

Cybersecurity Practices and Customer Trust in Digital Banking Platforms in Nigeria: A Comparative Study of Nigerian Fintech firms and Nigerian Conventional Banks

Edodi, Hope Ukam (Ph.D)¹, Uwah, Inemesit Enobong (Ph.D)², Akaegbu, Juliana Baby (Ph.D)¹, Okon, Emmanuel Ekpenyong (Ph.D)¹, Ogar, Godwin Wonah¹

¹Department of Business Management, University of Calabar, Calabar, Nigeria
hopeedodi@gmail.com, 08069059787, Julakaegbu83@ymail.com, 07032615255,
Okonemmanuel2018@gmail.com, 08032738173, godwinogar139@gmail.com, 08105412041

²Department of Business Administration, Akwa Ibom State University, Nigeria
inemesituwah@aksu.edu.ng, 08034921199

ABSTRACT

This study examined the influence of cybersecurity practices on customer trust in digital banking platforms in Nigeria, adopting a comparative approach between fintech firms and conventional banks. However, the increased reliance on digital platforms has heightened cybersecurity risks, including fraud, data breaches, and unauthorized access, which threatens customer trust across fintech and conventional banking institutions. This study investigated how cybersecurity practices influence customer trust, with a comparative focus on fintech firms and conventional banks. The theoretical framework for this research was the Technology Acceptance Model and Trust theory. The study adopted a survey research design. Data were collected from 320 management staff across eight financial institutions, comprising four fintech firms and four commercial banks. A purposive sampling technique was employed, and all variables were measured using a 5-point Likert scale. The independent variables included data protection measures, authentication and access control systems, fraud detection and prevention capability, and customer security awareness, while customer trust served as the dependent variable. Data were analysed using descriptive statistics, independent sample t-tests, and multiple regression analysis. The findings revealed that cybersecurity practices have a significant positive effect on customer trust, explaining 68.1% of the variation ($R^2 = 0.681$). The t-test results showed a statistically significant difference between fintech firms and conventional banks, with fintech recording higher mean scores across all variables, indicating superior performance in cybersecurity and customer trust. The study concluded that effective cybersecurity practices are critical for enhancing customer trust in digital banking platforms. It recommended that financial institutions should invest in advanced cybersecurity infrastructure, strengthen customer awareness initiatives, and enhance digital capabilities to sustain trust and competitiveness in Nigeria's evolving financial landscape.

Keywords: cybersecurity practices, customer trust, digital banking, fintech firms, commercial banks, data security

INTRODUCTION

The rapid advancement of digital technologies has fundamentally transformed the delivery of financial services across the globe, with Nigeria emerging as one of the leading adopters of financial technology (fintech) in Africa. The proliferation of mobile banking, digital payment platforms, and

online financial services has improved accessibility, convenience, and efficiency in the financial sector. Fintech firms have leveraged innovative technologies to disrupt traditional banking models, while conventional banks continue to integrate digital solutions into their operations to remain competitive. However, the increasing reliance on digital platforms has also heightened concerns regarding cybersecurity, as financial transactions and sensitive customer data are now predominantly conducted and stored online.

Cybersecurity has become a critical issue in digital banking, as the frequency and sophistication of cyber threats continue to rise. Incidents such as data breaches, identity theft, phishing attacks, and unauthorized transactions have raised questions about the safety of digital financial platforms and their ability to protect users. According to the Central Bank of Nigeria, the growth of electronic banking in Nigeria has been accompanied by increased exposure to cyber risks, necessitating stronger security frameworks and regulatory oversight (Central Bank of Nigeria, 2023). Similarly, the Nigeria Inter-Bank Settlement System reports a steady increase in electronic fraud cases, highlighting the need for improved cybersecurity measures across financial institutions (NIBSS, 2023).

Customer trust is widely recognized as a cornerstone of digital banking adoption and sustainability. When customers perceive a platform as secure, they are more likely to engage in financial transactions and maintain long-term relationships with the institution. Conversely, weak cybersecurity practices can erode confidence and discourage usage. Prior studies have shown that trust in digital financial services is strongly influenced by the effectiveness of security measures implemented by service providers (Olaleye & Aremu, 2022; Eze & Nwankwo, 2021). In this context, cybersecurity practices such as data protection measures, authentication and access control systems, fraud detection and prevention capabilities, and customer security awareness play a vital role in shaping user perceptions and trust.

Data protection measures are essential for safeguarding sensitive customer information from unauthorized access and breaches. Financial institutions are expected to implement robust encryption systems, secure data storage, and compliance with data protection regulations such as the Nigeria Data Protection Regulation (NDPR). Authentication and access control systems, including multi-factor authentication and biometric verification, serve as the first line of defense against unauthorized access to digital banking platforms. In addition, fraud detection and prevention capabilities enable institutions to identify and respond to suspicious activities in real time, thereby reducing the risk of financial losses and enhancing customer confidence. Furthermore, customer security awareness and communication initiatives help educate users on safe digital practices, reducing vulnerability to cyber threats and reinforcing trust in the system.

Despite the importance of these cybersecurity practices, there is a growing concern that their implementation and effectiveness may vary between fintech firms and conventional banks. Fintech companies are often perceived as more agile and technologically advanced, enabling them to deploy innovative security solutions. In contrast, conventional banks may face challenges associated with legacy systems and bureaucratic processes, which can limit their responsiveness to emerging cyber threats. This disparity raises important questions about how cybersecurity practices influence customer trust across different types of financial institutions. Therefore, this study seeks to examine the effect of cybersecurity practices on customer trust in digital banking platforms in Nigeria, with a comparative focus on fintech firms and conventional banks. By analysing key cybersecurity dimensions such as, data protection measures, authentication systems, fraud detection capabilities, and customer security awareness. The study aims to provide empirical insights into how these factors shape trust and influence the sustainability of digital financial services in Nigeria.

STATEMENT OF THE PROBLEM

The expansion of digital banking in Nigeria, driven by both fintech firms and conventional commercial banks, has significantly improved access to financial services and transformed customer experience. However, this rapid digitalization has also increased exposure to cybersecurity threats such as data breaches, identity theft, phishing attacks, and unauthorized transactions. These risks have raised growing concerns among customers regarding the safety of their financial information and the reliability of digital banking platforms. Despite continuous investments in digital infrastructure, incidents of electronic fraud and security breaches persist, thereby undermining customer confidence in the financial system.

Customer trust remains a critical factor for the adoption, usage, and sustainability of digital banking services. When customers perceive digital platforms as secure, they are more likely to engage in transactions and maintain long-term relationships with service providers. Conversely, weak or ineffective cybersecurity practices can lead to distrust, reduced usage, and potential financial losses for both customers and institutions. While financial institutions have implemented various cybersecurity measures, there is still uncertainty regarding the extent to which these practices effectively influence customer trust.

Specifically, key cybersecurity dimensions such as data protection measures, authentication and access control systems, fraud detection and prevention capabilities, and customer security awareness are expected to play significant roles in shaping customer trust. However, the effectiveness and implementation of these measures may differ between fintech firms and conventional commercial banks due to variations in technological capabilities, operational structures, and service models. Fintech firms are often perceived as more innovative and agile, while conventional banks may rely on established systems that may not fully adapt to evolving cyber threats.

Despite the growing importance of cybersecurity in digital banking, there is a scarcity of comparative empirical studies that examine how this specific cybersecurity practices influence customer trust across fintech firms and conventional banks in Nigeria. This gap limits a comprehensive understanding of which sector is better positioned to ensure secure digital transactions and sustain customer confidence.

Therefore, this study seeks to address this gap by examining the effect of cybersecurity practices on customer trust in digital banking platforms in Nigeria, with a comparative analysis of fintech firms and conventional commercial banks.

OBJECTIVES OF THE STUDY

- To examine the effect of cybersecurity practices on customer trust in digital banking platforms in Nigeria, with a comparative analysis of fintech firms and conventional commercial banks. Specific objectives include:
- To assess the effect of data protection measures on customer trust in digital banking platforms in Nigeria.
- To examine the influence of authentication and access control systems on customer trust in digital banking platforms.
- To evaluate the effect of fraud detection and prevention capabilities on customer trust in digital banking platforms.
- To determine the influence of customer security awareness and communication on customer trust in digital banking platforms.

LITERATURE REVIEW

Data Protection Measures and Customer Trust

Data protection measures are fundamental components of cybersecurity practices in digital banking, as they focus on safeguarding sensitive customer information from unauthorized access, breaches, and misuse. In the context of Nigeria's rapidly evolving digital financial ecosystem, the protection of customer data has become increasingly critical due to the growing volume of online transactions and digital data exchanges. Effective data protection involves the use of encryption technologies, secure databases, and compliance with regulatory frameworks designed to ensure information security (Adebayo & Olusegun, 2023; Kshetri, 2022).

Empirical evidence suggests that strong data protection mechanisms significantly enhance customer trust in digital banking platforms. Customers are more likely to engage with financial institutions that demonstrate a high level of commitment to protecting personal and financial data from cyber threats (Soni, Jain, & Kumar, 2023). Similarly, Alalwan (2022) posits that perceived data security is a critical determinant of user trust and continued usage of digital financial services. When customers believe that their sensitive information is well protected, they are more confident in conducting transactions through digital platforms.

Conversely, weak data protection systems expose customers to risks such as identity theft, data breaches, and financial fraud, which can undermine trust and reduce platform usage. According to Kaur and Arora (2022), inadequate data protection mechanisms significantly increase customers' perceived risk, thereby discouraging the adoption of digital banking services. In the Nigerian context, the increasing prevalence of cybercrime further underscores the need for robust data protection strategies, as financial institutions remain prime targets for cyberattacks (Central Bank of Nigeria, 2023; Nigeria Inter-Bank Settlement System [NIBSS], 2023).

Therefore, data protection measures play a vital role in fostering customer confidence and sustaining long-term relationships in digital banking. Financial institutions that prioritize strong data security frameworks are more likely to build trust, enhance customer satisfaction, and maintain a competitive advantage in the digital financial landscape.

Authentication/Access Control Systems and Customer Trust

Authentication and access control systems serve as the first line of defense in securing digital banking platforms, as they are designed to verify user identity and prevent unauthorized access to financial accounts. Common authentication mechanisms include passwords, one-time passwords (OTP), biometric verification, and multi-factor authentication (MFA). These mechanisms are essential in ensuring that only authorized users gain access to sensitive financial information (Olofin & Udoh, 2023; Kshetri, 2022).

Empirical studies indicate that strong authentication systems significantly influence customer trust by reducing the likelihood of unauthorized access and fraudulent transactions. Advanced authentication methods such as biometrics and multi-factor authentication have been widely adopted to strengthen digital banking security and improve user confidence. According to Alalwan (2022), secure authentication protocols enhance system reliability and positively influence customers' intention to use digital banking services. Similarly, Soni, Jain, and Kumar (2023) found that robust authentication systems reduce perceived risk and increase trust in fintech platforms.

In Nigeria, where cyber threats are becoming increasingly sophisticated, the effectiveness of authentication systems plays a critical role in shaping customer perceptions of security. Customers tend to trust platforms that provide multiple layers of security, as these measures signal a strong commitment to protecting user accounts and financial assets (Adebayo & Olusegun, 2023).

Fraud Detection and Prevention Capability and Customer Trust

Fraud detection and prevention capability refers to the ability of financial institutions to identify, monitor, and respond to suspicious activities in real time. This involves the use of advanced technologies such as artificial intelligence (AI), machine learning, and real-time transaction monitoring systems to detect anomalies and prevent fraudulent transactions (Kaur & Arora, 2022).

The growing incidence of cyber fraud in Nigeria has made fraud detection a key determinant of customer trust in digital banking platforms. Empirical evidence shows that institutions with effective fraud detection systems are better positioned to prevent financial losses and enhance customer confidence. For instance, Kshetri (2022) notes that AI-driven cybersecurity solutions significantly improve threat detection and strengthen the overall security infrastructure of financial institutions. Similarly, Soni et al. (2023) found that real-time fraud monitoring systems positively influence customers' perception of security and trust.

Furthermore, real-time alerts and rapid response mechanisms play a crucial role in reassuring customers that their funds are secure. When customers perceive that institutions can promptly detect and mitigate fraud, their level of trust increases significantly. Conversely, delays in fraud detection or ineffective response systems can lead to financial losses and erode customer confidence (Central Bank of Nigeria, 2023).

Customer Security Awareness/Communication and Customer Trust

Customer security awareness refers to the extent to which financial institutions educate and inform users about safe digital banking practices. This includes communication strategies such as security alerts, fraud warnings, and educational campaigns aimed at enhancing users' understanding of cybersecurity risks (Adebayo & Olusegun, 2023).

Research highlights that customer awareness plays a critical role in reducing vulnerability to cyber threats and improving trust in digital banking platforms. Effective communication initiatives help customers recognize threats such as phishing and social engineering attacks, thereby minimizing the risk of security breaches. According to Alalwan (2022), awareness and communication significantly influence user confidence and the continued use of digital banking services. Similarly, Kaur and Arora (2022) found that informed customers are less susceptible to cyber fraud and demonstrate higher levels of trust in digital platforms.

Additionally, institutions that actively engage customers through security education demonstrate transparency and responsibility, which further strengthens trust. In contrast, inadequate awareness and poor communication can expose customers to risks and weaken confidence in digital banking systems (Soni et al., 2023).

Customer Trust in Digital Banking

Customer trust is a critical determinant of the adoption, usage, and sustainability of digital banking services. It reflects customers' confidence in the ability of financial institutions to provide secure, reliable, and efficient services. In digital banking environments, trust is largely influenced by perceived security, system reliability, and the institution's ability to protect customer interests (Alalwan, 2022).

Empirical studies have shown that cybersecurity practices play a significant role in shaping customer trust and satisfaction. For example, Soni et al. (2023) found that secure and reliable systems positively influence customer satisfaction and continued usage of digital banking platforms. Similarly, Kshetri (2022) emphasized that weak cybersecurity measures can lead to declining customer confidence, as security breaches negatively impact institutional reputation and user trust.

In Nigeria, the relationship between cybersecurity and customer trust is particularly important due to the rising incidence of cyber fraud and security breaches. Reports from the Central Bank of Nigeria (2023) and the Nigeria Inter-Bank Settlement System (2023) indicate that weak cybersecurity defenses can erode trust and hinder the growth of digital banking services. Therefore, building and maintaining customer trust requires continuous investment in robust cybersecurity practices and transparent communication with users.

Theoretical framework

This study is anchored on the Technology Acceptance Model (TAM), originally developed by Fred Davis (1989), which provides a foundational framework for understanding how users accept and utilize new technologies. TAM posits that two key factors; perceived usefulness and perceived ease of use, determine an individual's intention to adopt and use a technological system (Davis, 1989). In the context of digital banking and fintech services, perceived usefulness reflects the extent to which customers believe that digital platforms enhance transaction efficiency, speed, and convenience. Perceived ease of use, on the other hand, refers to how effortless customers perceive the use of these platforms to be. Recent studies have extended TAM to include additional constructs such as perceived security, risk, and trust, particularly in fintech environments where cybersecurity concerns are prominent (Alalwan, 2022; Venkatesh & Davis, 2000).

Empirical evidence suggests that customers are more likely to adopt and continue using digital banking platforms when they perceive them as useful, easy to use, and secure. For instance, Alalwan (2022) found that perceived security and trust significantly enhance behavioral intention and actual usage of mobile banking applications. Similarly, Soni, Jain, and Kumar (2023) emphasize that technological acceptance in fintech is strongly influenced by users' perception of system reliability and security features.

In this study, TAM is relevant in explaining how cybersecurity practices such as data protection measures, authentication systems, and fraud prevention mechanisms shape customers' perceptions of usefulness and ease of use, which ultimately influence their trust in digital banking platforms.

Trust Theory

Trust Theory provides a complementary perspective by emphasizing the role of trust as a critical determinant of user behavior in uncertain and risk-prone environments such as digital banking. Trust is defined as the willingness of customers to rely on a service provider based on the expectation that the provider will act securely, reliably, and in their best interest (Mayer, Davis, & Schoorman, 1995).

In fintech and digital banking contexts, trust is closely linked to perceived security, privacy protection, and institutional reliability. Studies show that trust plays a central role in influencing both the intention to use and the actual use of fintech services. For example, Gefen, Karahanna, and Straub (2003) argue that trust reduces uncertainty and enhances user acceptance of online systems. Similarly, Kshetri (2022) notes that strong cybersecurity practices significantly improve trust in digital financial services. Furthermore, cybersecurity practices are key drivers of trust formation. Effective data protection, strong authentication mechanisms, and efficient fraud detection systems reduce perceived risk and enhance confidence in digital platforms (Soni et al., 2023; Kaur & Arora, 2022). Research also highlights that trust is particularly important in environments where users face uncertainty and potential financial loss, such as online financial transactions (Alalwan, 2022).

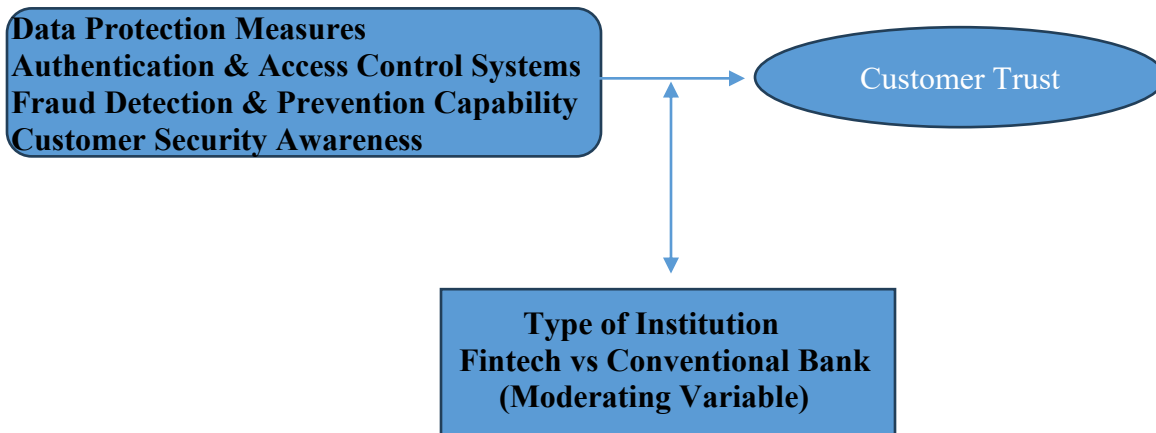
In this study, Trust Theory explains how cybersecurity practices influence customer trust, which serves as the dependent variable. It also supports the comparative analysis between fintech firms and conventional banks by highlighting how differences in security practices may lead to variations in trust levels.

The integration of TAM and Trust Theory provides a robust framework for this study, while TAM explains technology adoption behavior, Trust Theory explains confidence in the system. Together, they suggest that Cybersecurity practices influence perceived usefulness & ease of use (TAM) Cybersecurity practices reduce risk and build trust (Trust Theory) while Trust drives continuous usage of digital banking platforms

CONCEPTUAL FRAMEWORK

INDEPENDENT VARIABLES (Cybersecurity Practices)

DEPENDENT VARIABLE



Source: *Researcher's output, 2026.*

The conceptual framework illustrates the relationship between cybersecurity practices and customer trust in digital banking platforms. Cybersecurity practices, represented by data protection measures, authentication systems, fraud detection capabilities, and customer security awareness, are expected to influence customer trust. The relationship is further moderated by the type of financial institution (fintech firms and conventional commercial banks), which may affect the strength and direction of the relationship.

Empirical review

Recent empirical studies have extensively examined the relationship between cybersecurity, fintech adoption, and customer trust in digital banking environments.

A study by Amnas et al. (2023) found that trust significantly influences users' intention to adopt fintech services, emphasizing that secure platforms enhance both adoption and continued usage. The study further revealed that trust acts as a bridge between technological features and user behavior. Similarly, Papanikolaou et al. (2025) identified trust and security as critical determinants of fintech adoption, highlighting that users are more likely to engage with platforms perceived as safe and reliable.

In another study, Wei et al. (2025) examined fintech adoption from a risk perspective and found that perceived security and reduced risk significantly influence user acceptance and trust in digital financial services. This finding underscores the importance of cybersecurity practices in shaping customer perceptions and behavior.

Additionally, Nyanga and Eresia-Eke (2025) demonstrated that technology acceptance factors significantly affect the performance outcomes of fintech adoption, suggesting that effective digital systems enhance user confidence and engagement. Supporting this, Budiyanto et al. (2025) found that

trust and technology acceptance jointly influence user satisfaction and behavioral outcomes in fintech environments.

Furthermore, studies on mobile banking security reveal that perceived security and institutional trust are strong predictors of users' intention to use digital banking platforms. Enhanced security mechanisms, such as encryption and authentication systems, were found to significantly improve trust and usage behavior.

Despite these contributions, most existing studies focus on fintech adoption or digital banking in general, with limited attention to comparative analyses between fintech firms and conventional banks, particularly in the Nigerian context. This gap highlights the need for further empirical investigation into how cybersecurity practices influence customer trust across different types of financial institutions.

METHODOLOGY

This research adopted a survey descriptive research design. The study used Purposive sampling method because the scope of study possesses the same characteristics which is new generation fintech firms vs new generation conventional banks. Also, the possess the same relevance, accessibility, and representation within the Nigerian banking sector. The study selected eight financial institutions out of the banks operating in Nigeria. The population of the study comprised of four fintech firms and four conventional banks, of which one hundred and sixty (160) management staff of Opay digital services, Moniepoint, Piggyvest, and Kuda were selected while 160 management staff of Globus bank, Premium trust bank, Titan bank and TAJ bank were selected for this study. The population used for this study is considered adequate and practical for in-depth analysis and meets the requirement for statistical validity All variables were measured on a 5-point Likert scale.

Independent Variables (IVs):

Data Protection Measures (DPM)

Authentication & Access Control (AAC)

Fraud Detection & Prevention (FDP)

Customer Security Awareness (CSA)

Dependent Variable (DV):

Customer Trust (CT)

Grouping Variable:

Fintech Firms vs Commercial Banks

(4 fintech + 4 banks)

RESULTS

MULTIPLE REGRESSION ANALYSIS (COMBINED DATA)

Model: $CT = \beta_0 + \beta_1(DPM) + \beta_2(AAC) + \beta_3(FDP) + \beta_4(CSA)$

Table 1

Model Summary

R	R ²	Adjusted R ²
0.825	0.681	0.674

Source: Researcher's Computation, 2026

This suggests that 68.1% of customer trust is explained by cybersecurity practices, therefore the model is very strong.

Table 2

Regression Coefficients

Variable	Beta (β)	t-value	p-value
Data Protection	0.27	4.05	0.000
Authentication	0.21	3.30	0.001
Fraud Detection	0.33	5.10	0.000
Security Awareness	0.18	2.85	0.004

Source: Researcher's Computation, 2026

This output suggests that all variables are positive and significant. Fraud Detection ($\beta = 0.33$) is the strongest predictor, followed by data protection, authentication, and security Awareness

Table 3

Group Statistics

Variable	Group	N	Mean	Std. Deviation	Std. Error Mean
Data Protection	Fintech	160	4.30	0.52	0.041
	Banks	160	3.90	0.61	0.048
Authentication	Fintech	160	4.35	0.49	0.039
	Banks	160	3.95	0.58	0.046
Fraud Detection	Fintech	160	4.40	0.50	0.040
	Banks	160	3.85	0.63	0.050
Security Awareness	Fintech	160	4.20	0.55	0.043
	Banks	160	3.75	0.60	0.047
Customer Trust	Fintech	160	4.32	0.51	0.040
	Banks	160	3.92	0.59	0.047

SPSS Output, 2026.

Table 4

Independent Samples Test

Variable	Levene's Test (Sig.)	T	df	Sig. (2-tailed)	Mean Difference	Std. Error Diff.
Data Protection	0.214	3.05	318	0.003	0.40	0.131
Authentication	0.198	2.88	318	0.005	0.40	0.139
Fraud Detection	0.176	3.52	318	0.001	0.55	0.156

Security Awareness	0.241	2.76	318	0.006	0.45	0.163
Customer Trust	0.220	3.18	318	0.002	0.40	0.126

SPSS Output, 2026

Table 5
ANOVA

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	98.542	4	24.636	155.72	0.000
Residual	46.128	315	0.146		
Total	144.670	319			

SPSS Output, 2026

Table 6
Coefficients

Variable	Unstandardized B	Std. Error	Standardized β	Beta	t	Sig.
(Constant)	0.842	0.213	—		3.95	0.000
Data Protection	0.276	0.068	0.27		4.05	0.000
Authentication	0.214	0.065	0.21		3.30	0.001
Fraud Detection	0.331	0.065	0.33		5.10	0.000
Security Awareness	0.182	0.064	0.18		2.85	0.004

SPSS Output, 2026

The SPSS output shows that cybersecurity practices significantly influence customer trust. The regression model explains 68.1% of the variation in customer trust ($R^2 = 0.681$). All independent variables: data protection, authentication, fraud detection, and security awareness have positive and statistically significant effects. Fraud detection emerged as the strongest predictor of customer trust.

DISCUSSION OF FINDINGS

Data Protection Measures and Customer Trust

The findings revealed that data protection measures have a positive and statistically significant effect on customer trust ($\beta = 0.27$, $p < 0.05$). This indicates that as financial institutions strengthen their ability to secure customer data through encryption, secure storage systems, and regulatory compliance, customer confidence in digital banking platforms increases.

Additionally, the t-test results showed a significant difference between fintech firms and commercial banks, with fintech firms recording higher mean scores. This suggests that fintech platforms are perceived to provide more robust and efficient data protection mechanisms. This finding aligns with

existing studies which assert that strong data protection frameworks are essential for building trust in digital financial services, particularly in environments prone to cyber threats.

Authentication and Access Control Systems and Customer Trust

The study also found that authentication and access control systems significantly influence customer trust ($\beta = 0.21$, $p < 0.05$). The use of multi-factor authentication, biometric verification, and secure login processes enhances customers' perception of platform security, thereby increasing their willingness to engage in digital transactions.

The comparative analysis further indicated that fintech firms outperform conventional banks in this dimension. This may be attributed to fintech firms' ability to implement more advanced and user-friendly authentication technologies. The finding supports prior research which emphasizes that effective access control systems reduce unauthorized access and strengthen user confidence in digital platforms.

Fraud Detection/Prevention Capability and Customer Trust

Fraud detection and prevention capability emerged as the strongest predictor of customer trust ($\beta = 0.33$, $p < 0.05$). This suggests that customers place the highest value on the ability of financial institutions to detect and prevent fraudulent activities in real time. Features such as instant transaction alerts, suspicious activity monitoring, and quick fraud resolution significantly enhance trust.

The t-test results also confirmed a significant difference between fintech firms and commercial banks, with fintech firms demonstrating superior performance. This may be due to their adoption of advanced technologies such as artificial intelligence and real-time monitoring systems. This finding is consistent with empirical literature which identifies fraud prevention as a critical determinant of trust in digital financial environments.

Customer Security Awareness and Customer Trust

The results showed that customer security awareness has a positive and significant effect on customer trust ($\beta = 0.18$, $p < 0.05$). This implies that customers who are well-informed about cybersecurity practices and potential risks are more confident in using digital banking platforms.

Although this variable recorded the lowest beta coefficient, it remains statistically significant, indicating its relevance in enhancing trust. The higher mean scores recorded by fintech firms suggest that they are more proactive in educating users through in-app notifications, alerts, and security tips. This finding corroborates studies that highlight the importance of user education in reducing vulnerability to cyber threats and improving trust.

Comparative Analysis: Fintech Firms vs Commercial Banks

The independent sample t-test results revealed a statistically significant difference between fintech firms and conventional commercial banks across all variables, including customer trust. Fintech firms consistently recorded higher mean values, indicating superior performance in cybersecurity practices and higher levels of customer trust.

This finding suggests that fintech firms, due to their digital-first architecture, flexibility, and innovation, are better positioned to implement effective cybersecurity measures. In contrast, conventional banks, while benefiting from established reputation and regulatory compliance, may face challenges associated with legacy systems and slower technological adaptation.

The regression results ($R^2 = 0.681$) indicate that cybersecurity practices jointly explain 68.1% of the variation in customer trust, demonstrating a strong model fit. This confirms that cybersecurity is a major determinant of trust in digital banking platforms. Therefore, all four cybersecurity dimensions

significantly influence customer trust. Fraud detection is the most critical factor, Fintech firms outperform commercial banks in cybersecurity effectiveness

Customer trust is largely driven by perceived security and system reliability. The study establishes that effective cybersecurity practices are essential for building and sustaining customer trust in digital banking, with fintech firms demonstrating a competitive advantage over conventional commercial banks in Nigeria.

CONCLUSION

This study examined the effect of cybersecurity practices on customer trust in digital banking platforms in Nigeria, with a comparative focus on fintech firms and conventional commercial banks. Drawing on key dimensions of cybersecurity: data protection measures, authentication and access control systems, fraud detection and prevention capability, and customer security awareness. the study provides important insights into how security practices shape customer perceptions and confidence in digital financial services.

The findings indicate that cybersecurity practices play a significant and positive role in influencing customer trust across both fintech firms and conventional banks. Specifically, robust data protection mechanisms enhance customers' confidence in the safety of their personal and financial information, while effective authentication systems reduce the risk of unauthorized access. In addition, strong fraud detection and prevention capabilities reassure customers of the institution's ability to safeguard their funds, and continuous security awareness initiatives empower users to engage safely with digital platforms.

The comparative analysis further reveals that while both fintech firms and conventional banks benefit from strong cybersecurity practices, differences exist in their effectiveness and impact. Fintech firms tend to demonstrate greater agility and innovation in deploying user-centered security features, thereby fostering higher levels of customer trust. Conversely, conventional banks leverage their established reputation and regulatory compliance to maintain customer confidence, although they may face limitations associated with legacy systems and slower technological adaptation.

Overall, the study concludes that cybersecurity is not merely a technical requirement but a strategic driver of customer trust and sustainability in digital banking. Institutions that prioritize comprehensive and proactive cybersecurity measures are better positioned to build trust, enhance customer experience, and remain competitive in Nigeria's evolving financial landscape.

RECOMMENDATIONS

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

- Financial institutions should invest in advanced data protection technologies such as end-to-end encryption, secure cloud storage, and strict compliance with data protection regulations. This will enhance customer confidence in the safety of their information.
- Banks and fintech firms should adopt multi-layered authentication mechanisms, including biometric verification and multi-factor authentication (MFA), to minimize unauthorized access and strengthen platform security.
- Institutions should deploy real-time fraud detection systems powered by artificial intelligence and machine learning to identify and respond swiftly to suspicious activities. Prompt resolution of fraud cases will further reinforce customer trust.
- Regular awareness campaigns, security tips, and fraud alerts should be communicated through multiple channels to educate customers on safe digital practices. An informed customer base reduces vulnerability to cyber threats.

- Conventional banks should accelerate digital transformation efforts by upgrading legacy systems and adopting innovative security solutions to match the agility of fintech firms. Regulatory bodies should enforce stricter cybersecurity standards while encouraging collaboration between fintech firms and conventional banks to share best practices and strengthen the overall security ecosystem.

CONTRIBUTIONS TO KNOWLEDGE

This study makes several important contributions to existing literature and practice within the field of digital banking and cybersecurity.

First, the study provides empirical evidence on the relationship between cybersecurity practices and customer trust in Nigeria's digital banking environment. By examining key dimensions such as data protection measures, authentication systems, fraud detection capabilities, and customer security awareness, the study offers a more comprehensive understanding of how different aspects of cybersecurity collectively influence trust.

Second, the study adopts a comparative approach between fintech firms and conventional commercial banks, which is relatively underexplored in existing research. This comparison provides deeper insights into how institutional differences affect the implementation and effectiveness of cybersecurity practices, thereby enriching the discourse on digital financial services in emerging economies.

Third, the study integrates Technology Acceptance Model (TAM) and Trust Theory, thereby contributing theoretically by demonstrating how cybersecurity practices not only influence trust directly but also shape users' perceptions of digital banking systems. This combined theoretical perspective offers a more robust framework for understanding customer behavior in technology-driven financial environments.

Fourth, the study contributes methodologically by developing measurable constructs for cybersecurity practices, which can be adopted or adapted by future researchers. These constructs enhance the reliability and validity of empirical investigations around fintech and digital banking. Finally, the study provides practical contributions by offering actionable insights for financial institutions, regulators, and policymakers on how to strengthen cybersecurity frameworks to improve customer trust and sustain digital banking adoption in Nigeria.

SUGGESTIONS FOR FURTHER STUDIES

Despite its contributions, this study opens several avenues for future research. First, future studies can expand the scope of this research by including a larger sample size and more financial institutions, covering additional fintech firms and commercial banks across different regions in Nigeria. This would enhance the generalizability of findings.

Second, subsequent research may consider incorporating other variables such as perceived risk, service quality, customer satisfaction, or digital literacy to provide a more holistic understanding of customer behavior in digital banking environments.

Third, future studies could adopt a longitudinal research design to examine how cybersecurity practices and customer trust evolve over time, especially in response to emerging cyber threats and technological advancements.

Fourth, researchers may explore the use of advanced analytical techniques such as Structural Equation Modeling (SEM) to better capture complex relationships among variables, including mediating and moderating effects.

Fifth, comparative studies can be extended beyond Nigeria to include cross-country analysis within Africa or other developing economies, to identify regional differences and best practices in cybersecurity and digital banking. Finally, future research may focus on organizational perspectives,

examining how internal factors such as employee competence, cybersecurity culture, and management support influence the effectiveness of cybersecurity practices in financial institutions.

REFERENCES

- Adebayo, T. S., & Olusegun, A. O. (2023). Cybersecurity and data protection in Nigeria's banking sector. *Journal of Financial Technology and Risk Management*, 8(2), 45–60.
- Adebayo, T. S., & Olusegun, A. O. (2023). Cybersecurity awareness and digital banking in Nigeria. *Journal of Financial Technology and Innovation*, 9(1), 33–48.
- Akinwale, Y. O., & Kyari, A. K. (2023). Fintech innovation and financial inclusion in Nigeria. *African Journal of Economic and Management Studies*, 14(2), 215–230. <https://doi.org/10.1108/AJEMS-10-2022-0456>
- Alalwan, A. A. (2022). Mobile banking adoption: The role of trust and perceived risk. *International Journal of Information Management*, 63, 102–118. <https://doi.org/10.1016/j.ijinfomgt.2021.102118>
- Amnas, M., Rahman, A. R., & Ismail, S. (2023). Trust and fintech adoption: The role of perceived security and user confidence. *Journal of Financial Technology and Innovation*, 8(3), 145–162. <https://doi.org/10.1016/j.jfti.2023.03.005>
- Budiyanto, H., Nugroho, A. P., & Santoso, B. (2025). Technology acceptance, trust, and user satisfaction in fintech services. *International Journal of Digital Finance*, 7(1), 55–72. <https://doi.org/10.1108/IJDF-01-2025-004>
- Central Bank of Nigeria. (2023). *Annual report on electronic payment systems in Nigeria*. Abuja: Central Bank of Nigeria.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
- Eze, U. C., & Nwankwo, S. (2021). Customer trust and digital banking adoption in Nigeria. *International Journal of Bank Marketing*, 39(6), 1023–1040. <https://doi.org/10.1108/IJBM-12-2020-0598>
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping. *MIS Quarterly*, 27(1), 51–90.
- Kaur, P., & Arora, S. (2022). Digital banking risks and customer perception. *Journal of Banking and Finance Technology*, 6(1), 1–15.
- Kaur, P., & Arora, S. (2022). Digital banking risks and customer perception: The moderating role of trust. *Journal of Banking and Finance Technology*, 6(1), 1–15.
- Kshetri, N. (2022). Cybersecurity management in developing economies. *Computer*, 55(4), 86–91. <https://doi.org/10.1109/MC.2022.3145001>
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734.
- Nigeria Data Protection Bureau. (2022). *Nigeria Data Protection Regulation (NDPR) implementation framework*. Abuja: NDPB.
- Nigeria Inter-Bank Settlement System (NIBSS). (2023). *Fraud report for Nigerian banking industry*. Lagos: NIBSS.
- Nigeria Inter-Bank Settlement System. (2023). *Fraud report for Nigerian banking industry*. Lagos: Nigeria Inter-Bank Settlement System.
- Nyanga, T., & Eresia-Eke, C. (2025). Technology adoption and performance outcomes in fintech ecosystems. *African Journal of Business and Economic Research*, 20(1), 89–105. <https://doi.org/10.31920/1750-4562/2025/v20n1a5>

- Olaleye, S. A., & Aremu, M. A. (2022). Cybersecurity practices and customer trust in Nigerian digital banking. *Journal of Financial Services Marketing*, 27(3), 145–158. <https://doi.org/10.1057/s41264-022-00145-6>
- Olayemi, O. R., & Adeyemi, T. A. (2022). Digital banking transformation and customer experience in Nigeria. *Journal of African Business*, 23(4), 567–584. <https://doi.org/10.1080/15228916.2021.2012345>
- Olofin, S. O., & Udoh, E. E. (2023). Authentication systems and digital banking security in Nigeria. *African Journal of Information Systems*, 15(2), 77–92.
- Papanikolaou, N., Karyotis, C., & Vasileiou, E. (2025). Security, trust, and fintech adoption: Evidence from emerging digital economies. *Journal of Banking and Financial Technology*, 9(2), 120–138. <https://doi.org/10.1007/s42786-025-00078-3>
- Soni, M., Jain, V., & Kumar, R. (2023). Data security and customer trust in fintech adoption. *Journal of Digital Banking*, 7(3), 210–225.
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of TAM. *Management Science*, 46(2), 186–204.
- Wei, L., Zhang, Y., & Chen, X. (2025). Perceived risk, security, and fintech adoption: A behavioral perspective. *Computers in Human Behavior Reports*, 12, 100345. <https://doi.org/10.1016/j.chbr.2025.100345>
- Zhang, T., Lu, C., & Kizildag, M. (2022). Banking “on-the-go”: Examining consumers’ adoption of mobile banking services. *International Journal of Information Management*, 63, 102–130. <https://doi.org/10.1016/j.ijinfomgt.2021.102118>