strengthening customer trust in digital financial platforms.

Digital Banking

Digital banking encompasses the use of electronic platforms, such as mobile apps, online portals, and other digital channels, to conduct financial transactions and access banking services (Gargouri, 2023). It represents a significant shift from traditional brick-and-mortar banking to technology-driven solutions that offer convenience, accessibility, and efficiency. Digital banking allows customers to perform a wide range of activities, including account management, fund transfers, bill payments, and loan applications, from the comfort of their homes or on the go. This transformation has been driven by advancements in technology, changing customer expectations, and the need for financial institutions to remain competitive in a rapidly evolving landscape (Chauhan et al., 2022).

The success of digital banking hinges on its ability to provide secure, reliable, and user-friendly services while addressing customer concerns about privacy and data protection (Hidayat & Kassim, 2023). Scholars argue that digital banking platforms must prioritize cybersecurity, ease of use, and seamless integration with other financial tools to meet customer needs effectively (Chauhan et al., 2022; Gargouri, 2023). For instance, features such as real-time transaction alerts, biometric authentication, and personalized financial insights can enhance the user experience and foster customer loyalty. However, the rapid adoption of digital banking also introduces challenges, such as the need to combat cyber threats, ensure regulatory compliance, and bridge the digital divide for underserved populations (Makau & Olando, 2021).

Additionally, the effectiveness of digital banking is closely linked to its strategic implementation and customer satisfaction. Studies have shown that the adoption of digital banking services enhances financial inclusion and promotes accessibility for a broader customer base, particularly in emerging economies (Prakash & Mathew, 2020). The ability of banks to successfully integrate digital strategies determines their capacity to attract and retain customers while maintaining operational efficiency. As digital banking continues to evolve, financial institutions must focus on technological advancements and customer-centric solutions to remain competitive in the financial services industry.

Reliability

Reliability refers to the consistency and dependability of digital banking services in delivering accurate and timely transactions (Chege, 2021). In the context of customer trust, reliability is a key dimension because customers expect digital banking platforms to function seamlessly without errors or disruptions. Digital banking services must operate 24/7, ensuring that customers can access their accounts, transfer funds, and complete transactions at any time. Any failure in service delivery, such as delayed transactions, system downtime, or incorrect account balances, can lead to customer frustration and erode trust. Research suggests that reliability is achieved through robust infrastructure, effective error handling, and continuous system monitoring (Setiono & Hidayat, 2022). For example, banks invest in redundant systems, real-time monitoring tools, and disaster recovery plans to minimize service interruptions and maintain operational consistency.

When customers perceive a digital banking service as reliable, they are more likely to trust the platform and continue using it. Reliability also plays a significant role in building long-term customer relationships and fostering loyalty. Customers who experience consistent and error-free service are more likely to recommend the platform to others, contributing to the bank's reputation and market share. Furthermore, reliability is closely tied to customer confidence, as it reassures users that their financial activities are being handled accurately and efficiently. Studies show that reliability, along with assurance and service tangibles, significantly impacts customer trust and satisfaction across various industries, including banking and hospitality (Aruho & Kansiime, 2021). Thus, reliability is not just a technical attribute but a critical component of customer satisfaction and trust in digital banking.

Perceived Security

Perceived security refers to the customer's subjective belief that their personal and financial information is safe from threats when using digital banking services (Zhang et al., 2019). Perceived security refers to customers' confidence in a digital banking platform's ability to protect their personal and financial data from unauthorized access, fraud, and cyber threats (Marianus & Ali, 2021). Digital banking platforms handle sensitive information, making security a fundamental determinant of trust. Customers expect banks to implement robust security measures, such as encryption, multi-factor authentication, and fraud detection systems, to safeguard their data. When users feel that their transactions are secure, they are more likely to engage with digital banking services and develop long-term trust in the institution (Zhang et al., 2019).

Security perception also plays a crucial role in shaping customer satisfaction and adoption of digital banking services. Studies indicate that perceived security directly influences user trust and satisfaction, as customers prioritize platforms that offer transparency and proactive security measures (Trang, Thang, & Quy, 2024). Additionally, research suggests that perceived trust mediates the relationship between perceived privacy, security, and technology acceptance in digital banking (Zhang, 2024). If users believe that their financial data is well-protected, they are more likely to continue using the service, whereas security concerns may lead to hesitation or disengagement.

Ultimately, digital banking institutions must continuously enhance their security infrastructure and educate customers on safety measures to strengthen trust and ensure a secure banking experience. Effective security strategies, combined with a user-friendly interface and reliable service delivery, contribute significantly to maintaining customer confidence in digital banking.

Empirical Review

Oyewole et al. (2024) examined cybersecurity risks in online banking, focusing on the effectiveness of existing security frameworks and proposing strategies for improvement. The study employed a literature review and analysis of recent cybersecurity incidents to assess cyber threats, financial impacts, and current security measures in the banking sector. Findings indicated a pressing need for dynamic cybersecurity strategies incorporating

DOI: 10.5281/zenodo.19843623

advanced technologies, regulatory compliance, and awareness programs. The study recommended integrating Big Data analytics, artificial intelligence, and continuous risk assessment to enhance cybersecurity resilience. However, the research did not provide empirical validation of the proposed strategies in real banking environments, leaving a gap for further practical implementation studies.

Cele and Kwenda (2025) investigated the impact of cybersecurity threats on the adoption of digital banking and proposed sustainable strategies to mitigate these risks. Using a systematic literature review, the study conducted a quantitative synthesis of 58 empirical studies after screening 84 initial articles. Findings revealed that identity theft, malware attacks, phishing, and vishing were major cybersecurity threats discouraging digital banking adoption. The study emphasized the need for enhanced security measures to address these risks. However, the study primarily relied on secondary data without empirical validation of the proposed strategies, presenting a gap for further research on real-world applications.

Alrababah et al. (2024) examined the effect of user behavior on cybersecurity knowledge in online banking, particularly in mobile banking. The study employed a survey method using standardized questionnaires and a convenience sampling technique, collecting data from 500 respondents across different demographic and professional backgrounds. Findings indicated that despite the increasing adoption of mobile banking, users' cybersecurity awareness remained insufficient, with many underestimating security threats associated with online transactions. The study emphasized the need for more effective cybersecurity training programs and the integration of security measures into mobile banking services. However, the study focused on consumer awareness without assessing the effectiveness of existing cybersecurity interventions, presenting a gap for further research on practical security enhancements.

Nguyen et al. (2024) assessed cybersecurity risks in Vietnam's finance and banking system and prioritized top mitigation strategies. The study employed a Multi-Criteria Decision-Making (MCDM) approach, integrating the DELPHI technique, Decision-Making Trial and Evaluation Laboratory (DEMATEL), and Combined Compromise Solution (COCOSO) methods, along with Neutrosophic Sets (NS) and Z-number concepts. Findings identified 15 cybersecurity risks, with Malware Infections and Supply Chain Vulnerabilities being the most critical. The study recommended investing in advanced threat detection systems to strengthen cybersecurity resilience. However, the research focused primarily on risk identification and prioritization, leaving a gap in evaluating the real-world effectiveness of these strategies.

Sekhar and Kumar (2023) provided an overview of cybersecurity in the digital banking sector, focusing on the increasing prevalence of cybercrimes such as ATM fraud, debit card fraud, and net banking breaches. The study employed a literature review approach to examine the nature of cyber threats and the security measures implemented in digital banking. Findings indicated that cyberattacks in the banking sector occur more frequently than in other industries, with 50% of cybercrimes linked to banking transactions. The study recommended enhancing cybersecurity frameworks through stronger authentication methods and continuous monitoring. However, the study lacked empirical validation of the proposed security measures, highlighting a gap in assessing their practical effectiveness.

Theoretical Framework

This study is anchored on the Technology Acceptance Model (TAM), proposed by Davis in 1989. The TAM posits that perceived usefulness and perceived ease of use are the primary determinants of technology adoption (Davis, 1989). The major assumption of the theory is that users are more likely to adopt a technology if they believe it will enhance their performance and if it is easy to use (Wang et al., 2023)

TAM is widely recognized for its simplicity and applicability in studying technology adoption. Its focus on perceived usefulness and perceived ease of use makes it highly relevant for understanding customer behaviour in digital banking, particularly in microfinance banks where user-friendliness and security are critical (Musa et al., 2024). The model's adaptability allows it to incorporate additional variables, such as perceived security and reliability, which are central to this study.

One limitation of TAM is its reliance on perceptual measures, which may not fully capture the complexities of real-world technology adoption. Additionally, the model does not explicitly account for external factors such as cultural influences or infrastructural challenges, which may be significant in the context of microfinance banks in FCT-Abuja.

In this study, TAM was applied to explore how customers' perceptions of cybersecurity measures (e.g., data privacy, fraud prevention) and the reliability of digital banking services influence their trust and adoption intentions. By integrating perceived security and reliability into the TAM framework, the study provided a deeper understanding of the factors that drive customer trust in digital banking services within microfinance banks in FCT-Abuja. This approach highlighted the importance of user-friendly and secure digital platforms in fostering customer confidence and loyalty.

Methodology

This study adopted a cross-sectional survey research design, which is appropriate for examining the relationship between cybersecurity and customer trust at a single point in time. This design was justified as it allows for the collection of primary data from a specific population within a defined period, ensuring a comprehensive analysis of the subject matter. The population of the study comprised customers of microfinance banks in FCT-Abuja. However, the accessible population was limited to customers of two selected microfinance banks operating in Wuse 2 in FCT Abuja, with a total customer base of 2,791. The information on the customer base was obtained from the operation managers of the banks. The unit of analysis was the customers of these banks, as they are the primary users of digital banking services and their perceptions directly impact trust and service adoption. The sample size for the study is 350 and was determined using Taro Yamane formula for sample size determination, which is denoted as:

$$\mathbf{n = N / (1 + N(e)^2)}$$

where:

n = sample size

N = population size (2,791)

e = margin of error (5% or 0.05)

Hence:

DOI: 10.5281/zenodo.19843623

$n = 2791 / (1 + 2791(0.05)^2)$

$n = 2791 / (1 + 2791(0.0025))$

$n = 2791 / (1 + 6.9775)$

$n = 2791 / 7.9775 \approx 350$ respondents

The study employed a convenience and purposive sampling technique. Convenience sampling was used to select respondents based on their availability and willingness to participate, while purposive sampling ensured that only active digital banking users were included. These techniques were justified as they facilitated the collection of relevant and accurate data.

Primary data was collected through a structured questionnaire. The reliability of the instrument was determined using Cronbach's alpha, with coefficients as follows: data privacy and protection (0.82), fraud prevention (0.85), perceived security (0.78), and reliability in digital banking services (0.80), indicating acceptable reliability levels. The validity of the instrument was determined through content validity, ensuring that the questionnaire adequately captured the study variables. Data analysis was conducted using simple regression analysis with the aid of SPSS version 23 to examine the relationship between cybersecurity dimensions and customer trust in digital banking services.

Results and Discussions

In line with the determined sample size, 350 questionnaires were distributed to respondents. Out of the 350 questionnaires distributed, 189 were retrieved, representing a retrieval rate of 54%. Preliminary analysis of the retrieved questionnaires revealed that 178 questionnaires (approximately 51% of the sample) were complete and suitable for further analysis. Naing (2003) and Olukemi et al. (2016) confirmed that a 50% response rate is acceptable, it is the minimum threshold for minimizing nonresponse bias, thus, supporting the use of the data. The demographic characteristics of the 178 respondents are summarized in Table 1. The breakdown includes age, gender, average work experience, and educational level.

Table 1: Demographic Profile of Respondents

Variable	Category	Frequency	Percentage (%)
Age	18–30 years	75	42.1
	31–40 years	62	34.8
	41–50 years	28	15.7
	Above 50 years	13	7.3
Gender	Male	102	57.3
	Female	76	42.7
Educational Level	Secondary Education	25	14.0
	Bachelor's Degree	98	55.1
	Master's Degree	45	25.3
	PhD/Professional	10	5.6

Source: Fieldwork, 2025

The demographic profile of respondents provides insight into the customer base of microfinance banks in this study. The majority (42.1%) fall within the 18–30 years age group, followed by the 31–40 years group (34.8%), indicating that younger and middle-aged adults are the primary users. Older individuals above 50 years (7.3%) represent a smaller segment.

Gender distribution shows a slight male dominance (57.3% vs. 42.7%), suggesting moderate gender disparity in microfinance participation. Educationally, most respondents hold a Bachelor's Degree (55.1%), followed by a Master's Degree (25.3%), indicating a well-educated customer base. A smaller percentage have Secondary Education (14.0%) or PhD/Professional qualifications (5.6%). Overall, microfinance banks in this study primarily serve younger, educated individuals, with a slightly higher male representation. Before conducting further analysis, the major assumptions of simple regression were tested and satisfied.

H_0: Data privacy and protection have no significant effect on perceived security in digital banking services.

Table 2: Model Summary on Data privacy, protection and perceived security

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.600[a]	.360	.356	1.02379
a. Predictors: (Constant), Data privacy and protection				

Table 3: ANOVA on Data privacy, protection and perceived security

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	103.772	1	103.772	99.005	.000[a]
	Residual	184.475	176	1.048		
	Total	288.247	177			
a. Predictors: (Constant), Data privacy and protection						
b. Dependent Variable: Perceived security						

Table 4: Coefficients on Data privacy, protection and perceived security

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.818	.215		8.446	.000
	Data privacy and protection	.567	.057	.600	9.950	.000
a. Dependent Variable: Perceived security						

Sources: Fieldwork, 2025

The Model Summary (Table 2) shows an R-value of 0.600, indicating a moderate positive correlation between data privacy and protection and customers' trust in digital banking services. The R-square value of 0.360 suggests that 36% of the variance in customer trust (perceived security) can be explained by data privacy and protection, demonstrating a meaningful impact.

The ANOVA results (Table 3) further confirm the model's significance, with an F-statistic of 99.005 and a p-value of 0.000

DOI: 10.5281/zenodo.19843623

(p<0.05). This indicates that the model is statistically significant, rejecting the null hypothesis and confirming that data privacy and protection significantly influence perceived security in digital banking.

The coefficients table (Table 4) provides further insight into this relationship. The constant term is 1.818 (p<0.05), while the coefficient for data privacy and protection is 0.567 with a t-value of 9.950 (p<0.05), suggesting a strong and statistically significant effect. The positive beta coefficient (0.600) indicates that an increase in data privacy and protection enhances customers perceived security in digital banking services in microfinance banks. The findings provide empirical evidence that data privacy and protection will significantly influence perceived security in digital banking services in microfinance banks in FCT-Abuja.

H_0: Fraud prevention has no significant effect on customers' reliability in digital banking services.

Table 5: Model Summary on Fraud prevention and customers reliability

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.717[a]	.515	.512	.99922
a. Predictors: (Constant), Fraud prevention				

Table 6: ANOVA on Fraud prevention and customers reliability

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	186.295	1	186.295	186.585	.000[a]
	Residual	175.727	176	.998		
	Total	362.022	177			
a. Predictors: (Constant), Fraud prevention						
b. Dependent Variable: Reliability						

Table 7: Coefficients on Fraud prevention and customers reliability

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.479	.242		1.984	.049
	Fraud prevention	.848	.062	.717	13.660	.000
a. Dependent Variable: Reliability						

Sources: Fieldwork, 2025

The Model Summary (Table 5) reveals an R-value of 0.717, indicating a strong positive correlation between fraud prevention and customer reliability in digital banking services. The R-square value of 0.515 suggests that 51.5% of the variance in customer reliability can be explained by fraud prevention measures, highlighting its substantial impact.

The ANOVA results (Table 6) confirm the statistical significance of the model, with an F-statistic of 186.585 and a p-value of 0.000 (p<0.05). This result rejects the null hypothesis and affirms that fraud prevention significantly influences customer reliability in digital banking.

The coefficients table (Table 7) further supports this conclusion. The constant term is 0.479 (p=0.049), while the coefficient for fraud prevention is 0.848 with a t-value of 13.660 (p<0.05), indicating a highly significant and positive effect. The standardized beta coefficient (0.717) suggests that fraud prevention plays a dominant role in enhancing customer reliability in digital banking services. The findings demonstrate that fraud prevention will significantly contributes to customer reliability in digital banking services in microfinance banks in FCT-Abuja.

Discussion of Findings

The broad objective of this study was to assess the effect of cybersecurity on customer trust in digital banking services in microfinance banks in FCT-Abuja. The study successfully achieved this objective by evaluating the impact of two key cybersecurity dimensions—data privacy and protection, and fraud prevention—on customer trust. The findings provided empirical validation of the relationship between cybersecurity and customer trust in digital banking services. Two hypotheses were tested to establish the effect of cybersecurity on customer trust. The first hypothesis examined the effect of data privacy and protection on customer trust, while the second hypothesis assessed the impact of fraud prevention on customer reliability in digital banking services.

The findings from the first hypothesis revealed that data privacy and protection significantly influence customer trust in digital banking services. The study found a moderate positive relationship, indicating that enhanced data privacy measures lead to increased customer confidence in digital banking. These findings align with the study by Oyewole et al. (2024), which examined cybersecurity risks in online banking and emphasized the importance of dynamic cybersecurity strategies incorporating advanced technologies and regulatory compliance. Similarly, Cele and Kwenda (2025) highlighted the role of cybersecurity threats, such as identity theft and phishing, in discouraging digital banking adoption. The findings of this study reinforce their argument by empirically demonstrating that robust data privacy measures enhance customer trust, countering the negative impact of cyber threats on digital banking adoption.

The second hypothesis tested the effect of fraud prevention on customer reliability in digital banking services. The findings indicated a strong positive relationship between fraud prevention and customer reliability, with fraud prevention explaining a significant proportion of the variance in customer trust. This aligns with the study by Alrababah et al. (2024), which highlighted the role of cybersecurity awareness in influencing user behavior in online banking. Moreover, Nguyen et al. (2024) identified malware infections and supply chain vulnerabilities as top cybersecurity risks in banking, recommending investments in advanced threat detection systems. The findings of this study support the need for enhanced fraud prevention measures, reinforcing the argument that robust security frameworks directly influence customer trust and reliability in digital banking services.

Overall, the study contributes to the cybersecurity and digital banking literature by providing empirical validation of the impact of data privacy and fraud prevention on customer trust. The findings emphasize the necessity for microfinance banks in FCT-Abuja to enhance their cybersecurity measures to strengthen

DOI: 10.5281/zenodo.19843623

customer confidence and promote the widespread adoption of digital banking services.

Conclusions and Recommendations

Cybersecurity has become a critical determinant of customer trust in digital banking services, particularly in microfinance banks, where security vulnerabilities can significantly impact customer confidence. This study examined the effect of cybersecurity on customer trust in digital banking services in microfinance banks in FCT-Abuja. The study focused on two key dimensions of cybersecurity: data privacy and protection, and fraud prevention. The findings provided empirical evidence that cybersecurity significantly influences customer trust, reinforcing the need for banks to implement robust security measures.

Specifically, the study established that data privacy and protection play a vital role in enhancing customers' trust in digital banking services. The findings revealed that ensuring the confidentiality and security of customer data directly impacts perceived security, which in turn fosters greater trust in digital banking platforms.

Furthermore, the study found that fraud prevention is a significant predictor of customer reliability in digital banking services. Customers are more likely to engage with digital banking platforms when they perceive strong fraud prevention mechanisms, including secure authentication processes and fraud detection systems. The findings underscore the necessity for financial institutions, especially microfinance banks, to prioritize proactive fraud mitigation strategies to enhance customer confidence and digital banking adoption.

Recommendations

Based on the findings, the following recommendations are made to improve cybersecurity and enhance customer trust in digital banking services:

1. Given that data privacy and protection significantly influence customer trust, microfinance banks should implement comprehensive data security policies. This includes encrypting customer data, employing multi-layered authentication protocols, and regularly updating security frameworks to prevent data breaches. Banks should also comply with regulatory standards on data protection and ensure transparency in how customer data is handled.

2. Since fraud prevention significantly affects customer reliability in digital banking, microfinance banks should invest in advanced fraud detection and prevention technologies. Implementing artificial intelligence-driven fraud detection systems, biometric authentication, and real-time transaction monitoring can help prevent unauthorized access and fraudulent activities. Banks should also adopt multi-factor authentication to enhance security in digital transactions. Furthermore, they should establish dedicated fraud response teams to promptly investigate and mitigate fraudulent incidents.

References

1. Agyei, J., Sun, S., Abrokwah, E., Penney, E. K., & Ofori-Boafo, R. (2020). Influence of Trust on Customer Engagement: Empirical Evidence From the Insurance Industry in Ghana. SAGE Open, 10(1). https://doi.org/10.1177/2158244019899104
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*(3), 643–652.
3. Al-Dwairi, R., Shehabat, I., Zahrawi, A., & Al-Hammouri, Q. (2024). Building customer trust, loyalty, and satisfaction: The power of social media in e-commerce environments. *International Journal of Data and Network Science, 8*(3), 1883-1894. https://doi.org/10.5267/j.ijdns.2024.2.001
4. Aruho, A. R., & Kansiime, N. K. (2021). Relationship between reliability, assurance, the tangible clues of customer service and customer satisfaction and trust in hotels in Uganda. *American Research Journal of Humanities & Social Science (ARJHSS, 4*(10), 1-7.
5. Austin-Olowo, L. B. A., Anike, O. I., & Ailemen, I. O. (2023). Cybersecurity issues affecting online banking and transactions in Nigeria. *International Journal of Arts, Languages and Business Studies, 9*, 25–35.
6. Cardoso, A., Gabriel, M., Figueiredo, J., Oliveira, I., Rêgo, R., Silva, R., Oliveira, M., & Meirinhos, G. (2022). Trust and loyalty in building the brand relationship with the customer: Empirical analysis in a retail chain in Northern Brazil. *Journal of Open Innovation: Technology, Market, and Complexity, 8*(3), 109. https://doi.org/10.3390/joitmc8030109
7. Cardoso, A., Gabriel, M., Figueiredo, J., Oliveira, I., Rêgo, R., Silva, R., Oliveira, M., & Meirinhos, G. (2022). Trust and loyalty in building the brand relationship with the customer: Empirical analysis in a retail chain in Northern Brazil. *Journal of Open Innovation: Technology, Market, and Complexity, 8*(3), 109. https://doi.org/10.3390/joitmc8030109
8. Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime, 32*(1), 31–48. https://doi.org/10.1108/JFC-10-2023-0263
9. Chauhan, S., Akhtar, A., and Gupta, A. (2022). Customer Experience in Digital Banking: A Review and Future Research Directions. International Journal of Quality and Service Sciences, 14(2), 311-348.
10. Chege, C. N. (2021). Examining the influence of service reliability on customer satisfaction in the insurance industry in Kenya. *International Journal of Research in Business and Social Science (2147- 4478), 10*(1), 259–265. https://doi.org/10.20525/ijrbs.v10i1.1025
11. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.
12. Firmansyah, N., & Ali, H. (2019). Consumer trust model: The impact of satisfaction and e-service quality toward repurchase intention in e-commerce. *Saudi Journal of Humanities and Social Sciences, 4*(8), 552-559.
13. Gargouri, O. (2023). Digital banking services: Customers' pros and cons. A theoretical literature review. Business Excellence and Management, 13(2), 5-13. https://doi.org/10.24818/beman/2023.13.2-01
14. Gogoi, B.J. (2021). Customer trust influencing customer perceived value and brand loyalty. Academy of Marketing Studies Journal, 25(5), 1-11.

DOI: 10.5281/zenodo.19843623

15. Hidayat, A., & Kassim, S. (2023). The digital banking services: A selection model from Islamic banks. International Journal of Islamic Business, 8(1), 41–58. https://doi.org/10.32890/ijib2023.8.1.3
16. Makau, J. M., & Olando, C. O. (2021). Digital Banking Strategy and Financial Inclusion among Commercial Banks in Kajiado County. A Case of Kenya Commercial Bank in Kajiado County, Kenya. Asian Journal of Economics, Business and Accounting, 21(5), 1–14. https://doi.org/10.9734/ajeba/2021/v21i530376
17. Marianus, S., & Ali, S. (2021). Factors determining the perceived security dimensions in B2C electronic commerce website usage: An Indonesian study. *Journal of Accounting and Investment*, *22*(1), 104–132. https://doi.org/10.18196/jai.v22i1.8171
18. Musa, H. G., Fatmawati, I., Nuryakin, N., & Suyanto, M. (2024). Marketing research trends using technology acceptance model (TAM): a comprehensive review of researches (2002–2022). *Cogent Business & Management*, *11*(1). https://doi.org/10.1080/23311975.2024.2329375
19. Naing, N. N. (2003). Determination of sample size. *Malaysian Journal of Medical Sciences*, *10*(2), 84–86. PMID: 23386802; PMCID: PMC3561892.
20. Nguyen, P.-H., Pham, T.-V., Nguyen, L.-A. T., Pham, H.-A. T., Nguyen, T.-H. T., & Vu, T.-G. (2024). Assessing cybersecurity risks and prioritizing top strategies in Vietnam's finance and banking system using strategic decision-making models-based neutrosophic sets and Z number. *Heliyon*, *10*(19), e37893. https://doi.org/10.1016/j.heliyon.2024.e37893
21. Olukemi, O., & Ifijeh, G. (2016). Towards a better response rate for questionnaires: Current trends among librarians in Nigerian academic libraries. *Library Progress (International)*, *36*(2), 79. https://doi.org/10.5958/2320-317X.2016.00007.6
22. Oyewole, A., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, *21*(3), 625–643. https://doi.org/10.30574/wjarr.2024.21.3.0707
23. Prakash, C., & Mathew, T. (2020). Effectiveness of digital banking. International Journal of Research and Analytical Reviews (IJRAR), 7(1), 108-111.
24. Sekhar, S. C., & Kumar, M. (2023). An overview of cyber security in the digital banking sector. *East Asian Journal of Multidisciplinary Research*, *2*(1), 43–52.
25. Setiono, B. A., & Hidayat, S. (2022). Influence of service quality with the dimensions of reliability, responsiveness, assurance, empathy, and tangibles on customer satisfaction. *International Journal of Economics, Business and Management Research*, *6*(9), 330-341.
26. Trang, T. T. N., Thang, P. C., & Quy, T. Q. (2024). Examining the influence of security perception on customer satisfaction: A quantitative survey in Vietnam. *EAI Endorsed Transactions on Internet of Things*, *10*. https://doi.org/10.4108/eetiot.5210
27. Wang, C., Ahmad, S. F., Ayassrah, A. Y. B. A., Awwad, E. M., Irshad, M., Ali, Y. A., Al-Razgan, M., Khan, Y., & Han, H. (2023). An empirical evaluation of technology acceptance model for artificial intelligence in e-commerce. *Heliyon*, *9*(8), e18349. https://doi.org/10.1016/j.heliyon.2023.e18349
28. Zhang, J., Luximon, Y., & Song, Y. (2019). The role of consumers' perceived security, perceived control, interface design features, and conscientiousness in continuous use of mobile payment services. *Sustainability*, *11*(23), 6843. https://doi.org/10.3390/su11236843
29. Zhang, Y. (2024). Impact of perceived privacy and security in the TAM model: The perceived trust as the mediated factors. *International Journal of Information Management Data Insights*, *4*(2), 100270. https://doi.org/10.1016/j.jjimei.2024.100270

DOI: 10.5281/zenodo.19843623