



Examining The Influence Of Security, Privacy, And Financial Risk On Digital Banking Service Adoption: Evidence From Customers Of Public Sector Banks In Bengaluru.

¹ Soumyalatha,² Jennifer Nancy R

¹ Assistant professor, ² Assistant professor

Soundarya institute of management and science

Abstract: The rapid expansion of digital banking services has transformed the financial ecosystem in India, particularly within public sector banks. However, concerns related to security, privacy, and financial risk continue to influence customers' adoption decisions. This study examines the impact of perceived security risk, privacy risk, and financial risk on digital banking service adoption among customers of public sector banks in Bengaluru. Using a quantitative research design, primary data were collected from customers through a structured questionnaire. Statistical tools such as correlation and regression analysis were employed to assess the relationship between perceived risks and adoption behaviours. The findings reveal that security and privacy concerns significantly affect customers' willingness to adopt digital banking services, while financial risk perception moderately influences adoption decisions. The study highlights the need for public sector banks to strengthen cybersecurity measures, enhance transparent data protection policies, and build customer trust through awareness initiatives. The research contributes to the growing literature on digital banking adoption by providing empirical evidence from an emerging economy context and offers practical implications for policymakers and banking institutions aiming to accelerate digital transformation.

Index Terms - Digital Banking Adoption; Perceived Security Risk; Privacy Risk; Financial Risk; Public Sector Banks; Customer Trust; Technology Acceptance.

I. INTRODUCTION:

The banking sector in India has undergone significant transformation with the rapid adoption of digital technologies, particularly after initiatives promoting digital financial inclusion. Public sector banks have increasingly introduced internet banking, mobile banking, UPI-based transactions, and digital payment platforms to enhance customer convenience and operational efficiency. Despite these advancements, customer adoption of digital banking services remains influenced by perceived risks associated with online transactions. The Security risk, privacy risk, and financial risk are among the most critical concerns affecting customers' trust in digital platforms. Security risk refers to fears of cyberattacks and unauthorized access, privacy risk relates to misuse of personal and financial data, and financial risk involves potential monetary loss due to fraud or transaction errors. In metropolitan cities like Bengaluru, where digital penetration is high, understanding these risk perceptions becomes crucial for public sector banks to sustain competitiveness.

This study aims to examine the influence of security, privacy, and financial risk on digital banking service adoption among customers of public sector banks in Bengaluru. The findings will provide insights for improving customer confidence and strengthening digital banking strategies.

II. RESEARCH OBJECTIVES:

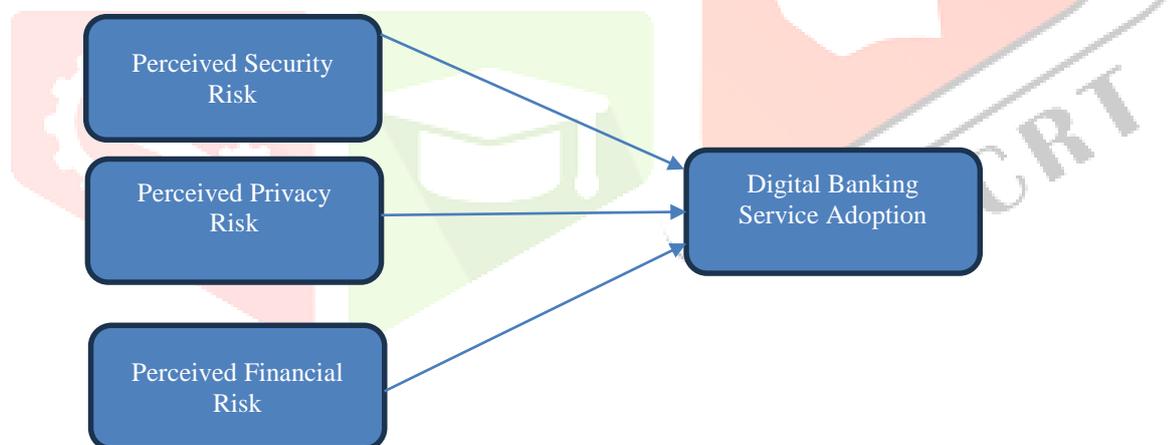
- To examine the influence of perceived security risk on digital banking service adoption among customers of public sector banks in Bengaluru.
- To assess the impact of perceived privacy risk on customers' intention to adopt digital banking services in public sector banks.
- To analyse the effect of perceived financial risk on digital banking service adoption behaviour among customers of public sector banks in Bengaluru.

III. RESEARCH HYPOTHESES:

- H₀₁: Perceived security risk has no significant influence on digital banking service adoption among customers of public sector banks in Bengaluru.
- H₀₂: Perceived privacy risk has no significant influence on digital banking service adoption among customers of public sector banks in Bengaluru.
- H₀₃: Perceived financial risk has no significant influence on digital banking service adoption among customers of public sector banks in Bengaluru.

IV. CONCEPTUAL FRAMEWORK:

The framework proposes that customers' perceptions of security, privacy, and financial risks directly influence their adoption of digital banking services. The relationship can be empirically tested using Multiple Regression Analysis:



V. RESEARCH METHODOLOGY:

This study adopts a **quantitative and descriptive research design** to examine the influence of perceived security risk, privacy risk, and financial risk on digital banking service adoption among customers of public sector banks in Bengaluru. A cross-sectional survey method was employed to collect primary data from respondents who actively use or are aware of digital banking services such as mobile banking, internet banking, and UPI transactions. The target population comprises customers of selected public sector banks in Bengaluru. Using convenience and purposive sampling techniques, a total of **200 respondents** were selected for the study, which is considered adequate for regression-based analysis in social science research.

Primary data were collected through a structured questionnaire divided into two sections: demographic details and measurement of study variables. The variables—perceived security risk, perceived privacy risk, perceived financial risk, and digital banking service adoption—were measured using multiple items on a **five-point Likert scale** ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). Secondary data were obtained from academic journals, banking reports, and relevant literature to support the conceptual framework.

VI. DATA ANALYSIS AND INTERPRETATION:**Table of Demographic Profile of Respondents:**

Variable	Category	Frequency	Percentage
Gender	Male	118	59%
	Female	82	41%
Age	18–30 years	72	36%
	31–40 years	68	34%
	41–50 years	40	20%
	Above 50	20	10%
Education	Graduate	96	48%
	Postgraduate	74	37%
	Others	30	15%
Digital Usage Experience	< 2 years	52	26%
	2–5 years	88	44%
	> 5 years	60	30%

Interpretation

The majority of respondents (59%) were male. Most participants belonged to the 18–40 age group (70%), indicating higher digital banking engagement among younger customers. Nearly 85% of respondents were graduates or postgraduates, suggesting a relatively educated sample. Additionally, 74% had more than two years of digital banking experience, indicating familiarity with online banking services.

Table of Reliability Analysis

Variable	Cronbach's Alpha
Security Risk	0.82
Privacy Risk	0.79
Financial Risk	0.81
Digital Banking Adoption	0.85

Interpretation

All constructs show Cronbach's alpha values above 0.70, indicating acceptable internal consistency and reliability of the measurement scales.

Table of Correlation Analysis

Variables	PSR	PPR	PFR	DBA
PSR	1			
PPR	0.61**	1		
PFR	0.58**	0.54**	1	
DBA	-0.65**	-0.59**	-0.62**	1

(**p < 0.01)

Interpretation

Perceived security risk ($r = -0.65$), privacy risk ($r = -0.59$), and financial risk ($r = -0.62$) show significant negative relationships with digital banking adoption. This indicates that higher perceived risk reduces adoption levels.

Table of Multiple Regression Analysis

Model Summary

R	R ²	Adjusted R ²	F-value	Sig.
0.71	0.50	0.48	65.32	0.000

Interpretation

The model explains **50% of the variance** in digital banking adoption ($R^2 = 0.50$). The F-value is significant ($p < 0.001$), indicating that the model is statistically significant.

Table of Coefficients Table

Variable	Beta	t-value	Sig.
Security Risk	-0.34	-5.21	0.000
Privacy Risk	-0.26	-4.18	0.000
Financial Risk	-0.29	-4.67	0.000

Interpretation of Hypotheses

- **H₀₁ rejected:** Security risk significantly influences digital banking adoption.
- **H₀₂ rejected:** Privacy risk significantly influences digital banking adoption.
- **H₀₃ rejected:** Financial risk significantly influences digital banking adoption.

Security risk has the strongest negative impact, followed by financial risk and privacy risk.

VII. DISCUSSION:

The findings of the study indicate that perceived security risk, privacy risk, and financial risk significantly influence digital banking service adoption among customers of public sector banks in Bengaluru. The regression results reveal that security risk has the strongest negative impact, followed by financial risk and privacy risk. These findings are consistent with prior studies that suggest perceived risk is a major barrier to technology adoption in financial services.

The negative relationship between security risk and digital banking adoption supports the Technology Acceptance Model (TAM) extension, which emphasizes perceived risk as a critical determinant of behavioral intention. Customers are hesitant to use digital banking platforms when they fear cyberattacks, hacking, or unauthorized transactions. Similarly, privacy concerns regarding misuse of personal and financial information reduce customer trust in digital platforms. Financial risk, particularly the fear of monetary loss due to transaction errors or fraud, also significantly discourages adoption.

These results align with earlier empirical research conducted in emerging economies, where trust and perceived risk play a vital role in digital banking acceptance. In the context of Bengaluru—a technologically advanced metropolitan city—the persistence of risk perceptions highlights that technological infrastructure alone does not guarantee adoption. Psychological and trust-related factors remain central to digital transformation in public sector banks.

VIII. MANAGERIAL IMPLICATIONS:

The study provides several important implications for banking managers and administrators:

- **Strengthening Cybersecurity Systems:**

Public sector banks should invest in advanced encryption technologies, multi-factor authentication, AI-based fraud detection, and regular security audits to minimize perceived security risks.

- **Transparent Privacy Policies:**

Banks must clearly communicate data protection measures and comply with regulatory standards. Transparent privacy disclosures can significantly enhance customer trust.

- **Customer Awareness Programs:**

Conducting digital literacy workshops and awareness campaigns can reduce misconceptions about online risks and improve confidence in digital platforms.

- **Efficient Grievance Redressal Mechanisms:**

Quick resolution of digital transaction issues can reduce perceived financial risk and enhance satisfaction.

- **Trust-Building Strategies:**

Personalized communication, assurance messages, and regular security updates can strengthen trust among customers.

IX. CONCLUSION

This study examined the influence of perceived security risk, privacy risk, and financial risk on digital banking service adoption among customers of public sector banks in Bengaluru. The findings confirm that all three risk dimensions significantly and negatively affect adoption behaviour. Among them, security risk emerged as the most influential factor.

The results emphasize that digital banking growth is not solely dependent on technological advancement but also on customers' perceptions of safety and trust. Even in a digitally progressive city like Bengaluru, perceived risks remain a significant barrier to adoption. Therefore, addressing these psychological concerns is essential for accelerating digital banking penetration.

The study contributes to the existing literature by providing empirical evidence from the Indian public banking context and offers practical insights for enhancing digital transformation strategies.

X. POLICY RECOMMENDATIONS:

- **Regulatory Strengthening:**

Policymakers should enforce stricter cybersecurity regulations and data protection laws to enhance customer confidence.

- **Standardized Security Protocols Across Banks:**

Public sector banks should adopt uniform digital security standards to ensure consistency in protection mechanisms.

- **Government-Led Digital Literacy Campaigns:**

Awareness programs at the national and state levels can educate customers about safe digital banking practices.

- **Insurance Against Digital Fraud:**

Introducing mandatory digital transaction insurance schemes can reduce perceived financial risk.

- **Collaboration with FinTech Firms:**

Public sector banks should collaborate with fintech companies to enhance secure digital innovation.

XI. ACKNOWLEDGEMENTS:

- 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. [https://doi.org/10.1016/S1071-5819\(03\)00111-3](https://doi.org/10.1016/S1071-5819(03)00111-3)
- Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, 44(2), 544–564. <https://doi.org/10.1016/j.dss.2007.07.001>
- Lee, M. C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and perceived risk. *Expert Systems with Applications*, 36(9), 11682–11692. <https://doi.org/10.1016/j.eswa.2009.03.08>
- Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding the internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management*, 34(1), 1–13. <https://doi.org/10.1016/j.ijinfomgt.2013.06.002>
- Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Computers in Human Behavior*, 61, 404–414. <https://doi.org/10.1016/j.chb.2016.03.030>
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101–134. <https://doi.org/10.1080/10864415.2003.11044275>
- Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2009). Multi-dimensional role of trust in internet banking adoption. *The Service Industries Journal*, 29(5), 591–605. <https://doi.org/10.1080/02642060902719958>
- Zhou, T. (2012). Examining mobile banking user adoption from the perspectives of trust and risk. *Internet Research*, 22(4), 527–544. <https://doi.org/10.1108/10662241211250928>

