Biometric Authentication and Fraud Detection in Fintech Companies in Nigeria

Ogunjide, Julius Oluwatobi
Master of Business Administration,
Estonian Entrepreneurship University of Applied Sciences, Estonia
Email: onetobile@gmail.com

Awowole Abiodun Olalekan
Bachelor of Software Development and Entrepreneurship
Estonian Entrepreneurship University of Applied Sciences, Estonia
Email: maseabiodun@gmail.com
DOI 10.56201/ijebm.vol.11.no4.2025.pg183.189

Abstract
The increasing reliance on digital financial services in Nigeria has amplified concerns about fraud within the Fintech sector. This study investigates the role of biometric authentication technologies—specifically iris/retina scanning and fingerprint identification systems—in detecting and curbing fraud in Nigerian Fintech companies. Leveraging a descriptive survey research design, data were gathered from 170 respondents comprising customers and staff of selected Fintech firms through structured questionnaires. The study utilized descriptive and inferential statistics to analyze the relationship between biometric technologies and fraud detection. Findings reveal a significant positive relationship between iris/retina biometric systems and fraud detection, suggesting that advanced biometric technologies enhance the security infrastructure of Fintech services. However, despite these advancements, fraud persists, emphasizing the need for continuous innovation and multi-layered security frameworks. The study recommends enhanced adoption of biometric systems alongside other robust authentication measures to strengthen fraud prevention mechanisms in Nigeria' s rapidly evolving digital financial landscape.

Keywords*: Biometric Authentication, Fraud Detection, Fintech, Iris Scanning, Fingerprint Identification, Nigeria.*

Introduction

Financial fraud entails the employment of fraudulent or illegal methods in getting monetary advantages. It involves finding illegal means, bypassing the financial institutions as well as legal procedures and processes in obtaining gains and access to institutional finances or information. This can occur across several financial sectors like banking, insurance, taxation, and corporate settings (Ashtiani & Raahemi, 2022).

According to Reurink (2019), financial fraud consists of three main categories: deceptive financial disclosures, financial scams, and fraudulent financial mis-selling. False financial disclosures consist of misleading assertions on an investment entity's performance or financial condition, whereas financial scams are fraudulent schemes designed to obtain funds or sensitive information from individuals. Fraudulent financial mis-selling entails deceptive marketing or counsel concerning financial products or services. Although contemporary discourse addresses

numerous financial crimes, including mismanagement and money laundering, it is essential to acknowledge that financial fraud has historical origins that before the digital era.

It is important to note that, several attempts have been made in the age of digital technology to curb this fraud activities in the financial sector. Rahman et al. (2021) have recognized the advancement of technology and the advent of the digital era as variables that enhance the complexity and prevalence of fraud in the financial industry. This has also hindered developments that are directed towards improvement in the financial services. The contemporary interconnected global financial system, which enables local and international transactions, along with technical advancements like the internet and electronic fund transfers, provides opportunities for financial criminals to execute fraudulent schemes.

Development via technological innovations in the financial sector has however been improved with the advent of financial technological services often referred to as Fintechs. These solutions and services were developed to ease financial activities in the sector thereby providing viable solutions to different issues that are synonymous with the sector. These has been achieved via the use of different models like use of artificial intelligence, big data among others. Big data use has empowered fintech to contest traditional financial intermediaries, such as Deposit Money Banks (DMBs), by implementing innovative business models (Awotunde et al., 2021).

Fintech companies have expanded their services beyond traditional payment solutions to encompass insurance, loans, savings, and investments. Utilizing technology, they can broaden their clientele without significant investment in infrastructure. This results in decreased expenses in financial intermediation and facilitates improvements in products and services for clients. In 2016, electronic payment transactions in Nigeria experienced a 32.5% increase, totaling N83.1 trillion, up from N62.7 trillion the preceding year. This has shown the unprecedented improvements in the adoption of fintechs in providing financial solutions in the sector.

Fintech has become a significant force in the global financial sector, as evidenced by scholarly articles (Elsaid, 2023; Martinčević et al, 2020; Jalal et al, 2023) that highlight its impacts, opportunities, and challenges. Manyika et al. (2016) assert that the widespread use of digital finance might significantly elevate the GDP of developing countries by approximately 6%, projected to attain $3.7 trillion by 2025. Fintech has transformed financial efficiency, resulting in streamlined processes, cost savings, and improved competitiveness (Harsono & Suprapti, 2024). Mobile banking has enabled convenient financial transactions and optimized financial management for SMEs, while online invoicing and payment systems have enhanced financial management for SMEs.

One of the ways that these services has been enhanced had been through the use of Biometric identification technologies. This has been done via different means such as ocular identification, voice identification, and finger print identification amongst others. Among these, the fingerprints and ocular identification has been the most common in the fintech companies in Nigeria. Biometric technology facilitates precise identity authentication without the necessity of a PIN, password, or card. The creation of a client enrollment template has been facilitated by video-based technologies. These technologies rely on pattern recognition, utilizing a pattern capture mechanism akin to video camera technology and various other mechanisms often seen in consumer gadgets, such as camcorders (Trivedi & Patel, 2012). These technologies capture detailed information that delineates the complex architecture of the different morphological and physiological patterns of users. The information can thereafter be transformed into a mathematical and statistical pattern capable of identifying an individual. Databases house these templates and are queried by matching engines at remarkably high velocities. Biometric

authentication systems are equipped with numerous security measures that render them difficult for hackers to compromise (Syed, et al., 2024). This is accomplished by the utilization of sophisticated sensors capable of detecting frame temperature, motion, or responses. Furthermore, biometric records are encrypted and stored in secure databases, complicating access and manipulation by thieves. A crucial security measure in biometric authentication systems is the use of multi-faceted authentication (Adeyemo & Obafemi, 2024). In addition to the biometric feature, users must provide an additional form of identification verification, such as a password or PIN. This adds an additional degree of security by making it significantly more difficult for an unauthorized user to access an account, even if they possess the biometric data (Sokolov & Mileva, 2024). Biometric authentication is advantageous as it diminishes the likelihood of human error.

In contrast to traditional authentication methods, where users may easily forget passwords or PINs, biometric features are unique to each individual and cannot be forgotten, lost, or shared (Kamuangu, 2024). This mitigates the risk of unauthorized access to an account through stolen or shared credentials. These improvements have markedly improved accessibility and efficiency in financial services; yet, they have also introduced new vulnerabilities to fraud.

Despite the sophistication of these technological innovations, cases of fraud have still been recorded. With the expansion of digital banking, the complexity and prevalence of fraudulent activities increase, presenting significant threats to individuals, enterprises, and financial institutions (Brynjolfsson & McAfee, 2014). Fraud in FinTech encompasses a variety of forms, including identity theft, phishing campaigns, and intricate money laundering operations. Conventional fraud detection systems, dependent on rule-based models, find it challenging to adapt to the evolving nature of these threats (Kokina et al., 2017). Fraudsters consistently adapt their strategies, utilizing sophisticated technology like artificial intelligence [AI] and automated bots to attack weaknesses in digital systems. Cryptocurrency platforms have experienced an increase in fraud incidents, with perpetrators employing tactics such as social engineering and ransomware to appropriate assets (Moon & Khrael, 2020). This mismatch between the improvement between biometric development in fintechs, especially with the commonly used ocular scanning and fingerprints and the corresponding rise in fraudulent activities calls for urgent action and study as there is a dearth of information as far as this is concerned. Hence, this study.

Purpose of the Study

This study is carried out to assess the relationship between biometric technologies in the Fintech sectors and fraudulent activities in Nigeria. Specifically, the study seeks to:

(i) Assess the relationship between Iris/Retina scanning Biometric Identification System and fraud detection in the Fintech company; and

(ii) examine Fingerprint scanning Biometric Identification System and fraud detection in the Fintech company.

Methodology

The study adopts descriptive survey research design. The population comprises of all Fintech companies in Nigeria. From this, two fintech companies will be selected using random sampling technique. Questionnaires will be distributed to both staff and customers of the company to gather information on their perceptions regarding biometric systems and fraud detection in the Fintech companies. Convenience sampling will be used to selected these staff and customers of

the banks in the study area. From this 20 bank officials and 150 customers of banks were purposively selected making a total of 170 respondents. Questionnaire on Biometric Identification and Fraud detection was used to collect data for the study. The questionnaire contained 30 items, with 10 items addressing each of the variables (iris/retina scanning biometric identification, fingerprint scanning biometric identification and fraud detection). Responses was collected on a 4-point Likert Scale which include " Strongly Agree" , " Agree" , " Disagree" and " Strongly Disagree" . Data was analysed using descriptive and inferential statistics.

Results

Demographic information of respondents and Descriptive statistics of the major variables

Table 1: Demographic information of respondents

Variables		Freq.	Percent
Age	18-25	27	15.88
	26-30	50	29.41
	31-35	42	24.71
	36-40	32	18.82
	Above 40	19	11.18
	Total	**170**	**100.00**
Sex	Male	97	57.06
	Female	73	42.94
	Total	**170**	**100.00**
Occupation	Student	47	27.65
	Government Employed	68	40.00
	Self-employed	33	19.41
	Not Employed	22	12.94
	Total	**170**	**100.00**
Education	No Formal Education	17	10.00
	Primary Education	25	14.71
	Secondary Education	47	27.65
	Higher Education	81	47.65
	Total	**170**	**100.00**

Table 1 presents the demographic information of the respondents. On the Table, 15.88% were between age 18-25, 29.41% were between age 26-30, 24.71% were between age 31-35, 18.82% were between age 36-40 and 11.2% were above the age of 40. Thus, respondents from diverse age group were adequately represented. Also, the results show that 57.06% were males, while 42.94% were females. Thus, more males were represented than females. In addition, the results show that 27.65% of the respondents were students, 40.00% were government employed, 19.41% were self-employed, while 12.94% were not employed. Thus, people from different work group and profession were represented in the data. In addition, 10.00% of the respondents had no formal education, 14.71% had primary education, 27.65% had secondary education, while 47.65% had higher education. Thus, most of the respondents were educated.

Table 2: Descriptive statistics of the major variables

Statistics	Observation	ir_biometric	fp_biometric	fraud_detection
Mean	170	8.710	6.901	12.332
Standard Deviation	170			
Minimum	170	9	10	10
Maximum	170	38	40	40

Hypothesis 1

There is no significant relationship between Iris/Retina scanning Biometric Identification System and fraud detection in the Fintech company

To test this hypothesis, responses of the respondents to the items on iris/retina scanning biometric identification system were summed together to represent the independent variable. This was also done for responses to items on fraud detection which then represented the dependent variable. The scores were then subjected to Pearson Correlation and the result is presented in Table 3.

Table 3: Relationship between Iris/Retina scanning Biometric Identification System and fraud detection in the Fintech company

	r	Sig. (2-tailed)	N
Ir_biometric	0.262	.002	170

Table 3 presents the results of the relationship between Iris/Retina scanning Biometric Identification System and fraud detection among the selected banks. On the Table, the r value showed 0.262, while the relationship is significant as the p-value is less than 0.05 threshold. From this, it can be concluded that there is a significant and positive relationship between iris/retina scanning biometric and fraud detection. Also from the r value (0.262), it can be concluded that the relationship is positive. This implies that the more the use of iris/retina scanning biometric, the higher the propensity for fraud detection.

Hypothesis 2

There is no significant relationship between fingerprint scanning biometric identification system and fraud detection in the Fintech company.

Table 4: Relationship between fingerprint scanning biometric identification system and fraud detection in the Fintech company

	r	Sig. (2-tailed)	N
fp_biometric	0.141	.004	170

Table 4 presents the results of the relationship between fingerprint scanning biometric identification system and fraud detection among the selected banks. On the Table, the r value showed 0.141, while the relationship is significant as the p-value is less than 0.05 threshold. From this, it can be concluded that there is a significant and positive relationship between fingerprint scanning biometric identification and fraud detection. Also from the r value (0.141), it can be concluded that the relationship is positive. This implies that the more the use of fingerprint scanning biometric, the higher the propensity for fraud detection.

Discussion of Findings

Results from this study showed that both iris/retina scanning biometric identification system and fingerprint scanning biometric identification system had positive and significant relationship with fraud detection. Thus, the use of both of the biometric identification systems lead to high chances of fraud detection among the banks and their customers in Nigeria. These findings are in line with the research of Singh, et al. (2019), Banga and Pillai (2021), Morake et al. (2021) among others found fingerprint biometric and iris/retina scanning biometric identification to be effective in detecting fraud and avoiding the same in the banking industry. Reason for this result may be due to the fact that some of these features are highly unique to individual customer, thus, forging or replicating the same is largely difficult, if not impossible. This is consistent with the ideas of Liébana-Cabanillas et al. (2024) Also, unlike passwords and PINs, iris/retina scanning and fingerprint provides one-to-one match, which aids banks and other financial institutions to reduce fraudulent activities and access to the barest minimum, thus, leading to decreased fraud in the Banking industry.

Conclusion and Recommendations

The study concluded that both iris/retina scanning biometric identification system and fingerprint scanning biometric identification system help in significantly identifying fraud detection among the respondents. Thus, both systems are effective in detecting cases and incidences of fraud in the banking sector. Thus, it is recommended that Nigeria' s banking and financial technology introduce these features into their system as part of criteria for logging into the online banking system and in making transactions.

References

Adeyemo, K. and Obafemi, F. J. (2024). A Survey on the role of technological innovation in Nigerian deposit money bank fraud prevention. *South Asian Journal of Social Studies and Economics,* 21(3), pp.133-150.

Banga, L. and Pillai, S. (2021). Impact of behavioural biometrics on mobile banking system. *Journal of physics: Conference series* (Vol. 1964, No. 6, p. 062109). IOP Publishing.

Brynjolfsson, E. and McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies.* New York: Norton & Company.

Kamuangu, P. (2024). A review on cybersecurity in Fintech: Threats, solutions, and future trends. *Journal of Economics, Finance and Accounting Studies,* 6(1), pp.47-53.

Kokina, J., Pachamanova, D. and Corbett, A. (2017). The role of data visualization and analytics in performance management: The case of higher education. *Journal of Accounting Education,* 38, pp.50– 62. doi:10.1016/j.jaccedu.2017.03.002

Liébana-Cabanillas, F., Kalinic, Z., Muñoz-Leiva, F. and Higueras-Castillo, E. (2024). Biometric m-payment systems: A multi-analytical approach to determining use intention. *Information & Management,* 61(2), p.103907.

Moon, D. and Krahel, J. P. (2020). Continuous risk monitoring and assessment: New component of continuous assurance. *Journal of Emerging Technologies in Accounting,* 1(17), pp.173-200.

Morake, A., Khoza, L.T. and Bokaba, T. (2021). Biometric technology in banking institutions: The customers' perspectives. *South African Journal of Information Management,* 23(1), pp.1-12.

Singh, A., Srivastava, R. and Singh, Y.N. (2019). Prevention of payment card frauds using biometrics. *International Journal of Recent Technology and Engineering (IJRTE),* 8, pp.516-525.

Sokolov, S. and Mileva, L. (2024). Technique for enhancing fraud detection in banking with facial biometric feature storage. In *AIP Conference Proceedings* (Vol. 3063, No. 1). AIP Publishing.