Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 12. No. 2, 2024 Series

Article Citation Format
Agwi, C. U. & Akpojaro, J. (2024): An Exploratory Study of Fintech Security Concerns among its Users in Nigeria. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 12, No. 2. Pp 17-28.
www.isteams.net/digitaljournal.
dx.doi.org/10.22624/AIMS/DIGITAL/V11N2P3

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received: 11th February, 2024
Review Type: Blind Peer
Final Acceptance: 22nd April, 2024

An Exploratory Study of Fintech Security Concerns among its Users in Nigeria

[1]Agwi, C. U. & [2]Akpojaro, J.
[1,2]Department of Mathematics and Computer Science
University of Africa
Toru-Orua, Bayelsa State
E-mails: celestine.agwi@uat.edu.ng, jackson.akpojaro@uat.edu.ng
Corresponding Author: jakpojaro@yahoo.com

ABSTRACT

The rapid growth of financial technology (Fintech) in Nigeria has revolutionized the way people conduct financial transactions. However, this technological advancement brings along a host of security concerns that impact users' trust and confidence in using Fintech platforms. This exploratory study aims to investigate the security concerns among Fintech users in Nigeria, shedding light on the underlying factors contributing to these concerns. This research employs a mixed-methods approach, combining qualitative interviews and quantitative surveys to gather comprehensive data. The qualitative phase involves in-depth interviews with a diverse sample of Fintech users, exploring their perceptions, experiences, and concerns related to the security aspects of Fintech services. The quantitative phase consists of a survey administered to a larger sample, aiming to quantify the prevalence and intensity of security concerns among Fintech users in Nigeria. The results highlighted the importance of addressing data breaches, privacy concerns, and authentication methods to alleviate user apprehensions. Participants expressed a desire for more transparency regarding the security practices of Fintech providers through improved communication and education to enhance user awareness and understanding of the security measures in place. This corroborates the notion that users' trust in Fintech services is depends on their perception of the security measures implemented by providers. The study's contribute to the existing literature on Fintech security, providing an in-depth understanding of the specific security concerns faced by Nigerian users, and identify potential strategies to enhance the security measures and alleviate users' concerns, which will ultimately foster greater adoption and utilization of Fintech services.

Keywords: Fintech, financial services, security concerns, privacy, data breaches

1. INTRODUCTION

Fintech is an abridge form for financial technology that encompasses a broad range of digital platforms, applications, and solutions that utilize advancements in technology, such as mobile devices, artificial intelligence, blockchain, and data analytics, to transform financial transactions and services (Demirgüç-Kunt *et al.,* 2020).

International Monetary Fund (IMF), defined Fintech as innovation in financial services that leverages technology to deliver new and improved financial products and services (IMF, 2020). Fintech has emerged as a significant driver for change in the financial industry, bringing about numerous benefits that have enhanced financial inclusion as well as providing access to financial services for underserved populations (Klapper *et al.,* 2019). Through mobile banking, digital wallets, and peer-to-peer lending platforms, Fintech has extended financial services to previously unbanked or underbanked individuals, facilitating economic participation and reducing inequalities (World Bank, 2020).

Fintech has also greatly improved the efficiency and cost-effectiveness of financial transactions. By automating processes and leveraging digital platforms, Fintech has streamlined payment systems, reduced transaction costs, and enhanced operational efficiency for both financial institutions and consumers (Biswas *et al.*, 2021; Yermack, 2017). In terms of customer experiences, Fintech has revolutionized the way individuals interact with financial services. Personalized solutions, user-friendly interfaces, and data-driven insights have empowered users to have greater control over their finances, access real-time information, and make informed decisions (Gomber *et al.*, 2018).

Despite the transformative impact Fintech has brought, it is not without security risks and vulnerabilities. The increasing reliance on digital platforms and the storage of sensitive financial data have brought new challenges in terms of security. Many users who entrust Fintech platforms with their personal and financial information have brought some concerns about data breaches and unauthorized access a very serious issue for consideration (Lacity *et al.*, 2020). The risk of cyberattacks and identity theft is prevalent in the Fintech ecosystem. Attackers target Fintech platforms to gain unauthorized access to user data, which can lead to financial fraud or misuse of personal information (Hua *et al.*, 2021). Additionally, the rise of mobile Fintech applications has introduced specific risks related to mobile device security, including malware infections, phishing attacks, and the compromise of user credentials (Kim *et al.*, 2019).

To address these concerns, regulatory frameworks, encryption technologies, multi-factor authentication mechanisms, and ongoing monitoring are employed (Laudon & Laudon, 2020). However, understanding the specific security concerns faced by Fintech users in Nigeria is crucial for developing tailored strategies to mitigate the risks effectively. In this study, we will conduct an exploratory investigation of security concerns among Fintech users in Nigeria. Through a mixed-methods approach involving qualitative interviews and quantitative surveys; we aim to gain comprehensive insights into the underlying factors contributing to these concerns. The findings will contribute to the development of strategies and recommendations to enhance security measures and alleviate users' concerns, ultimately fostering greater adoption and utilization of Fintech services.

2. LITERATURE REVIEW

Numerous studies have investigated the security concerns in Fintech, providing valuable insights into the various dimensions of these issues. Smith & Telang (2016) conducted a comprehensive analysis of security breaches in the Fintech sector, highlighting the growing frequency and severity of cyberattacks targeting financial institutions. Their research emphasized the need for robust security measures and proactive risk management strategies. Also, Lee & Yoon (2019) conducted a systematic review of the literature on Fintech security concerns, identifying key themes such as data breaches, privacy concerns, authentication methods, and regulatory challenges.

Their analysis shed light on the multifaceted nature of security concerns and highlighted the importance of user awareness and education in addressing these issues.

2,1 Types of Security Concerns in Fintech

Security concerns in Fintech can manifest in various forms, requiring attention and mitigation strategies. One common concern is data breaches, where sensitive user information, including financial data and personal details, is compromised (Gupta *et al.*, 2020). These breaches can result from cyberattacks, system vulnerabilities, or internal lapses in security protocols (Liébana-Cabanillas *et al.*, 2020). Another significant concern is privacy, as Fintech platforms handle vast amounts of personal data. Users may worry about how their data is collected, stored, and shared with third parties (Ryu *et al.*, 2018). Privacy breaches can erode trust and discourage users from adopting Fintech services. Authentication methods and identity theft are additional concerns. Fintech users expect secure and reliable authentication mechanisms to protect their accounts from unauthorized access (López-González *et al.*, 2020). Failure to implement strong authentication measures can lead to financial fraud and identity theft, damaging users' confidence in Fintech platforms.

2.2 Factors Influencing Security Concerns in Fintech

Several factors influence users' security concerns in the Fintech domain. Trust plays a pivotal role, as users must have confidence in the security measures implemented by Fintech providers (Kshetri, 2017). Trust can be influenced by factors such as platform reputation, transparency in data handling practices, and clear communication regarding security measures (Yoon *et al.*, 2018).

Perceived risk is another important factor. Users assess the potential threats and vulnerabilities associated with using Fintech services, considering factors like financial loss, reputation damage, and negative impacts on personal privacy (Mehmood *et al.*, 2020). Higher perceived risk tends to increase security concerns and decrease user willingness to adopt Fintech platforms. Socio-demographic characteristics, such as age, gender, and educational background, can also shape security concerns. Research has shown that older users may exhibit higher levels of security concerns due to their limited familiarity with technology and potential mistrust of digital platforms (Ndou *et al.*, 2018). Additionally, individuals with higher levels of digital literacy and awareness tend to be more concerned about security and take proactive measures to protect their information (Islam *et al.*, 2019).

2.4 Fintech Landscape in Nigeria

The Fintech landscape in Nigeria has experienced significant growth in recent years, driven by factors such as a large unbanked population, increasing smartphone penetration, and supportive government policies (Eze *et al.*, 2020). The Nigeria Fintech sector encompasses various services, including mobile payments, digital banking, peer-to-peer lending, and investment platforms (Omotoso & Ogunnaike, 2019). While Fintech presents numerous opportunities, security concerns pose challenges to its widespread adoption in Nigeria. The country faces unique security risks, including cybercrime, fraudulent schemes, and inadequate cybersecurity infrastructure (Awe *et al.*, 2021). Understanding the specific security concerns within the Nigerian Fintech context is crucial for developing targeted strategies and regulations to safeguard users and promote the growth of the industry. Though previous researches have shed light on security concerns in the Fintech sector, including data breaches, privacy concerns, and authentication methods. Factors such as trust, perceived risk, and socio-demographic characteristics influence users' security concerns.

Within the Nigerian context, the Fintech landscape is rapidly evolving, presenting both opportunities and security challenges. Analyzing the security concerns specific to the Nigerian Fintech ecosystem will help inform strategies for improving security measures and fostering user trust.

3. METHODOLOGY

3.1 The Study Design

This study employed the mixed-methods research design to gain a comprehensive understanding of the security concerns among Fintech users in Amasoma province in Bayelsa State, Nigeria. Combination of qualitative and quantitative methods allowed for a more holistic exploration of the problem being investigated and provided better insights into the underlying factors contributing to these concerns. The qualitative phase of the study involved an in-depth interview with a diverse sample of Fintech users. A purposive sampling technique was used to select participants who have experience using Fintech platforms in Nigeria. The sample size was determined based on the principle of data saturation, while additional interviews were conducted until no new themes or insights emerged from the data. The inclusion criteria for participants included being at least 18 years old and having used Fintech services within the past six months.

The interviews were conducted face-to-face or through video conferencing, depending on the participants' preferences and geographical locations. Each interview was audio-recorded with the participants' consent and later transcribed for analysis. Semi-structured interview guides were developed to ensure consistency in data collection while allowing flexibility for participants to share their experiences, perceptions, and concerns related to the security aspects of Fintech services. During the interviews, participants were encouraged to share their experiences, concerns, and suggestions regarding the security of Fintech services in Nigeria. Probing questions were asked to delve deeper into specific topics and explore emerging themes. Field notes were taken to capture non-verbal cues, contextual information, and any relevant observations during the interviews. Participants were assured of confidentiality and informed that their participation was voluntary. Informed consent was obtained before the interviews were commenced.

The qualitative data collected through the interviews were analyzed using thematic analysis. The transcribed interviews were carefully read and coded to identify recurring patterns, themes, and categories related to security concerns in Fintech. The initial codes were derived both deductively from the research questions and inductively from the data. These codes were then organized into meaningful themes, and relationships between themes were explored. The qualitative analysis process followed an iterative approach, with constant comparison and refinement of the emerging themes.

For the quantitative survey, the survey instrument developed was based on the findings from the qualitative phase and relevant literature on security concerns in Fintech. The survey consisted of multiple-choice questions, Likert-scale items, and open-ended questions to capture both quantitative and qualitative data. To ensure a representative sample, an online survey platform was utilized to administer the survey. The survey was distributed to Fintech users across different demographic groups including age, gender, education level, and income in Amasoma province in Bayelsa State, Nigeria. To enhance response rate and data quality, various strategies were employed, such as providing clear instructions, ensuring anonymity, and offering incentives for participation. The quantitative survey data were analyzed with descriptive and inferential statistics.

Frequencies and percentages were used to summarize participants' responses to closed-ended survey questions that were conducted to examine associations between variables and identify significant relationships, where applicable. Open-ended survey responses were analyzed using content analysis to extract key themes and insights.

Measures which include maintaining an audit trail of decisions made during analysis, seeking peer debriefing to validate interpretations, and conducting member checking to verify the accuracy of findings with participants were taken to ensure the trustworthiness and rigor of the findings, throughout the data analysis process. The mixed-methods approach ensured that this study provided a comprehensive understanding of security concerns among Fintech users in Nigeria. The triangulation of findings from both methods enhanced the validity and reliability of the study's results.

4. RESULTS AND DISCUSSIONS

This section provides analysis of data obtained from the mixed-methods approach and using qualitative and quantitative data collection**.** The responses were gotten from the three major stakeholders of Fintech such as the Fintech providers, institutions and users.

Fintech Providers: These are the companies or organizations that develop and offer Fintech products and services. They leverage technology and innovation to provide financial solutions, such as mobile payment apps, online lending platforms, robo-advisors, and blockchain-based solutions. Fintech providers aim to meet the evolving needs of customers by offering convenient, efficient, and user-friendly financial services.

Financial Institutions: Traditional financial institutions, such as banks and credit unions, are important stakeholders in the Fintech ecosystem. They often collaborate with or invest in Fintech providers to enhance their own digital capabilities and expand their service offerings. Financial institutions may also face competition from Fintech companies but can leverage their existing infrastructure, customer base, and regulatory expertise to adapt and innovate.

Users: The end-users or customers of Fintech services are essential stakeholders. They include individuals, businesses, and organizations that utilize Fintech solutions for their financial needs. Users benefit from Fintech services by accessing faster, more convenient, and cost-effective financial solutions compared to traditional methods. Users' feedback, needs, and trust are critical to the success and sustainability of Fintech platforms.

4.1 Concerns about the Security of Personal and Financial Information

Table 1 and Figure 1 show responses from users who are concerned about the security of their personal and financial information

Table 1: Concern about the security of personal and financial information

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Fintech Provider	20	45	15	10	10
Fintech Institution	15	35	20	20	10
Users	40	35	10	10	15

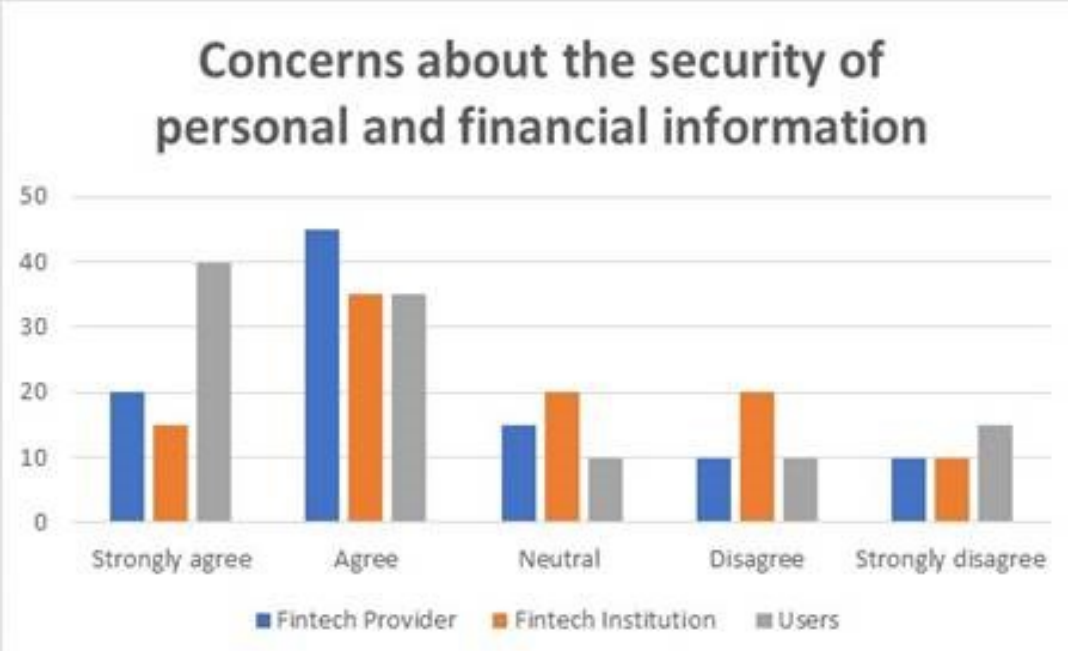

Figure 1: Concerns about the security of personal and financial information

Based on the survey responses, there is a moderate level of concern among Fintech providers, Fintech institutions, and users regarding the security of personal and financial information when using Fintech services. Users expressed the highest level of concern, with 40% strongly agreed while 35% agreed. This indicates a significant need for Fintech providers and institutions to prioritize robust security measures to address users concerns and build trust.

4.2 Worry about Data Breaches or Unauthorized Access

Table 2 and Figure 2 show responses from users concerns about data breaches or unauthorized access to their personal and financial information

Table 2: Worry about the possibility of data breaches or unauthorized access to my information

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Fintech Provider	10	20	30	30	10
Fintech Institution	5	10	15	20	30
Users	40	35	10	10	15

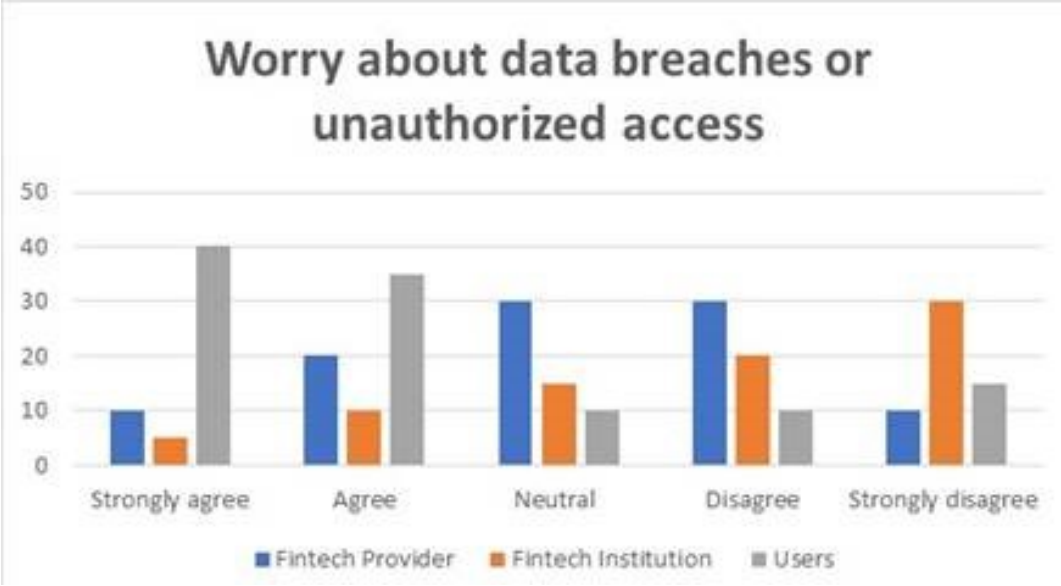

Figure 2: Worry about data breaches or unauthorized access

The survey results highlight a moderate level of worry about data breaches or unauthorized access to information among Fintech providers, Fintech institutions, and users. Users exhibit the highest level of worry, with 40% strongly agreed while 35% agreed. Fintech providers and institutions should consider implementing stringent security protocols and communication strategies to reassure users and mitigate their concerns.

4.3 Concerns about Privacy Practices of Fintech Providers

Table 3 and Figure 3 show responses from users concerns about privacy practices of Fintech providers with respect to how their data is being used

Table 3: Concerns about the privacy practices of Fintech providers

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Fintech Provider	5	15	30	35	15
Fintech Institution	10	25	30	25	10
Users	30	40	15	10	5

Figure 3: Concerns about privacy practices of Fintech providers

Concerns about the privacy practices of Fintech providers and how data is being used are prevalent across all three stakeholder groups, though the extent of concern varies. Users show the highest level of concern, with 30% strongly agreed while 40% agreed. Fintech providers and institutions should focus on transparent privacy policies, data protection practices, and ensuring users have control over their data.

4.4 Confidence in the Security Measures implemented by Fintech Providers

Table 4 and Figure 4 show responses from users concerning their confidence in the security measures implemented by Fintech providers to protect their personal and financial information

Table 4: Confident in the security measures implemented by Fintech providers to protect

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Fintech Provider	25	35	20	15	5
Fintech Institution	20	30	25	20	5
Users	10	25	30	25	10

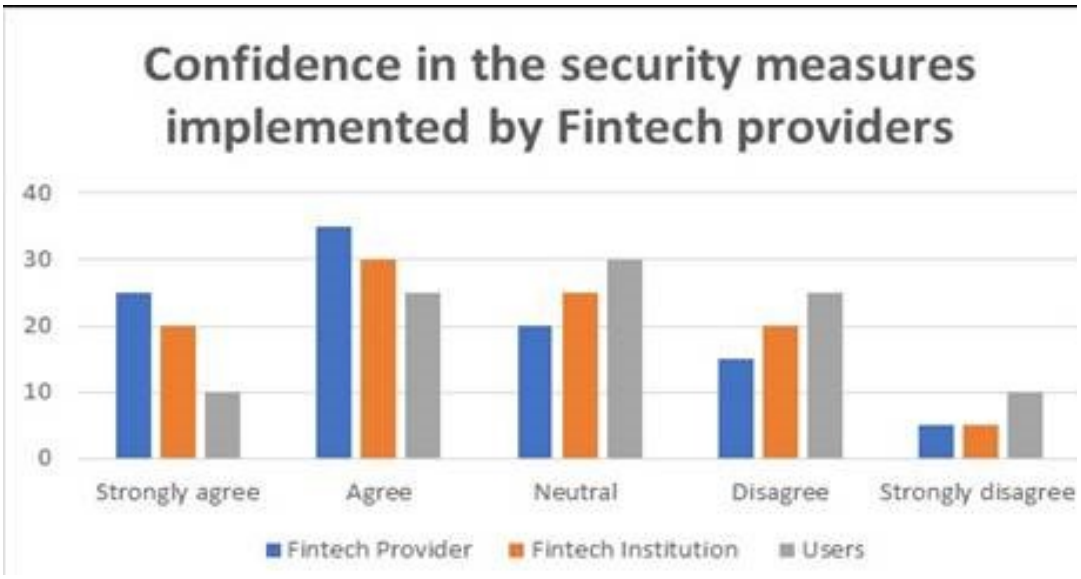

Figure 4: Confidence in the security measures implemented by Fintech providers

Confidence in the security measures implemented by Fintech providers is moderate, with users expressing the lowest level of confidence. Only 10% of users strongly agreed while 25% agreed. Fintech providers and institutions need to enhance their security measures and communicate their efforts effectively to increase user confidence and trust in their platforms.

4.5 Worry about the Risk of Identity theft or Fraudulent Activities

Table 5 and Figure 5 show responses from users with respect to their worry about the risk of identity theft or fraudulent activities to their personal and financial information

Table 5: Worry about the risk of identity theft or fraudulent activities.

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Fintech Provider	5	10	20	40	25
Fintech Institution	5	15	20	40	20
Users	30	40	15	10	5

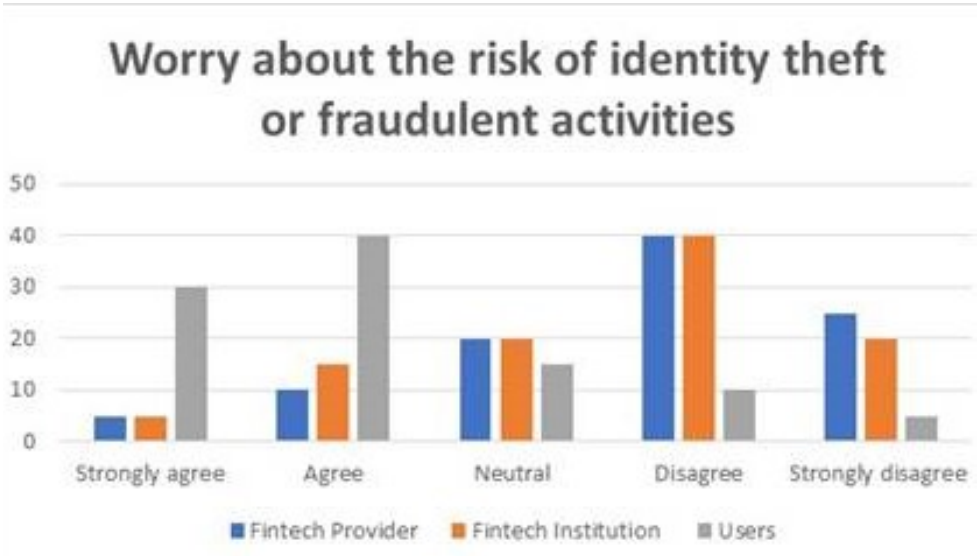

Figure 5: Worry about the risk of identity theft or fraudulent activities

Users show the highest level of worry about the risk of identity theft or fraudulent activities when using Fintech services, with 30% strongly agreed while 40% agreed. Fintech providers and institutions should prioritize robust identity verification processes, fraud detection mechanisms, and user education to address these concerns and protect user information.

The survey responses emphasize the significance of security and privacy concerns among Fintech users in Nigeria. Fintech providers and institutions must invest in comprehensive security measures, transparency, and effective communication strategies to build trust, alleviate concerns, and foster the sustainable growth of the Fintech industry.

5. SUMMARY

The findings of this study align with previous research on security concerns in the Fintech sector. The qualitative and quantitative results both highlighted the importance of addressing data breaches, privacy concerns, and authentication methods to alleviate user apprehensions. These findings support the notion that users' trust in Fintech services is closely tied to their perception of the security measures implemented by providers.

The qualitative findings shed light on the specific concerns of Fintech users. Participants expressed a desire for more transparency and clarity regarding the security practices of Fintech providers. This emphasizes the need for improved communication and education efforts to enhance user awareness and understanding of the security measures in place.

The quantitative results further revealed that younger participants and those with higher levels of digital literacy tend to have higher security concerns. This finding suggests that targeted educational initiatives and user-centric security features may be effective in addressing the specific needs of different user segments.

5.1 Conclusion

The implications of these findings are significant for Fintech providers, policymakers, and users in Nigeria. Fintech providers need to prioritize security measures and invest in robust systems to protect user data. Clear and transparent communication about security practices can help build trust and confidence among users. Policymakers should innovate in developing regulations and standards to ensure the security of Fintech services and protect users' interests. By doing so, the Nigerian Fintech ecosystem can flourish and contribute to financial inclusion and economic growth.

REFERENCES

Awe, O., Alade, T., & Ogunnaike, O. (2021). Fintech in Nigeria: Concept, emergence, and challenges. In M. Saridakis, E. T. Ngwu, & B. Alola (Eds.), Handbook of Research on Fintech Innovation and Entrepreneurship (pp. 218-238). IGI Global.

Biswas, R., Pal, D., & Das, B. (2021). How fintech firms are revolutionizing the financial services industry? A systematic review. *International Journal of Information Management*, 57, 102287.

Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2020). The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. World Bank Policy Research Working Paper No. 8299. World Bank Group.

Eze, S. C., Amankwah-Amoah, J., & Osabutey, E. L. C. (2020). Exploring Fintech developments in Sub-Saharan Africa: The role of institutional factors. *Technological Forecasting and Social Change*, 158, 120155.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems*, 35(1), 220-265.

Gupta, S., Aujla, G. S., & Bhowal, S. (2020). Cybersecurity and financial technology: Issues, challenges, and opportunities. *International Journal of Information Management*, 52, 102069.

Hua, L., Zhu, K., Guo, H., Zhang, M., & Wang, W. (2021). Users' information privacy concerns on mobile Fintech applications. *Computers & Security*, 104, 102235.

IMF. (2020). Fintech and Financial Services: Initial Considerations. International Monetary Fund. Retrieved Date from.https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2020/08/25/Fintech-and-Financial-Services-Initial-Considerations-49640

Islam, M. S., Miah, S. J., & Kabir, N. (2019). Understanding factors influencing users' information security behavior in social media: A systematic review and meta-analysis of the literature. *Computers & Security*, 83, 207-222.

Kim, D., Lee, Y., & Han, I. (2019). Understanding users' mobile Fintech adoption: A Comparative Analysis of South Korea and the United States. *Journal of Global Information Management*, 27(4), 98-116.

Klapper, L., Singer, D., & Ansar, S. (2019). The Global Findex Database 2017: Measuring financial inclusion and the fintech revolution. *Journal of Financial Intermediation*, 39, 1-16.

Kshetri, N. (2017). Can blockchain strengthen the internet of things? *IT Professional*, 19(4), 68-72.

Lacity, M., Yan, A., & Willcocks, L. (2020). AI in business process outsourcing: A research agenda. *MIS Quarterly*, 44(1), 293-316.

Laudon, K. C., & Laudon, J. P. (2020). Management Information Systems: Managing the Digital Firm (16th ed.). Pearson.

Lee, H., & Yoon, C. (2019). Understanding and mitigating security concerns in FinTech: A systematic literature review. *Journal of Business Research*, 104, 77-87.

Liébana-Cabanillas, F., Sánchez-Fernández, J., & Muñoz-Leiva, F. (2020). Internet of Things, Big Data, and Security Risks in Fintech: A systematic literature review. *International Journal of Information Management,* 50, 366-379.

López-González, H., Molina-Castillo, F. J., & Liébana-Cabanillas, F. (2020). Analysis of the impact of information security awareness on the acceptance and use of FinTech services. *International Journal of Information Management*, 52, 101976.

World Bank. (2020). Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. World Bank Group. Retrieved Date from https://globalfindex.worldbank.org/sites/globalfindex/files/2018-04/2017%20Findex%20full%20report_0.pdf