Relationship Between Biometric Technology and Customer Satisfaction in the Fintech Sector

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

Agboola, Olatoye Kabiru
Department of Business Analytics & Data Science
School of Business, New Jersey City University, Jersey City, New Jersey, USA
Email: agboolaolatoye@gmail.com
ORCID iD: 0009-0004-0905-0175

Adamaagashi, Izuchukwu Prince
Department of Sociology and Anthropology
Enugu State University of Science and Technology, Enugu State, Nigeria
Corresponding Author: adamaizuchukwu@gmail.com
DOI 10.56201/ijebm.vol.11.no4.2025.pg190.204

Abstract
This study explores the relationship between the adoption of biometric technology and customer satisfaction in the fintech sector. As financial institutions increasingly integrate biometric systems—such as fingerprint, facial recognition, and iris scanning—into their service offerings, understanding the impact on customer experiences has become crucial. Through a mixed-method approach, combining both qualitative and quantitative data, the research examines how biometric authentication influences customer perceptions of security, convenience, and trust, key components of overall satisfaction. The findings indicate a positive correlation between the use of biometric technologies and improved customer satisfaction, particularly in terms of enhanced security, reduced fraud risks, and streamlined service delivery. However, the study also highlights challenges, such as privacy concerns and the need for robust data protection measures, which can affect customer trust and satisfaction. Additionally, the research identifies demographic factors, such as age and technological literacy, that influence the acceptance and effectiveness of biometric systems. This paper contributes to the growing body of knowledge in fintech by providing actionable insights for industry stakeholders seeking to optimize customer experiences through innovative technological solutions. The study concludes with recommendations for fintech firms to address potential barriers, ensuring that biometric technology is leveraged effectively to enhance customer satisfaction while safeguarding privacy.

Introduction

Biometric technologies utilise individuals' distinct physiological and behavioural traits that can be quantified for automatic identifying purposes (Piotrowski, 2024). These technologies exhibit different diversities owing to the various properties that require measurement. This has led to the development market solutions which exist in ways that they utilise fingerprint, vein pattern, facial structure, iris, retina, hand geometry, voice, gait, or signature (handwriting) recognition (Tassabehji & Kamala, 2012), among other modalities. Biometric authentication systems offer significant ease and security, leading to its growing use across various applications. The inception of biometrics dates to the 19th century, primarily concentrating on the acquisition of individuals' physical characteristics to authenticate their identification (Morake et al., 2021). Previously, biometrics was mostly utilised in high-security applications as it was originally employed to assess an individual's physical and behavioural characteristics (Morake et al., 2021). In recent times, biometric verification applications include ATM usage, workplace authentication, network access, travel and tourism, internet connections, and mobile connectivity. In recent years, there has been a greater focus on digital banking, financial technology, and other domains, rather than on the use of biometrics in banking and retail.

Broadly divided into physiological and behavioural biometrics as explained by Misini et al. (2022), biometric technology provides authentication and identifying mechanism. Unique bodily traits that stay rather constant across time define physiological biometrics. Typical instances are hand geometry, which studies a person's hand shape and measurements, and fingerprint recognition, which analyses the unique ridges and patterns of an individual's fingerprint. Other often used physiological biometrics are facial recognition, which maps facial traits to Authenticate users, and iris recognition, which distinguishes people according on the distinct patterns in their irises. While vein recognition and retina identification employ vascular patterns in the hand or eye for authentication, signature recognition checks a person's identity by examining their handwriting style. By matching people based on their genetic information, advanced techniques including DNA recognition offer even more security. Conversely, behavioural biometrics centre on trends in human relationships and behaviour. These include gait analysis—which looks at a person's particular walk—and typing rhythm, which studies keystroke speed and pattern. Other behavioural biometrics examine individual typing behaviours using keyboard dynamics and mouse dynamics—that is, how a person operates a computer mouse. Analysing vocal traits including pitch, tone, and speech patterns to validate identity, voice recognition is another often used behavioural biometric technique. Particularly in the financial and technology industries, both physiological and behavioural biometric systems are progressively being included into digital security architectures in order to improve authentication accuracy and stop identity fraud.

For this study, the researcher seek to utilize fingerprint, voice recognition, facial recognition, signature recognition, multi modal biometric authentication. This sub variables are selected they are the most commonly used sub-variables used in the Nigerian fintech space. Studies shows that the use of biometric technology may begin to influence both individuals and enterprises or clients and organisations. Furthermore, biometrics can be regarded as a more expedient way for information tracing and recovery compared to manual or conventional verification techniques performed at the counter (Ahmad et al. 2012; Jain & Kumar 2010; Jain, Ross & Pankanti 2006). However, biometric security is a mechanism that dramatically enhances the integrity, confidentiality, and availability of information (Ahmad et al. 2012). The use of biometric may help to protect both logical and physical access constraints. Logical access controls safeguard network facilities, computers, and information systems from unauthorised access (Jain et al. 2006), whereas physical access controls guarantee that only approved individuals can access IT infrastructures and document storage (Jain et al. 2006). This emphasises the importance of biometric and its usefulness for ensuring efficient running of systems and operations.

Faster development of financial technology (FinTech) has transformed client interaction with financial services. Widely accepted by financial organisations to improve security, increase service efficiency, and optimise identification processes, biometric technology marks a major breakthrough in this field. More securely and conveniently than traditional authentication systems like passwords and PINs, biometric authentication methods—which include fingerprint recognition, facial recognition, voice recognition, and iris scanning—offer. The success of FinTech products depends critically on client pleasure since it influences client loyalty, confidence, and continuous interaction with digital financial platforms (Rane, Achari &Chowdhury, 2023). Consumer experience is shaped in great part by security and accessibility; biometric authentication provides seamless, fraud-resistant identity verification, therefore addressing both problems. Financial service companies under pressure to embrace increasingly strict security measures while preserving client convenience as cyber risks and digital fraud grow. As a way to balance security with user-friendly access, biometric technology has developed and could help to increase customer confidence and happiness.

Still, even although biometric authentication offers some advantages, problems related to data privacy, system dependability, and the possibility of biometric data leaks remain rather significant (Balamurugan, 2024). Some customers could find it difficult to adjust to biometric systems because of technological limitations or lack of experience. Financial institutions need to understand how biometric technologies affect consumer happiness in the FinTech section. The fast development of financial technology (FinTech) has transformed banking and financial services, so enabling the general acceptance of digital solutions for transactions, identity verification, and client contacts (Feyen, et. al.,2021). Security issues have become a key difficulty as financial institutions keep moving towards digital platforms since conventional authentication techniques like passwords and PINs are more prone to fraud and cyber threats (Cele & Kwenda, 2025). Biometric technology has become a potential answer to these difficulties since it provides safe and easy-to-use identification systems including voice recognition, iris scanning, fingerprint recognition, and facial recognition.

By means of a flawless and dependable substitute for traditional security mechanisms, biometric authentication improves security and convenience for consumers. Biometric technologies lower the danger of identity theft, illegal access, and fraudulent transactions by doing away with the necessity for memorised passwords and physical identification cards. This technical development has fundamentally changed the FinTech industry since financial institutions look for creative solutions to safeguard client information while guaranteeing seamless and quick banking FinTech experiences. The success of digital financial services depends mostly on consumer pleasure, which shapes customer retention, confidence, and involvement. Although biometric technology improves security, its effects on user satisfaction rely on several elements including ease of use, system dependability, privacy issues, and technological confidence. While some consumers would struggle with technological issues or system failures, others would view biometric authentication as an invasion of privacy. Therefore, financial organisations trying to maximise user experiences and create customer confidence in digital banking services must first grasp the link between biometric technology and customer experiences such as satisfaction, perception and confidence.

A customer is a principal stakeholder in an organisation who renders payment in return for products or services (Ateba et al., 2013). Customers encompass not only individuals but also entities such as universities, banks, construction enterprises, schools, legal practices, and hospitals that acquire goods and services from various retailers (Rahman & Safeena, 2016). It is important that FinTech acknowledge that their consumers originate from various occupational backgrounds and this may impact of various forms of satisfaction they get from the use of different services (Rahman & Safeena,2016). As online banking and financial transactions has increased, fraudsters have evolved by creating more advanced attack techniques. With the increase in digital crime and financial theft, organisations are proactively pursuing effective solutions to address these dangers. Conventional security protocols, including passwords, PINs, and identification cards, are inadequate to mitigate the escalating incidence of transaction fraud and security violations. As a result, digital banking solutions have arisen as a formidable means to improve security (Hosseini & Mohammadi, 2012). Given that PIN verification alone fails to give robust security against cyber risks, digital banking systems through FinTech guarantee that critical user data is safely housed within encrypted containers or sandboxes, thereby providing augmented safeguards against unauthorised access (Johnson,2019).

To maximise investments and ensure value delivery to customers from different stakeholders, it is imperative to have an awareness of the factors that influence the desire to use biometric technology. (Irimia-Diéguez et al., 2023). This then explains why this study seeks to assess the extent to which biometric authentication influences consumer confidence, security perceptions, and overall service experience. The study seeks to provide understanding on the relationship between biometric technology and customer-related factors in the FinTech sector. Although studies have shown that there are concerns and challenges as regards the adoption of FinTech and Ai biometrics, it is important that the study will provide comprehensive insight as to how FinTech may use biometric technology to increase consumer satisfaction, influence security and privacy issues while enhancing the customer experience

LITERATURE REVIEW

Heracleous and Writz (2006) explained that the capacity of innovative technologies may be influential in cultivating sustainable competitive advantage as well as how these can be evaluated based on their prospective influence on customer experience. It was also explained that the degree to which their implementation influences the reconfiguration of business processes that are challenging for competitors stands as a strong advantage for the use of Biometric technology in different organisations.

By improving safety procedures and boosting user confidence, AI-driven biometric technology is transforming security in the financial technology (FinTech) industry, assert Ozigagun et al. (2024). This analysis examines how AI-powered biometrics protect FinTech operations, emphasising both its advantages and broader implications. The use of artificial intelligence (AI) algorithms to assess biological data for authentication purposes is known as AI-driven biometrics. Because it is more secure than conventional authentication techniques, this technology has found widespread application in the FinTech industry. AI-driven biometrics ensure precise identity verification by analysing unique biological traits like fingerprints, face features, and speech patterns, making unlawful access to private financial data much more challenging. The ability of AI-driven biometrics in FinTech to enhance security is one of its main benefits. Traditional authentication methods, such as PINs and passwords, are more susceptible to fraud and hackers. On the other hand, biometric authentication makes use of unique biological traits, which makes unauthorised access much more difficult. AI-driven biometrics not only improve security but also optimise user experience by replacing laborious authentication methods with simple biometric verification. Without having to remember complex passwords or PINs, users may quickly and easily access their accounts, reducing the possibility of user error and account lockouts. By offering sophisticated authentication solutions and enhancing client convenience, AI-driven biometrics is revolutionising security and trust in the FinTech industry. It is projected that this developing technology would strengthen consumer trust in digital financial services and improve the security of financial transactions.

The goal of another study, according to Piotrowska (2024), is to investigate the variables that affect the use of biometric technology in bank and FinTech financial applications. The research is based on data from a survey of 1,000 Polish individuals. The estimated logit model indicates that the probability of using biometric solutions decreases with age and increases with educational attainment and technological sophistication in relation to individual inventiveness, biometric technology experience, and digital technology use in both financial and non-financial domains. According to the study, the COVID-19 pandemic has accelerated the use of biometric solutions and increased awareness of the potential for digital technology to infringe on respondents' privacy. The study demonstrates how the confidence that phone manufacturers use to ensure the security of stored cash and data processing has a favourable impact on the adoption of biometric solutions in financial services. This relationship supports the idea that financial institutions should encourage biometric technologies.

According to Oto (2024), their study was to investigate the variables that affect the use of biometric technologies in bank and FinTech financial applications. The analysis used data from a survey of 1,000 adults in Poland. The estimated logit model indicates that technological sophistication and educational attainment increase the likelihood of using biometric solutions in relation to individual inventiveness, biometric technology experience, and digital technology use in both financial and non-financial domains, while age decreases this likelihood. The COVID-19 epidemic is cited in the study as a factor hastening the adoption of biometric solutions and raising awareness of the risk of respondents' privacy being invaded by digital technologies. The study shows how the adoption of biometric solutions in financial services is positively impacted by the trust that phone manufacturers utilise to guarantee the security of stored funds and data processing. The suggestion that financial organisations promote biometric technologies is supported by this relationship.

OBJECTIVES

The objectives of this research are to:

i. to evaluate the level of customer perception about biometric technologies in FinTech companies.
ii. to assess how biometric authentication affects financial service security, customer satisfaction, and confidence

RESEARCH QUESTIONS

i. What is the level of Customer perception about biometric technologies in FinTech companies in the study area
ii. What is the relationship between biometric authentication, financial service security, customer satisfaction, and confidence

THEORETICAL FRAMEWORK

The intricacies of human behaviour with regard to the acceptance of technology breakthroughs are addressed by the Technology Acceptance Model (TAM) (Bagozzi, 2007; Eshiett & Eshiett, 2024). This model provides comprehensive insight for assessing technology acceptance processes (Davis et al., 1989). It is based on the concepts of technological development, adoption, and user engagement (Bagozzi et al., 1992). The Diffusion of Innovation Theory (DIT) (Rogers, 2010) and frameworks examining human behavioural tendencies in product adoption (Legris et al., 2003). All these represents further theoretical models pertinent to technology adoption.

The Technology Acceptance Model has faced criticism from scholars despite its widespread application. Some argue that it lacks a definitive basis for evaluation (Chuttur, 2009), while others highlight the absence of measurable criteria for assessing technology adoption (Moore & Reid, 2008). Conversely, proponents argue that the model's emphasis on perceived benefits and usability positively influences user adoption (Lunceford, 2009). Furthermore, by taking into account employees' concerns during the implementation of technical change, TAM's inclusion of human behavioural inclinations makes it an effective instrument for promoting organisational adoption of new technology. This study finds this model applicable in that it seeks to explain how the adoption of biometric technology impacts on customer related factors as well as financial security of end users to the end that it improves the quality of services as well as the adoption of this technology by end users. This study aims to close the gap in the literature by investigating the applicability of TAM in addressing customer related and security issues in FinTech vis-à-vis the impact of biometric authentication, as it has not been examined in prior research.

METHODOLOGY

The study adopted descriptive survey research design by collating data from different fintech companies in Nigeria. The population comprised of all FinTech companies in Nigeria as the study adopted random sampling technique to select the samples that will be involved in the sample based on the objectives of the study (Saunders, et. al, 2019). A total of 329 respondents were randomly selected from the study using customers that used the FinTech companies with the highest revenue or customer base as at 2024.

In addition, closed-ended surveys were selected (Saunders et al., 2019) since they were simpler to gather, compile, and evaluate data on. A self-constructed instrument was used in gathering data for this study. The questionnaire consist of 6 Sections which comprise of Section A, comprising information on demography of the respondents, the Section B which contained items on customer perception to biometric authentication, then Section C which contained items on Biometric authentication, Section D which contained items on financial service security, then Section E with items on Customer satisfaction and Section F with items on Customer confidence. Items on these scales were developed from past research. Responses to Section B to F were on a four-point Likert scale, which include Strongly Agree = SA; Agree = A; Disagree = D; Strongly Disagree = SD.

Copies of the questionnaire were administered to customers of Fintech both online and offline. A total of 500 hard copies of the questionnaire were distributed, while only 218 copies were retrieved and properly filled, from the online responses, a total of 111 copies that were completely filled were found useful. Thus, a total of 329 responses were used for the data analysis.

The reliability of the instrument was assessed using the Cronbach's Alpha coefficient. The basis for this assessment was Field's (2009) dependability criterion, which holds that a measurement tool is judged dependable if its Cronbach's alpha surpasses 0.7. Reducing researcher bias and improving the acceptability and openness of the research process define validity and reliability's main goals (Singh, 2014). Because of their simplicity of data collecting, compiling, and analysis, closed-ended questionnaires were used (Saunders et al., 2019). Using a four-point Likert scale, the designations Strongly Agree = SA; Agree = A; Disagree = D; Strongly Disagree = SD. Reliability of the instrument was assessed using the Cronbach's Alpha coefficient. Field's (2009) reliability argument formed the basis of the assessment since it holds that a measurement tool is judged reliable if its Cronbach's alpha surpasses 0.7. Validity and dependability mostly aim to reduce researcher bias and improve the acceptability and openness of the research process (Singh, 2014).

Results

Reliability of the Instrument

Table 1: Cronbach's Alpha Values for Research Instrument

Variables	Cronbach's Alpha
Customer perception	0.871
Biometric authentication	0.759
Financial service security	0.812
Customer satisfaction	0.940
Customer confidence	0.655

Table 1 presents the reliability information of the scales used in collecting data for this study. On the Table, the Cronbach's Alpha values include 0.871 for customer perception scale, 0.759 for biometric authentication scale, 0.812 for financial service security scale, 0.940 for customer satisfaction scale and 0.655 for customer confidence scale. From these, it can be concluded that these scales are adequate for the data collection.

Demographic Information

Table 2: Respondents' Demographic Information

Demographic		Freq.	Percent
Age	18 – 30 Years	157	47.72
	31 – 40 Years	98	29.79
	41 Years and Above	74	22.49
	Total	329	100.0
Sex	Male	172	52.28
	Female	157	47.72
	Total	329	100.0
Occupation	Students	69	20.97
	White Collar Jobs	144	43.77
	Blue Collar Jobs	100	30.40
	Unemployed	16	4.86
	Total	329	100.0
Highest Educational Qualification	No Formal Education	08	2.43
	Secondary Schools and Less	82	24.92
	First Degree	190	57.75
	Second and Other Degree	49	14.89
	Total	329	100.0

Table 2 presents the demographic information of the respondents. On the Table, results show that 47.7% of the respondents were between the ages of 18 and 30, 29.8% of the respondents were between the ages of 31 and 40, while 22.5% were above the age of 40. Thus, every age group was adequately represented. Also, the Table show that 52.3% of the respondents were males, while 47.7% were females. Thus, the two genders were evenly represented in the study. Also, the Table shows the distribution of the respondents' occupation. On the Table, 21% of the respondents were students, 43.8% held white collar jobs, 30.4% held blue collar jobs, while 4.9% were not employed as at the time of the study. Thus, respondents were represented across different occupational groups. Also, the Table show that 2.4% of the respondents had no formal education, 24.9% had secondary education and less, 57.8% had first degree, while 14.9% had second and other degrees. This implies that most of the respondents were formally educated.

Research Question 1

What is the perception of customers about biometric technologies in financial establishments?

To answer this question, responses to Section B of the questionnaire were scored in a way that a score of 4 was allotted to "Strongly Agree", a score of 3 was allotted to "Agree", a score of 2 was allotted to "Disagree" and a score of 1 was allotted to "Strongly Agree". These were summed together to represent respondents' measure on perception about biometric technology. On the measure, the minimum and maximum scores were 10 and 40 respectively, while the mean and standard deviation scores were 25.41 and 8.86 respectively. In order to divide into categories of perception, respondents whose scores ranged from 1 standard deviation below the mean was regarded as possessing negative perception, those who scored within 1 standard deviation of the mean were regarded as neutral and those whose score were within 1 standard deviation above the mean were considered as possessing positive perception. These were subjected to descriptive statistics and the results are presented in Table 3.

Table 3: Categories of customer perception about biometric technologies in financial establishments

Perception	Freq.	Percent
Positive	131	39.82
Neutral	174	52.89
Negative	24	7.29
Total	329	100.0

Table shows the results of the perception of customers on biometric technologies in financial institution. On the Table, results show that 39.8% had positive perception, 52.9% had neutral perception and 7.3% had negative perception of biometric technologies in financial institution. From this, it can be concluded that respondents' perception of biometric technologies in financial institution tilt between neutral and positive perception.

Research Question 2

What is the relationship between biometric authentication and financial service security, customer satisfaction, and customer confidence?

To answer this question, responses of the respondents to the sections of the questionnaire on biometric authentication, financial service security, customer satisfaction and customer confidence were summed together. The dimensions of biometric authentication were considered as the independent variables, while financial service security, customers' satisfaction and customers' confidence were regarded as the dependent variables. These were subjected to Pearson Correlation and the results are presented below:

Table 3: Relationship between biometric authentication and financial service security, customer satisfaction, and customer confidence

Biometric Authentication	Financial service security	Customers' satisfaction	Customers' confidence
Fingerprint recognition			
Person's Correlation	0.129	0.248	0.162
Sig. (2-tailed)	0.045	0.001	0.005
N	329	329	329
Facial Recognition			
Person's Correlation	0.234	-0.006	0.014
Sig. (2-tailed)	0.001	0.917	0.875
N	329	329	329
Voice Recognition			
Person's Correlation	0.217	0.221	0.011
Sig. (2-tailed)	0.007	0.004	0.162
N	329	329	329

Signature Recognition			
Person's Correlation	0.234	0.181	0.310
Sig. (2-tailed)	0.001	0.017	0.002
N	329	329	329
Multi-Modal Biometric Authentication			
Person's Correlation	0.287	0.164	0.217
Sig. (2-tailed)	0.000	0.045	0.005
N	329	329	329

Table 3 presents the results of the relationship between biometric authentication and other variables such as financial service security, customer satisfaction, and customer confidence. On the Table, the fingerprint recognition has a significant and positive relationship with financial security ($r = 0.129$, $p < 0.05$), customer satisfaction ($r = 0.248$, $p < 0.05$) and customers' confidence ($r = 0.162$, $p < 0.05$). This implies that fingerprint recognition improved financial service security, the satisfaction of the customers and their confidence in using the financial services of the organization. In addition, facial recognition was found to significantly and positively influence financial service security ($r = 0.234$, $p < 0.05$), however, facial recognition has no significant relationship with customers' satisfaction ($r = -0.006$, $p > 0.05$) and confidence ($r = 0.014$, $p > 0.05$). This implies that face recognition only influences financial service security and not customers' satisfaction and confidence in the financial institutions' services. Moreover, the results showed that voice recognition significantly and positively relate with financial service security ($r = 0.217$, $p < 0.05$) and customer satisfaction ($r = 0.221$, $p < 0.05$), however, there is no significant relationship between voice recognition and customer confidence ($r = 0.011$, $p > 0.05$). Also on Table 3, results showed that signature recognition significantly and positively influences financial service security ($r = 0.234$, $p < 0.05$), customer satisfaction ($r = 0.181$, $p < 0.05$) and customer confidence ($r = 0.310$, $p < 0.05$). This implies that the use of significant recognition biometric authentication improves financial service security, the satisfaction and confidence of customers in the services of the financial institutions. Results on the Table finally show that the use of multi-modal biometric authentication significantly influence financial service security ($r = 0.287$, $p < 0.05$), customers' satisfaction ($r = 0.164$, $p < 0.05$) and customers' confidence ($r = 0.217$, $p < 0.05$), implying that multi-modal biometric authentication significantly contributes to financial service security, the satisfaction and confidence of customers in the services of the financial organizations sampled.

Discussion of Findings

Results of this study found that respondents' perception of biometric technologies in financial institution tilt between neutral and positive. This implies that respondents perceived some advantages of the use of biometric technologies by financial institutions, while some are uncertain on the usefulness and advantages. This result is consistent with prior research such as that of Hong et al. (2017), Patil et al. (2020) and Lee and Pan (2022) where respondents demonstrated positive perception to the introduction of biometric feature to the use of ATM and other aspects of banking system. Reason for the findings of this research maybe due to the fact that customers now prefer to carry out financial transactions without having to physically visit banking physical locations, thus, the introduction of biometric technologies may be perceived as part of organizational efforts to achieving those dreams. Also, most respondents now use phones and personal computers which require biometric authentication, especially fingerprint identification as means of passwords. This understanding might have impacted on customers on the advantages of introducing biometric authentication to financial services.

Results also showed the relationship between different aspects of biometric authentication/technologies and customers' perception of financial service security, satisfaction and confidence in the services of the financial institutions. Results from this showed that fingerprint biometric authentication had significant and positively relationship with customers' perceptions of financial service security, their satisfaction and confidence in the financial institutions. The use of fingerprint biometric authentication has been found to improve all aspects of financial services, most especially from customers' ends. For instance, the study of Al-Jundi et al. (2019) and Liébana-Cabanillas et al. (2020 a and b) found the introduction of fingerprint biometric authentication to the use of ATMs to be safer than the use of ordinary pin. This may suggest reduction of theft by close relative of customers who may be privy to secret information on customers' ATM and other bank applications. Moreover, the introduction of fingerprint may be considered to make access to banking services easy as customers do not need to memorize and remember their pins or codes wherever they want to access financial services. This may contribute to the reasons why the use of fingerprints authentication significantly contributes to financial services security, customers' satisfaction and confidence in financial services.

Also, the results showed that facial recognition biometric authentication significantly and positively relate with financial service security only, while there is no significant relationship between facial recognition and customers' satisfaction and confidence. Thus, customers believe that face recognition only influence the security of financial services, without additional advantages to customers' satisfaction and confidence in the services of the financial institutions. Wang (2021) and Zhang et al. (2021) discovered the use of facial biometric authentication as one of the new security measures in fintech and other areas of technology. This has been discovered to provide another layer of security for consumers of technological products. Even though, the introduction of facial recognition biometric is relatively new in fintech, with limited research, reason for this result may be tied to the fact that customers may sometimes encounter challenges in utilizing the technological features wherever they wish to access financial and other services. Unlike fingerprint, facial recognition biometric technology may be limited in use to specific hours and features available on customers' gadgets. Unlike fingerprint, which is more widely available on diverse gadgets, facial recognition cannot be said to be widely available most especially in many developing countries.

In addition, results show that voice recognition biometric had significant relationships with financial security services and customer satisfaction. However, this did not significantly relate to the confidence of customers. This suggests that the use of voice recognition added significantly to service security and customers' satisfaction, but not to the confidence of customers in financial services. This research is in line with that of Onesi-Ozigagun et al. (2024) found the introduction of voice recognition biometric as one of the novel ideas to ensuring security as they add as additional layers of security which could hardly be compromised by unauthorized individuals. In the same vein, Amjad Hassan Khan and Aithal (2024) opined that the use of voice recognition biometric to ensures the safety of vital information of consumers which cannot be leaked, hence, increasing customers' satisfaction and confidence in the services of fintech companies. This opinion was also supported by Wang (2021). Even though voice recognition was found to improve service security and customers' satisfaction in this study, this was not the same for customers' confidence in financial services. Reason for this may be due to personal experiences of recent bank thefts by unauthorized individuals in some of the Nigerian traditional banks and even among fintech companies. This may lead to customers believing that these measures are only to prevent unauthorized access from their personal devices, and not from the end of the service providers. This and many other experiences of breaches in the information of customers may affect their confidence in the services of some of the fintech companies.

Results also showed that signature recognition biometric relate significantly to financial service security, customers' satisfaction and confidence. This suggests that signature recognition biometric significantly improve service security, customers' satisfaction and confidence in financial institutions' services. Research on signature recognition biometric in the fintech and other tech areas could be said to be few as at when this study was being conducted. However, few available ones discovered signature recognition biometric as one of the most secured forms of biometric identification in tech. However, this was largely said to still be impossible for many institutions to implement due to the intricacies required in developing them (Kuraku et al., 2020). The maximum security features of this biometric system may be said to be responsible for improved service security, customers' satisfaction and confidence of customers in fintech services. Also, considering that signature is one of the means through which transactions are done in traditional banking systems, introducing this and enhancing it with the application of security measures may be considered as effective means of wining the interests and attention of service users most especially in developing countries like Nigeria.

Results finally show the use of multiple biometric authentications, that is, multi-modal biometric authentication, significantly relate to service security, customers' satisfaction and confidence. Implying that the combination of more than one biometric authentication significantly improve the security of services, the satisfaction and confidence of customers in the services of financial institutions. Most fintech companies in Nigeria often require multi-modal biometric authentication, especially in carrying out transactions which are beyond the usual, daily and often transactions of the customer. This many include the use of fingerprint, facial recognition, voice recognition among others. This has been popularly known to be the case in transferring huge amounts from one financial technology company to another or even to traditional banks. This idea has been supported by the research of Monisha et al. (2024). In addition, customers may have the perception that the more layer the security measures before accessing the services of the financial technology companies, the more secure their services, most especially from unauthorized individuals. Thus, the combination of two or more biometric authentications may translate to more security, customers' satisfaction and confidence in the services of the fintech companies.

Conclusion and Recommendations

The study concluded that even though biometric authentication is becoming increasingly popular among fintech companies in Nigeria, customers' perception to biometric authentication is neutrally positive. This posits that customers of fintech companies are adopting diverse biometric authentication methods and are willing to do more in the future. Also, diverse biometric authentication methods were found to improve financial security service, customers' satisfaction and customers' confidence in the services of fintech companies. Hence, it is recommended that fintech companies embark on more awareness on the importance of biometric authentication for customers and also work with other technological companies in Nigeria in providing seamless biometric authentication services for customers and end-users.

References

Ahmad, S.M.S., Ali, B.M. & Adnan, W.A.W. (2012). Technical issues and challenges of biometric applications as access control tools of information security. *International Journal of Innovative Computing, Information and Control*, 8(11), 7983–7999.

Al-Jundi, S.A., Shuhaiber, A. & Augustine, R. (2019). Effect of consumer innovativeness on new product purchase intentions through learning process and perceived value. Cogent Business & Management 6(1), 1698849.

Amjad Hassan Khan M. K, & Aithal, P. S. (2024). Identification of Customer Through Voice Biometric System in Call Centres. *International Journal of Applied Engineering and Management Letters (IJAEML), 8(1), 120-127. DOI:https://doi.org/10.5281/zenodo.1081018*

Ateba, B. B., Maredza, A., Ohei, K., Deka, P., & Schutte, D. (2015). Marketing mix: it's role in customer satisfaction in the South African banking retailing. Banks & bank systems, 10(1), 83-91.

Bagozzi, R.P. (2007). The legacy of the technology acceptance model and a proposal for a paradigm shift. *Journal of the Association for Information Systems, 8*(4), 244–254, https://doi.org 10.17705/1jais.00122

Bagozzi, R. P., Davis, F. D., & Warshaw, P. R. (1992). Development and test of a theory of technological learning and usage. *Human Relations, 45* (7), 660–686, https://doi.org 10.1177/001872679204500702, hdl:2027.42/67175

Balamurugan, M. (2024). Biometric Authentication: A Double-Edged Sword for Security? *International Journal of Science and Research (IJSR), 13*(9), 170–173. https://doi.org/10.21275/sr24901230354

Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime, 32*(1), 31-48.

Chuttur, M.Y. (2009). Overview of the Technology Acceptance Model: Origins, Developments and Future Directions, Indiana University, USA, Sprouts: Working Papers on Information Systems, archived from the original on 2013-01-12

Davis, F. D., Bagozzi, R. P., Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982–1003, https://doi.org 10.1287/mnsc.35.8.982.

Eshiett, I. O., & Eshiett, O. E (2024). Artificial intelligence marketing and customer satisfaction: An employee job security threat review. *World Journal of Advanced Research and Reviews, (WJARR), 21*(01), 446–456, https://doi.org/10.30574/wjarr.2024.21.1.2655

Feyen, E., Frost, J., Gambacorta, L., Natarajan, H., & Saal, M. (2021). Fintech and the digital transformation of financial services: implications for market structure and public policy. BIS papers.

Field, A. P. (2009), Discovering Statistics using SPSS, SAGE Publications; London

Heracleous, L., & Wirtz, J. (2006). Biometrics: the next frontier in service excellence, productivity and security in the service sector. *Managing Service Quality: An International Journal, 16*(1), 12-22.

Hong, J. C., Lin, P. H., & Hsieh, P. C. (2017). The effect of consumer innovativeness on perceived value and continuance intention to use smartwatch. *Computers in Human Behavior, 67*, 264–272.

Hosseini, S. S., & Mohammadi, S. (2012). Review banking on biometric in the world's banks and introducing a biometric model for Iran's banking system. Journal of Basic and Applied Scientific Research, 2(9), 9152-9160.

Irimia-Diéguez, A., Velicia-Martín, F., & Aguayo-Camacho, M. (2023). Predicting FinTech innovation adoption: the mediator role of social norms and attitudes. *Financial Innovation, 9*(1), 36.

Jain, A. K., & Kumar, A., (2010). Biometrics of next generation: An overview. *Second Generation Biometrics, 12*(1), 2–3.

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. *IEEE Transactions on Information Forensics and Security 1*(2), 125–143.

Johnson, A. A. (2019). Strategic alignment and information technology projects in the banking industry (Doctoral dissertation, Capella University).

Kothari, C. R. (2015). Research Methodology –Methods and Techniques, 2nd ed., New Age International (P) Ltd., New Delhi.

Kuraku, C., Gollangi, H. K., & Sunkara, J. R. (2020). Biometric Authentication In Digital Payments: Utilizing AI And Big Data For Real-TimeSecurity And Efficiency Educational Administration: Theory and Practice, 26(4), 954 - 964Doi: 10.53555/kuey.v26i4.7590

Lee, C. T. & Pan, L. Y. (2022). Resistance of facial recognition payment service: A mixed method approach. *Journal of Services Marketing, 37*(3), 392–407.

Legris, P., Ingham, J., Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management, 40*(3), 191– 204, https://doi.org 10.1016/s0378-7206(01)00143-4,

Liébana-Cabanillas, F., García-Maroto I, Muñoz-Leiva F, et al. (2020a) Mobile payment adoption in the age of digital transformation: The case of apple pay. Sustainability 12(13): 5443.

Liébana-Cabanillas F, Japutra A, Molinillo S, et al. (2020b) Assessment of mobile technology use in the emerging market: Analyzing intention to use m-payment services in India. Telecommunications Policy 44(9): 102009.

Lunceford, B, (2009). Reconsidering Technology Adoption and Resistance: Observations of a SemiLuddite. Explorations in Media Ecology. 8 (1): 29–47. https://doi.org 10.1386/eme.8.1.29_1.

Misini, S., & Mustafa, B. (2022). The relationship between economic growth, unemployment and poverty. Corporate Governance and Organizational Behavior Review, 6(4), 57-63.

Monisha, T., Reshma, J., & Shalini, S. (2024). Enhancing banking security through multi-modal biometric authentication system. International Research Journal of Engineering and Technology (IRJET), 10(3), 68-78. 10.5281/zenodo.11489033

Morake, A., Khoza, L.T. & Bokaba, T., 2021, 'Biometric technology in banking institutions: "The customers' perspectives"', South African Journal of Information Management 23(1), a1407. https://doi.org/10.4102/ sajim.v23i1.1407

Morake, A., Khoza, L.T. & Bokaba, T., 2021, 'Biometric technology in banking institutions: "The customers' perspectives"', South African Journal of Information Management 23(1), a1407. https://doi.org/10.4102/ sajim.v23i1.1407

Onesi-Ozigagun, O., Ololade, Y. J., Eyo-Udo, N. L., & Oluwaseun, D. (2024). AI-driven biometrics for secure fintech: Pioneering safety and trust. *International Journal of Engineering Research Updates, 2024, 06(02), 001–012*.

Oto, I. (2024). FinTech privacy security and customer engagement in Nigerian financial sector. Open Access Research Journal of Science and Technology, 12(2), 155–

168.https://doi.org/10.53022/oarjst.2024.12.2.0146

Patil P, Tamilmani K, Rana NP, et al. (2020) Understanding consumer adoption of mobile payment in India: Extending meta-UTAUT model with personal innovativeness, anxiety, trust, and grievance redressal. International Journal of Information Management 54: 102144.

Piotrowska, A. I. (2024). Determinants of consumer adoption of biometric technologies in mobile financial applications. Economics and Business Review, 10(1), 81–100. https://doi.org/10.18559/ebr.2024.1.1019

Piotrowska, A. I. (2024). Determinants of consumer adoption of biometric technologies in mobile financial applications. Economics and Business Review, 10(1), 81–100. https://doi.org/10.18559/ebr.2024.1.1019

Rahman, M. R., & Safeena, P. K. (2016). Customer needs and customer satisfaction.

Rane, N. L., Achari, A., & Choudhary, S. P. (2023). Enhancing Customer Loyalty through Quality of Service: Effective Strategies to Improve Customer Satisfaction, Experience, Relationship, and Engagement. International Research Journal of Modernization in Engineering Technology and Science, 5, 427-452.

Saunders, L. (2019). Fintech and Consumer Protection: A Snapshot, National Consumer Law Center, Inc

Singh, A., Squires, J., Yeh, C. J., Heo, K. H., & Bian, H. (2016). Validity and reliability of the developmental assessment screening scale. Journal of family medicine and primary care, 5(1), 124-128.

Tassabehji, R., & Kamala, M. A. (2012). Evaluating biometrics for online banking: The case for usability. International Journal of Information Management, 32(5), 489– 494. https://doi.org/10.1016/j.ijinfomgt.2012.07.001

Wang, J. S. (2021). Exploring biometric identification in FinTech applications based on the modified TAM, Financial Innovation, Springer, Heidelberg, 7(1), pp. 1-24, https://doi.org/10.1186/s40854-021-00260-2

Zhang, L. L., Xu, J., Jung, D., Ekouka, T., & Kim, H. K. (2021). The effects of facial recognition payment systems on intention to use in China. *Journal of Advanced Researches and Reports*, *1*(1), 33-40.