Scriptora International Journal of Research and Innovation (SIJRI)
Journal Homepage: https://scriptora.org

Evaluating the Role of Biometric Authentication in Enhancing Banking Service Quality and Customer Satisfaction Through Perceived Security

Khushboo Narang
Research Scholar
School of Commerce, Gujarat University, Ahmedabad, Gujarat

Dr. Seema Hariramani
Research Supervisor
School of Commerce, Gujarat University, Ahmedabad, Gujarat

Abstract

Biometric Authentication has been utilized in an increased number of ways with continual improvements to both security and the efficiency of providing service within the Digital Banking marketplace. The study explores how Effectiveness of Biometric Authentication (EBA), Perceived Security and Fraud Protection (PSFP) and Service Quality & Risk Management (SQRM) work together to create Customer Satisfaction and Trust (CST) within the banking Sector. The methodology applied was a quantitative research design where a sample size of 218 Bank Customers using Biometric Authentication was surveyed utilizing a structured questionnaire that was based on a Five Point Likert Scale. The research method employed included the use of correlation analysis, multiple regression, One-Way ANOVA using SPSS 20. Results indicated high and positive correlations between all variables studied. Multiple regression analysis results indicated that EBA, PSFP and SQRM collectively explained 87.7% of the variance in CST creating a very strong and statistically significant model. Regression analysis indicated that EBA, PSFP and SQRM all collectively play important roles in creating Customer Satisfaction and Trust. One-Way ANOVA results indicated that there are significant differences in the way that customers perceive EBA among different types of banks. However, customers perceived the security, service quality and customer satisfaction and trust to be similar among these types of banks. The findings of the study are supported by the Technology Acceptance Model, Trust Theory, SERVQUAL Model and Expectation–Confirmation Theory emphasizing the combined influence of technology, security and service quality. The study identifies practical applications for banks to expand their use of biometric systems, increase security assurance levels and ensure that their digital banking platforms provide customers with a high level of service so that they may maintain long-term confidence and satisfaction.

Keywords: Biometric authentication, Customer Satisfaction, Fraud Protection, Perceived Security, Risk Management, Service Quality.

1. Introduction

Biometric banking got its start with pilot programs in the US and Europe in the early 2000s. However, due to advancements in smartphone tech like Touch ID, the sector really took off after 2010. Big banks like HSBC and JPMorgan adopted fingerprint ID on their mobile apps and login failures to the apps dropped by an astonishing 90 percent. In 2010, the Unique Identification Authority (UIDAI) of India rolled out the Aadhaar biometric system, which allowed for paperless KYC procedures and the easy onboarding of over 1.3 billion people, especially in low literacy regions. There was an upsurge in digital transactions in India post demonetisation in 2016 along with the rise in dominance of the Unified Payments Interface (UPI), which meant an increased dependence on biometric facilities. With recent orders that endorse the use of biometrics (such as finger and facial recognition) for instant UPI and e-commerce transactions, the Reserve Bank of India (RBI) has implemented the use of multi-factor authentication which has done away with the use of OTPs and is steering the use of biometrics. With an industry expected to be losing substantial amounts to fraud, other industry players are now expected to follow the lead of the Federal Bank

which was the first to deploy biometric facilities for e-commerce, achieving authentication in under 2 seconds while complying with the Reserve Bank of India (RBI) tokenisation requirements. Biometrics outperform traditional methods by offering enhanced liveness detection, which prevents spoofing using advanced techniques like 3D mapping and behavioural analysis and achieves false acceptance rates below 0.01%. According to studies, the user experience is significantly improved, with a 40% increase in customers' perceptions of security and an 80% increase in the speed of the login process. Additionally, by lowering operational errors, they ensure compliance with stringent data protection regulations, such as the General Data Protection Regulation (GDPR) under India's Data Protection and Digital Personal Data Protection (DPDP) Act of 2023. Despite privacy and device dependency concerns, the use of encrypted cloud matching in accordance with FIDO standards is regarded as a practical strategy. The purpose of the study is to determine how biometric authentication affects Indian digital banking customers' perceptions of security, service quality, and satisfaction. It looks at how, in comparison to conventional techniques, technologies like fingerprint and facial recognition improve operational dependability, loyalty, and fraud prevention.

2. Literature Review

The trend toward rapid implementation of Digital Technologies is creating a very rapid rate of adoption of advanced digital technologies in Banking and Financial Services Sector, including AI and Biometric Authentication, which are both designed to improve Security, Enhanced Service Efficiency, and Enhanced Customer Experience. Research indicates that Biometric Authentication Systems (which include Fingerprint, Iris, and Voice Recognition), are much more secure and efficient than the traditional Password-based system for protecting Personal Data and Information (Deane et al., 1995). As such, Biometric Authentication has the potential to greatly reduce incidents of Identity Theft and Unauthorized Access, and Fraud. Biometric Authentication has become especially critical in Banking and Financial Services, where the confidentiality of Personal Data and Information, as well as Security of Transactions, is of utmost concern (Mihajlovic, 1999). A critical aspect of customers' confidence and continuing to utilize digital banking platforms for online transactions is said to be their perceived sense of security regarding the authentication methods used by these platforms (Siagian et al., 2022). Studies that have examined both technology acceptance and trust models support this assertion, finding that when users believe that the authentication mechanisms provided by a digital banking service are secure and trustworthy, they are much more likely to have confidence in those services (Siagian et al., 2022). In addition to reducing users' ultimately perceived risks, effective authentication methods can increase users' perception of the usefulness and ease of use of a digital banking service (Davis, 1989). Consequently, these elements of effective authentication collectively enhance users' intention to engage with and remain satisfied with a digital banking service (Davis, 1989). AI innovations have been shown through current research to affect banking performance and customer-driven results. AI provides banks with the ability to perform fraud detection, manage risk, and create predictive analytics, as well as provide personalized service. All of these factors contribute to improved operational efficiencies and ultimately an enhanced overall customer experience (Gyau et al., 2024). In addition, through AI-enhanced systems, travelers will have the ability to log in more quickly than ever before, enjoy a more streamlined transaction process, and receive proactive risk management services. Additionally, these enhancements will significantly help increase customers' trust and satisfaction with banks and their banking services. The enhanced security of AI-based systems will also play a crucial role in helping banks provide a secure environment to their customers (Shiyyab et al., 2023). Through the use of AI breakthroughs, banks' productivity can be improved through the use of advanced techniques for combating fraud, managing risk and analysing potential risks through predictive analytics as well as enabling a more tailored banking experience. The increasing number of banks that employ AI-enabling systems will generate greater improvement in their ability to be efficient and effective and provide better service to their clients (Gyau et al., 2024). The increased security offered through the use of AI systems is critical in creating a secure environment for both the banks and their clients (Shiyyab et al., 2023).

2.1 Effectiveness of Biometric Authentication

The security of digital banking is enhanced through the use of biometric authentication which has a high degree of accuracy, provides increased convenience and prevents identity theft. In contrast to traditional passwords that are easily forgotten or compromised, biometric authentication relies on unique physical or behavioural traits of the individual using the service, thereby significantly enhancing the degree of accuracy when authenticating users. According to Deane et al. (1995), some examples of biometric authentication methods include fingerprint scanning, iris scanning, and voice recognition (biometric authentication is highly reliable for securing sensitive financial data). The Technology Acceptance Model suggests that perceived usefulness and ease of use are the two major determinants influencing user acceptance of new technology (Davis, 1989). The implementation of effective biometric authentication results in faster access, requires less effort to login and consequently, increases user acceptance (Siagian, 2022). Evidence has shown that by providing users with secure and easy-to-use methods of authentication, trust is created, which increases the likelihood of using digital payment systems. Recent studies have demonstrated

that through sophisticated pattern matching and real-time verification of biometric information, AI is helping to improve biometric systems (Königstorfer & Thalmann, 2020; Gyau et al., 2024). Additionally, Shiyyab et al. (2023) have indicated that organisations adopting advanced technologies benefit from increased reliability and improved organisational performance. Overall, the use of effective biometric authentication will provide users with enhanced levels of security, increased trust and improved levels of customer satisfaction within the digital banking industry. Thus, in the context of Effectiveness of Biometric Authentication, the following hypothesis is proposed:

H_1: Effectiveness of Biometric Authentication has a positive impact on Customer Satisfaction & Trust.

2.2 Perceived Security & Fraud Protection

Building customer trust in digital banking services relies on perceived security and fraud protection. Customers trust that banks will protect their information and provide protection against fraud. According to Deane et al. (1995), customers perceive additional security from the use of biometric authentication, which reduces customers' confidence in the vulnerability of passwords and strengthens their perception of the security of online banking services. Studies conducted by Siagian (2022) demonstrate a very high positive correlation between perceived security, trust and the intent to act. Research studies conducted by Almaiah et al. (2019, 2021) show that perceived security and trust are major factors in making the decision to use mobile banking and payment methods. Additionally, artificial intelligence has improved the risk of fraud through real-time monitoring and the use of anomaly detection (Königstorfer & Thalmann, 2020; Gyau et al., 2024). Mondego and Gide (2023) also found that the inclusion of security features has a substantial impact on customers' trust and acceptance of technology. Overall, the literature indicates that having strong perceived security and fraud protection helps to reduce customer anxiety, build trust and enhance ongoing interaction with digital banking services. Thus, in the context of Perceived Security & Fraud Protection, the following hypothesis is proposed:

H_2: Perceived Security & Fraud Protection has a positive impact on Customer Satisfaction & Trust.

2.3 Service Quality & Risk Management

Service quality and risk management are critical for how customers view the reliability and performance of banking, especially in the digital space. Service quality includes efficiency, responsiveness, availability of systems and accuracy of transactions. Risk management reduces the risk of operational and technological failures. Research by Gyau et al. (2024) found that banks use AI advancements to increase efficiency for service delivery and assess risk. Other research by Königstorfer and Thalmann (2020) showed the role of AI in providing automated services, detecting fraud and managing compliance to ensure the delivery of consistent service. Transparency of AI use leads to improved governance and oversight of risk according to Shiyyab et al. (2023). From the perspective of technology acceptance, Davis (1989) found that users who perceive the usefulness and performance of their system are more likely to have positive user experiences, while Siagian (2022) found that reliable service providers build trust with customers. Mondego and Gide (2024) identified high-quality service as one of the factors that influence customers to trust and intend to use banking services. In summary, the combination of providing customers with high-quality service and managing risk effectively results in increased operational stability and customer confidence in banking services. Thus, in the context of Service Quality & Risk Management, the following hypothesis is proposed:

H_3: Service Quality & Risk Management has a positive impact on Customer Satisfaction & Trust.

2.4 Customer Satisfaction & Trust

Customer satisfaction and trust are two important factors in developing successful digital banking relationships. Customer satisfaction is due to positive experiences with a financial institution's services, while building trust means that the customer has continued confidence in that institution. As per Siagian (2022), trust acts as a mediator between how secure a customer feels about their information with a financial institution and their willingness to use that institution in the future. The presence of technology has changed the way financial institutions provide services to customers. As shown in the findings of Gyau et al. (2024), the application of artificial intelligence (AI) to improve service quality also has a positive impact on reducing customer risk associated with using that technology. Shiyyab et al. (2023) stress the need for transparency when developing and implementing AI solutions to establish a long-term trust relationship with customers. Almaiah et al. (2023) emphasized that the customer must feel secure using a financial institution's services, and that the quality of those services as perceived determines the level of trust between the customer and the financial institution, as well as the extent to which the customer continues to use the institution's services. The impact of perceived risk on customer satisfaction and the assurance of an institution's compliance with regulations on the establishment of trust with the customer has also been highlighted in recent research (Rakočević et al., 2025; Gupta & Shukla, 2024). Mondego and Gide (2024) have concluded that a customer's trust is an integral component of the customer-institution relationship between system quality and ongoing customer adoption. Thus, satisfied customers will continue to trust their bank as long as it delivers safe and secure, reliable and high-quality services.

Based on the above literature review, the following model of study was developed:

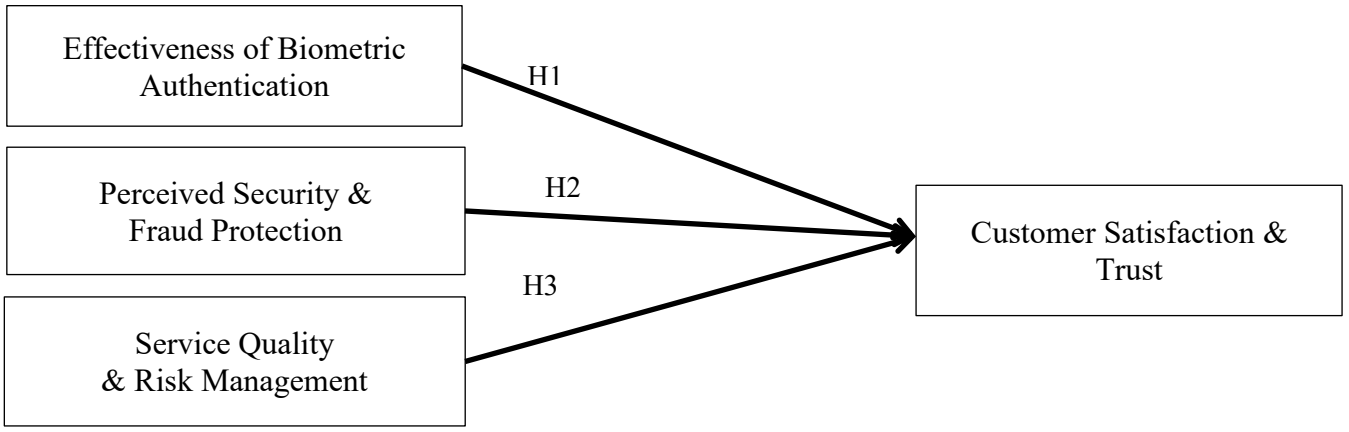


Figure 1 Proposed Model of Study

3. Research Methodology

The systematic process of gathering, evaluating and interpreting data to answer research questions while upholding validity, reliability and ethical standards is known as research methodology. This study investigates the function of biometric authentication in banking and its impact on Customer Satisfaction and Trust using a quantitative approach with a descriptive cross-sectional design. The study's four main goals are to evaluate the effectiveness of biometric systems, assess how satisfaction is affected by perceived security, analyse service quality & risk management and look at the collective effect of these factors. A five-point Likert scale was used to collect data via an online questionnaire and reliability was confirmed by a pilot study (Cronbach's alpha = 0.957). 218 active biometric users were the target of a non-probability convenience sampling technique, which offered a strong basis for quantitative analysis and hypothesis testing to guarantee trustworthy results. Analysis of the collected data was done using SPSS 20. The study includes several independent variables in the context of banking services: Effectiveness of Biometric Authentication (EBA), which measures the accuracy, reliability and convenience of biometric systems in authenticating customers, Perceived Security and Fraud Protection (PSFP) relates to customers' feelings of safety and data protection while using these services and Service Quality and Risk Management (SQRM) which reflects customers' evaluations of service efficiency, reliability, responsiveness and the management of operational and financial risks by the bank, each playing a pivotal role in influencing the Customer Satisfaction & Trust (CST) which measures the overall level of customer satisfaction and the chances of maintaining a longstanding trusting association with the bank.

4. Data Analysis & Discussions

Table 1 Demographic Composition of Sample

Demographics	Frequency	Percentage
Gender		
Male	98	45
Female	120	55
Age		
18-25	148	67.9
26-35	24	11
36-45	28	12.8
46+	18	8.3
Type of Bank		
Nationalized Bank	88	40.4
Private Bank	106	48.6
Co-operative Bank	24	11
Frequency of using Biometric		
Regularly	108	49.5
Often	56	25.7
Rarely	54	24.8
Biometric method preferred		
Fingerprint	130	59.6
Face Recognition	71	32.6
Voice Recognition	11	5.05
Iris Scan (Eye scan)	6	2.75
Total	218	100

Correlation Analysis

Correlations

		EBA	PSFP	SQRM	CST
EBA	Pearson Correlation	1	.809**	.825**	.767**
	Sig. (2-tailed)		.000	.000	.000
	N	218	218	218	218
PSFP	Pearson Correlation	.809**	1	.893**	.899**
	Sig. (2-tailed)	.000		.000	.000
	N	218	218	218	218
SQRM	Pearson Correlation	.825**	.893**	1	.919**
	Sig. (2-tailed)	.000	.000		.000
	N	218	218	218	218
CST	Pearson Correlation	.767**	.899**	.919**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	218	218	218	218

**. Correlation is significant at the 0.01 level (2-tailed).

Strong linear relationships between the variables are revealed by all correlation coefficients, which are all positive and significant at the 0.01 level. The strongest correlations are found between EBA and PSFP (r = 0.809), SQRM (r = 0.825), and CST (r = 0.767), indicating a close relationship between perceived security, service quality and customer satisfaction and successful biometric authentication. Higher security perceptions are associated with better service quality and customer trust, according to PSFP's very strong correlations with SQRM (r = 0.893) and CST (r = 0.899). Furthermore, SQRM has the strongest correlation (r = 0.919) with CST, highlighting the close connection between customer satisfaction, risk management and service quality. Significant relationships between all the variables under study are reflected in the correlations, which range from 0.767 to 0.919.

Regression Analysis

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.936[a]	.877	.875	.36570	.877	506.346	3	214	.000	1.744

a. Predictors: (Constant), SQRM, EBA, PSSP

b. Dependent Variable: CST

With a R value of 0.936, the regression model shows a strong correlation between the independent and dependent variables. SQRM, EBA and PSFP account for 87.7% of the variance in CST, according to the R Square value of 0.877. The robustness of the model is further supported by an Adjusted R Square of 0.875. The model's statistical significance is demonstrated by the F Change value of 506.346 (p = 0.000), indicating significant contributions from the predictors. The estimate's standard error of 0.36570 indicates a high level of model accuracy. Regression assumptions are also satisfied by the Durbin–Watson statistic of 1.744, which verifies that there is no significant autocorrelation in the residuals.

ANOVA[b]

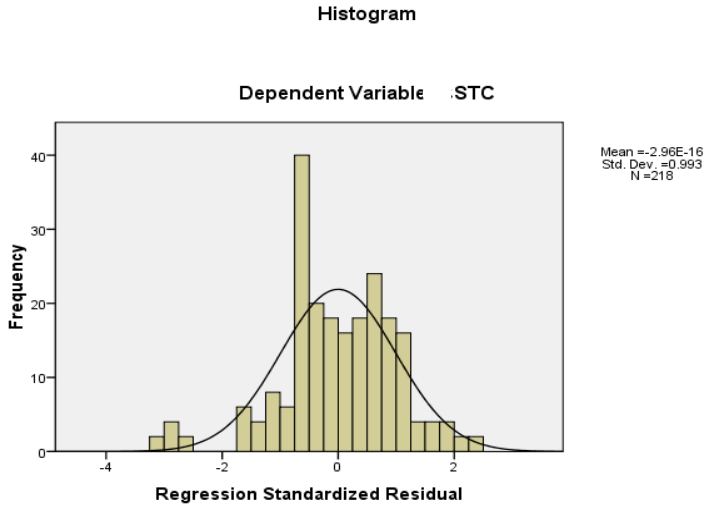
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	203.149	3	67.716	506.346	.000[a]
	Residual	28.619	214	.134		
	Total	231.768	217			

a. Predictors: (Constant), SQRM, EBA, PSSP

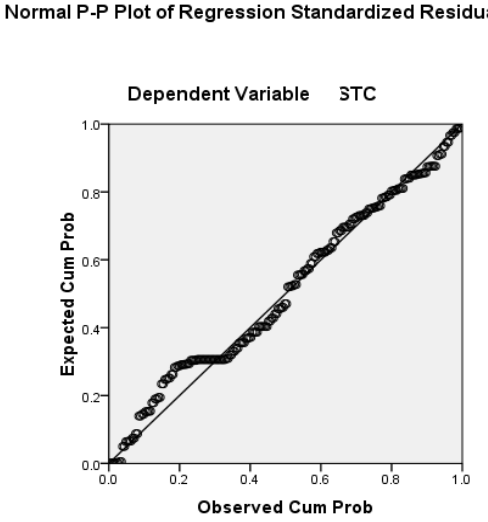
b. Dependent Variable: CST

Independent variables significantly explain the variation in CST, as evidenced by the Regression Sum of Squares

(203.149) being significantly larger than the Residual Sum of Squares (28.619). The regression explains the majority of the variability with a total sum of squares of 231.768. With three degrees of freedom for regression and 214 for residuals, the model's mean square for regression (67.716) is significantly higher than the mean square error (0.134). The model's statistical validity and the predictors' ability to explain CST variance are confirmed by the high F-statistic of 506.346, which is significant at p = 0.000.



The symmetry of the residuals around zero indicates that the residual distribution is normal based on factors such as centredness and standard deviation (standard deviation of the standardized residual is approximately 1 (i.e., 0.993), while the average is approximately 0 (i.e., −2.96E−16)). There are no unusually large or small residuals (outliers), and therefore, most of the residual values fall within the range of −3 to +3. As a result, there is very little difference between the histogram of the residuals and that of a normal distribution as indicated above. In conclusion, with 218 samples overall, the sample size is adequate to support the conclusion mentioned above.



The plotted points adhere closely to the diagonal reference line and exhibit strong congruence with both the observed values and those that were predicted. The presence of minor deviations from either extreme of the plot does not indicate any substantial deviation from what should be expected. The majority of residuals appear to closely approximate a normal distribution in that they are tightly clustered along the diagonal line in the central portion of the plot. It is considered acceptable to have small deviations at the tails of the distribution due to the large sample size of 218 observations and these do not impact the overall normality of the residuals.

ANOVA

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
EBA	Between Groups	8.234	2	4.117	5.178	.006
	Within Groups	170.939	215	.795		
	Total	179.174	217			
PSSP	Between Groups	4.444	2	2.222	2.836	.061
	Within Groups	168.454	215	.784		
	Total	172.898	217			
SQRM	Between Groups	1.259	2	.629	.772	.464
	Within Groups	175.362	215	.816		
	Total	176.621	217			
CST	Between Groups	3.912	2	1.956	1.845	.160
	Within Groups	227.857	215	1.060		
	Total	231.768	217			

With a F value of 5.178 and a p-value of 0.006, the EBA ANOVA results show a significant difference between bank types, indicating different customer perceptions of the effectiveness of biometric authentication. PSFP, on the other hand, has a p-value of 0.061 and a F value of 2.836, indicating no significant difference. Both SQRM (F value of 0.772, p-value of 0.464) and CST (F value of 1.845, p-value of 0.160) show no significant variation, indicating that customer satisfaction, risk management techniques and service quality are perceived similarly across bank types.

5. Findings & Discussion

1. The correlation results from the study support the proposed framework and show that there is a positive and significant correlation between the Perceived Security and Fraud Prevention (PSFP) and Effectiveness of Biometric Authentication (EBA), which suggest that increased trust in banking security for consumers is associated with enhanced Customer Satisfaction and Trust with their Bank (CST). Therefore, a more secure banking environment provides an environment for loyal customers to continue to utilize their banking services. The findings also highlight the importance of having a high level of Service Quality and Risk Management (SQRM) for maintaining customer confidence and loyalty. Collectively, less fraudulent attempts from biometric authentication, improved security perceptions associated with Biometric Authentication and Service Quality, can result in an increase in Customer Satisfaction and Trust.
2. Based on the results of regression analysis, the factors affecting both customer satisfaction and trust in a continued relationship with a bank are quality of services delivered, the effectiveness of biometric authentication systems and the level of security and fraud protection perceived by customers. The validity of this model framework has been established through a statistically significant F value, which indicates that the components of this model explain the behaviour of consumers toward banks and provide very high explanatory power for their behaviour. Therefore, if banks want to enhance their customers' trust in their products, then banks should focus on improving the technology and security associated with Biometric Authentication. Overall, Risk Management and Business Operational Efficiency are dominant variables affecting consumers' behaviour in Online Banking.
3. The standardized residuals' histogram indicates that the regression model is in compliance with the assumption of error normality and therefore indicates that the regression estimates and tests of significance derived from this model are therefore statically sound. As there is no evidence of significant skewness or kurtosis present in the residuals, it indicates that the independent variables provided an adequate explanation for CST and there are no patterns of systematic prediction errors within the model. Therefore, due to the normality of the residuals, the validity of the multiple regression analysis and its conclusions with respect to the effect of SQRM, EBA, and PSFP on Customer Satisfaction and Trust is supported.
4. According to the normal probability plot, one of the basic assumptions of a multiple regression is met that is, the standardized residuals from the regression appear to be almost normally distributed. The distribution of

the data points being aligned with a diagonal line shows that the errors associated with the predictions of Customer Satisfaction and Trust (CST) were randomly and normally distributed. The absence of systematic deviations suggests that there is no violation of normality in terms of how the model was specified. This data gives a greater confidence in the results and conclusions of this research regarding the influence of Service Quality and Risk Management (SQRM), Effectiveness of Biometric Authentication (EBA) and Perceived Security and Fraud Protection (PSFP) on Customer Satisfaction and Trust (CST).

5. The results of One-Way ANOVA indicate that although security perception, service quality, overall Customer Satisfaction and Trust were unaffected by the type of Bank, there was a significant impact on consumers' perception of the effectiveness of Biometrics verification from the type of Bank. The differences in effectiveness observed among the banks can be attributed to technological advances and the innovation of both banks and consumers; as well as the differences in the way banks apply biometrics and how consumers experience using them. The agreement among consumers of banks regarding the security and service quality between Banks indicates that financial services are becoming more standardized. As a result of the continued variation in the effectiveness of biometric authentication, it is evident that there are no major changes in service outcomes; however, it does indicate that the Banking Industry continues to demonstrate consistent procedures.

6. Study Implications

6.1 Theoretical Implications

Strong relationships exist between Customer satisfaction and trust (CST), Service Quality and Risk Management (SQRM), Perceived Security and Fraud protection (PSFP) and Effectiveness of Biometric Authentication (EBA). The research findings validate the Technology Acceptance Model (TAM), in general, when customers perceive a biometric system to be effective, they will enjoy higher levels of Customer Satisfaction and Trust. According to Trust Theory, customers must perceive security and fraud protection to have high levels of trust in the Digital Banking Services they use. The connection between SQRM and CST underscores the SERVQUAL Model of determining service quality. That is, when effective risk management practices are part of the customer experience of a Financial Institution, customers will perceive the service provided by that Institution to be reliable and of high customer satisfaction. High explanatory power (R-squared value of 0.877) validates the Expectation–confirmation Theory (ECT), which states that the more closely customers' expectations are met, the higher the level of customer satisfaction and trust in the service provided. Therefore, the research demonstrates that aligning the technology of the service with the customers' perception of security and fraud protection, as well as providing a high level of service quality, are all necessary to satisfy customer expectations and increase the level of trust in the service provided. Additionally, One-way ANOVA results indicate that while there is some difference between bank types regarding EBA, the regulatory framework of each bank type creates a standardised level of PSFP, SQRM and CST. Thus, the findings confirm the integrated technology-service-security framework for explaining Customer Satisfaction and Trust for Biometric Banking Services.

6.2 Practical Implications

By adopting advanced technology, banks can improve customer satisfaction and build customer trust by placing an emphasis on upgrading their biometric authentication systems. Through the use of a combination of high service quality, proper risk management (Service Quality and Risk Management), and fast dispute resolution, banks will be able to provide their customers with accurate transactions. In addition to providing an accurate transaction experience, banks must communicate clearly about the security measures they take to protect customers' data (i.e. how they protect customers' information) since doing so will increase the likelihood of strong customer perception of security. The effectiveness of biometric systems varies by bank, demonstrating a need for improved technology across banking institutions. Although customer trust does not vary significantly between banks, the study demonstrates that providing improved technology, security and customer service operations translates to increased customer loyalty. In conclusion, to continue benefiting from digital banking, banks must use advanced technology, provide reliable service and implement strong risk management practices to ensure continued trust from their customers.

6.3 Policy Implications

According to the research, banks should enforce a singular Biometric Authentication process to ensure standardized efficiency and dependability Company Policies and Regulations regarding Digital Security and Fraud Prevention must be strengthened significantly, as Perception of Safety directly impact Consumer Satisfaction and Trust. The study also highlights the need for mandatory Risk Management and Service Quality frameworks to be compiled through frequent audits and monitoring. Policymakers should promote greater transparency and consumer knowledge regarding Security Procedures and the usage of Biometric Authentication. Support should also be extended to banks that lack sufficient infrastructure to upgrade their technologies and to ensure their compliance with Data Protection and Privacy legislation. A risk-based Regulatory Approach that will provide stability and confidence to Customers in Digital Banking Systems creates trust indicators within Customers.

Directions for Further Research

Future research studies could increase sample size and conduct respondent demographic analysis for greater generalizability. Also, researchers may perform comparative analyses of biometric authentication with security measures like passwords, OTPs and multi-factor authentication. Longitudinal studies can be performed to investigate how perceptions changes over time. Future research may also delve into variables such as privacy concern, perceived risk, trust and technology awareness to provide further understanding. Cross-cultural researches might add to differences in adopting across areas. Also explore the impact of new technologies like AI-based biometrics and facial recognition, staff concerns about ethics and data security. Finally, comparative studies between sectors would bring a better overview of biometric authentication effectiveness.

References

1. Almaiah, M. A., & Alismaiel, O. A. (2019). Examination of factors influencing the use of mobile learning systems: An empirical study. Education and Information Technologies, 24(1), 885–909.
2. Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security, and perceived trust on smart m-banking applications using SEM. Sustainability, 15(13), 9908.
3. Alnaser, F. M., Rahi, S., Alghizzawi, M., & Ngah, A. H. (2023). Does artificial intelligence boost digital banking user satisfaction? Integration of expectation confirmation model and AI antecedents. Heliyon, 9(8), e18745.
4. Al-Okaily, M., Al-Kofahi, M., Shiyyab, F. S., & Al-Okaily, A. (2025). Determinants of user satisfaction with financial information systems in the digital transformation era: Insights from emerging markets. Global Knowledge, Memory and Communication, 74(3–4), 1171–1190.
5. Barjaktarovic Rakocevic, S., Rakic, N., & Rakocevic, R. (2025). An interplay between digital banking services, perceived risks, customers' expectations, and customers' satisfaction. Risks, 13(3), 39.
6. Batra, S., Gupta, M., Singh, J., Srivastava, D., & Aggarwal, I. (2020). An empirical study of cybercrime and its preventions. In Proceedings of the Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC) (pp. 42–46). IEEE.
7. Bhat, S. A., Islam, S. B., & Mir, M. F. (2024). Consumers' attitude toward biometric banking services: An empirical evaluation of determinants and outcomes. Journal of Financial Services Marketing, 29(4), 1572–1588.
8. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.
9. Deane, F., Barrelle, K., Henderson, R., & Mahar, D. (1995). Perceived acceptability of biometric security systems. Computers & Security, 14(3), 225–231.
10. Febriend, S. D., & Qastharin, A. R. (2024). The impact of service quality and electronic service quality on customer satisfaction and customer loyalty: A study of Bank Central Asia customers. Mandalika Journal of Business and Management Studies, 2(2), 167–188.
11. Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. International Journal of Human-Computer Studies, 59(4), 451–474.

12. Gupta, V., & Shukla, S. (2024). Consumer trust in digital banking: A qualitative study of legal and regulatory impacts. Interdisciplinary Studies in Society, Law, and Politics, 3(2), 18–24.
13. Gyau, E. B., Appiah, M., Gyamfi, B. A., Achie, T., & Naeem, M. A. (2024). Transforming banking: Examining the role of AI technology innovation in boosting banks' financial performance. International Review of Financial Analysis, 96, 103700.
14. Harasimiuk, A., & Czyżewski, A. (2023). Usability study of various biometric techniques in bank branches. Procedia Computer Science, 225, 2126–2135.
15. Jun, M., & Cai, S. (2001). The key determinants of internet banking service quality: A content analysis. International Journal of Bank Marketing, 19(7), 276–291.
16. Königstorfer, F., & Thalmann, S. (2020). Applications of artificial intelligence in commercial banks: A research agenda for behavioral finance. Journal of Behavioral and Experimental Finance, 27, 100352.
17. Li, C., & Li, H. (2023). Disentangling facial recognition payment service usage behavior: A trust perspective. Telematics and Informatics, 77, 101939.
18. Mondego, D., & Gide, E. (2024). The impact of security, service quality, perceived usefulness, perceived ease of use, trust, and price value on users' satisfaction in cloud-based payment systems in Australia: A PLS-SEM analysis. JISTEM – Journal of Information Systems and Technology Management, 21, e202421004.
19. Oliver, R. L. (1980). A cognitive model of the antecedents and consequences of satisfaction decisions. Journal of Marketing Research, 17(4), 460–469.
20. Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1988). SERVQUAL: A multiple-item scale for measuring consumer perceptions of service quality. Journal of Retailing, 64(1), 12–40.
21. Purohit, H., Dadhich, M., & Ajmera, P. K. (2023). Analytical study on users' awareness and acceptability toward adoption of multimodal biometrics in online transactions: A SEM–ANN approach. Multimedia Tools and Applications, 82(9), 14239–14263.
22. Shin, D. H. (2010). The effects of trust, security, and privacy in social networking: A security-based approach to understanding adoption. Interacting with Computers, 22(5), 428–438.
23. Shin, D. H. (2010). Modeling the interaction of users and mobile payment systems: A conceptual framework. International Journal of Human-Computer Interaction, 26(10), 917–940.
24. Siagian, H., Tarigan, Z. J. H., Basana, S. R., & Basuki, R. (2022). The effect of perceived security, perceived ease of use, and perceived usefulness on behavioral intention through trust in digital payment platforms. Doctoral dissertation, Petra Christian University.
25. Sultana, R., & Faisal, N. A. (2024). The role of digital banking features in bank selection: An analysis of customer preferences for online and mobile banking. SSRN Electronic Journal.
26. Syed, W. K., Mohammed, A., Reddy, J. K., & Dhanasekaran, S. (2024). Biometric authentication systems in banking: A technical evaluation of security measures. In Proceedings of the IEEE 3rd World Conference on Applied Intelligence and Computing (AIC) (pp. 1331–1336). IEEE.
27. Vergallo, R., & Mainetti, L. (2022). The role of technology in improving customer experience in the banking sector: A systematic mapping study. IEEE Access, 10, 118024–118042.