DIGITAL BANKING EMPOWERMENT: UNVEILING NOVEL STRATEGIES TO SAFEGUARD ONLINE TRANSACTIONS FROM FRAUDULENT ACTIVITIES

Dr. K. Moneesh Kumar
Assistant Professor PG & Research Department of Commerce
Dwaraka Doss Goverdhan Doss Vaishnav College (Autonomous), Chennai
dr.moneeshkumark@gmail.com

ABSTRACT
The Purpose of the Study was to examine the digital banking usage and risk mitigation online transaction frauds. A survey of 204 respondents was collected in Chennai city using a structure questionnaire with Likert scale type questions. Convenient sampling techniques were used in this study. Percentage analysis, Descriptive statistics, Regression analysis were used to test the research hypothesis. The findings indicate that the factors such as perceived ease of use, perceived benefits, apps internal attacks and apps external attacks. Perceived Ease of Use, Perceived Benefits, Apps Internal Attacks have positive and significant relationship with Risk Mitigation. Apps External Attacks have a negative and insignificant relationship with Risk Mitigation. The study's conclusions are based on feedback from Chennai. In order to generalise the results, it is crucial to incorporate responders from various cities and states. It would be useful for future researchers to compare the findings with those from other states. The results provide a better understanding of typical risk mitigation in online transaction fraud to digital banking users and make suggestions regarding how they can tailor their offerings to meet user needs. There is no one dominant viewpoint on the factors influencing the use of and risk mitigation for online transaction fraud; instead, these factors vary according to circumstances, markets, period, and national inventions. In regard to Chennai, the study examined a few crucial components that have been discussed in the literature.
Keywords: Risk Mitigation, Perceived Ease of Use, Perceived Benefit, Apps Internal and External Attacks.

Introduction

The rapid advancement of technology has brought significant and ongoing changes to the world. This digital convergence has led bank customers to prefer digital cashless e-transactions on virtual platforms. To address these changes, banks must understand consumer needs, knowledge levels, satisfaction, security concerns, and potential difficulties in online banking. Implementing preventive measures is crucial to mitigate online banking fraud.

The banking industry has transformed rapidly due to technological advancements, introducing new service delivery channels that save time and costs for transactions. Digital banking has become indispensable in society, uniting people under a unified banking system. However, this reliance on technology presents challenges in combating fraud.

The rise of financial technology has brought convenience but also an alarming increase in fraud. Customers now worry about the security of their bank accounts as online information becomes vulnerable to misuse. Hackers exploit sensitive information stored on computers during internet banking, leading to cyber fraud. Unfortunately, many customers are unaware or negligent about maintaining security measures in online banking, contributing to the persistently high number of fraud incidents despite regulatory efforts.

According to Accenture's paper on "Protecting the Customer: Fighting Bank Fraud in a New Environment," the dynamics of client demographics, bank expansion, and new technologies pose fresh challenges in fraud prevention. Criminals leverage computers to perpetrate e-banking fraud, accessing crucial data to harm individuals and businesses. E-banking scams continue to rise, impacting the Indian economy across societies, including Mumbai, where banking fraud is prevalent. The Information Technology Act of 2000 in India addresses e-commerce-related regulations, covering offenses related to e-banking scams.

Fraudsters adapt their strategies in response to fraud prevention measures, creating a cat and mouse game. Financial institutions must maintain vigilance to combat theft. Risk mitigation now utilizes predictive analytics to understand consumer behavior patterns and detect novel signs of fraud. This article examines the role of digital banking in mitigating fraud in online transactions, with the goal of protecting consumers and preventing significant financial losses.

Review of Literature

Ali, Ali, Surendran, and Thomas (2017), Cybercrime is cited as one of the world's most pressing challenges to increase and sustain their financial stability, all financial institutions must be aware of the hazards posed by the

internet and have implemented the necessary security measures. One must comprehend the methods and strategies used by cybercriminals, which they can employ for fraudulent operations, in order to comprehend the security risk. The article provides a starting point for additional research into the fraudsters' methods used in various situations.

Arora and Khannaand (2009), in the authors concentrated on the causes of bank frauds rather than the need to take seriously the raising of alerts regarding bank frauds and to ensure that internal control mechanisms were not lax or lacking in rigour. It is obvious that bank personnel do not have a high level of awareness of frauds, and they do not see the RBI method favourably. The Reserve Bank of India's guidelines for compliance still have poor levels of training, competition, and compliance. However, the document does not outline any potential legal changes or how they might be made.

Bhandari and Soni (2016), the author of "Indian Banking Sector: Then, Now, and the Road Ahead" has essentially examined the early history of banking in ancient India, when moneylenders were the first to collect deposits and issue receipts in their place. With the nationalisation of banks, the standard of banking was exemplified as moving from class banking to mass banking. Financial inclusion and technology are the main causes of the developments in the banking industry. It has been established that technology is an essential component for raising productivity and providing effective customer service.

Dzomira (2014), explored the types of electronic fraud that have been committed in banks and the difficulties they have faced. Even though technology has improved people's convenience, most individuals occasionally become victims of technology in an effort to harness its full potential. Technical disadvantages, ignorance and lack of awareness, and a lack of legal regulations are problems that banks must deal with. Although the study listed a number of electronic fraud subcategories, it omitted to emphasise the fraud's component parts.

Goel (2016), law enforcement should re-evaluate modern digital crime that targets banks and significant financial institutions. Financial gain will always be the driving force behind cybercriminals. Before it's too late, law enforcement organisations need to come up with fresh strategies to combat cyber fraud because it raises a lot of legal difficulties for the regulator as well.

Hoskote (1996), into great detail about how the transition from the barter system to gold to paper money to plastic money to electronic cash has brought us to where we are today with electronic banking, fund transfers, and automated teller machines. However, when electronic money became more widespread, problems with technology-assisted crime soon emerged.

Lal and Saluja (2012), banking services are now available around-the-clock and can even be completed with a single touch. Compared to debit/credit cards, we had less cash in our wallet. Therefore, the advent of information technology is to blame for this significant portion of developments. Our banking system and services have improved thanks to IT, but along with these improvements, cybercrime has become a menace.

Zahoor MoinUd-din, and Karuna, (2016) banking is growing more and more reliant on technology due to the widespread use of technology, particularly the internet. Unfortunately, as a result of this, bank-related cybercrimes are skyrocketing. The banking sector has experienced a significant number of cyber attacks on the security and privacy of their data, including scams involving online payments, net banking transactions, electronic cards, etc. The study also claims that the primary motivation for these institutions is to obtain sensitive information or to steal money from banks, but it does not address the operating methodology that would assist in overcoming the difficulties.

Need for the Study

Banking institutions face heightened risks when it comes to fraud due to the significant trust placed in them for safeguarding people's money and savings. While digital banking offers various benefits, it has also opened doors for fraudsters to exploit its vulnerabilities and carry out sophisticated fraud schemes, resulting in substantial financial losses for institutions. Electronic transfers enable quick and convenient money movement, but reversing transactions can be challenging or even impossible. This study examines the usage of digital banking in India and explores measures to mitigate online transaction fraud.

Objectives of the Study

- To examine the digital banking usage and risk mitigation online transaction frauds

Hypothesis of the Study

The following null hypothesis are

- H_{01}: Perceived Ease of Use was not influenced by Risk Mitigation
- H_{02}: Perceived Benefits was not influenced by Risk Mitigation
- H_{03}: Apps Internal Attacks was not influenced by Risk Mitigation
- H_{04}: Apps External Attacks was not influenced by Risk Mitigation

Limitations of the Study

- Only 408 respondents were included in the survey, so it can't be applied to other locations because it was only done in Chennai.
- Time restrictions are this investigation's main flaw.

Research Methodology

- Sample Location: The study's focus will be on the use of digital banking and the mitigation of online transaction fraud in Tamil Nadu's Chennai district.
- Data Source: The investigation's primary data was collected from primary sources.
- Sample Size: A total of 204 respondents who are customers of digital banking made up the sample.
- Sampling Method: This study employed the convenient sampling method.
- Statistical Tools: Regression analysis, descriptive statistics, and percentage analysis were utilised to analyse the data gathered from the primary source with the use of SPSS version 23.

Data Analysis and Interpretations

Demographic Profile (N = 204)	**Frequency**	**Percentage**
Educational Status		
School Level	12	5.9
Graduate	170	83.3
Post-Graduate	16	7.8
Professional	6	2.9
Number of times using UPI payment (per week)		
Less than 5 Times	110	53.9
5 to 10 Times	54	26.5
10 to 15 Times	14	6.9
More than 15 Times	26	12.7
How frequently do you prefer to use UPI App?		
Every day	132	32.4
Once a week	88	21.6
3-5 Times a Week	76	18.6
Occasionally	112	27.5
(Source: Primary Data)		

Table 1: Demographic Profile of the Respondents

Educational Status: The results of the study indicate that the majority of respondents belong to the graduate 83.3%, followed by 7.8% post-graduate, 5.9% school level and 2.9% belong to professionals.

Number of times using UPI payment (per week): In this study, the most of the respondents belong to less than 5 times 53.9%, followed by 26.5% 5 to 10 times, 12.7% more than 15 times and 6.9% are 10 to 15 times.

How frequent do you prefer to use UPI App: The result of the study among 204 respondents, the most of the respondents are belong to the Everyday usage 32.4%, followed by 27.5% Occasionally, 21.6% once a week, and 18.6% are 3 to 5 times a week.

UPI Apps	UPI Apps Preference in Making Transaction (in %)			
	Not Prefer to Use	**Occasionally**	**Sometimes**	**Often**
PhonePe	23.53	15.69	19.61	41.18
Gpay	2.94	15.69	37.25	44.12
Amazon Pay	35.29	38.24	11.76	14.71
Paytm	37.25	20.59	22.55	19.61
BHIM	37.25	26.47	19.61	16.67
MobiKwik	49.02	18.63	22.55	9.80
Airtel UPI	41.18	24.51	20.59	13.73
iMobile Pay	47.06	26.47	19.61	6.86
Payzapp	50.98	20.59	13.73	14.71
Freecharge	50.98	25.49	14.71	8.82
Others	50.00	24.51	13.73	11.76

Table 2: UPI Apps Preference in Making Transaction

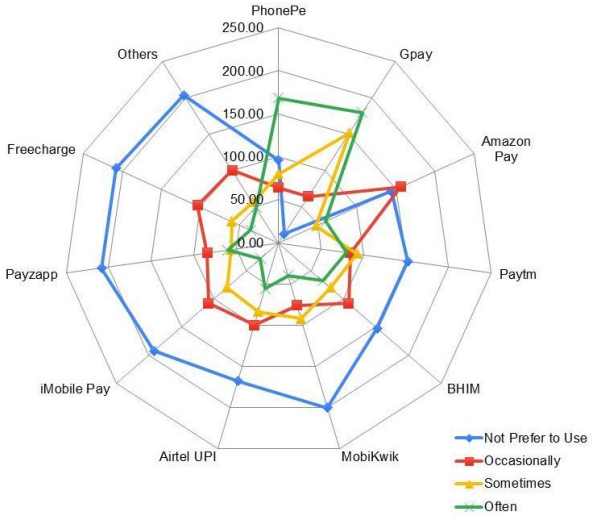

Fig. 1: UPI Apps Preference in Making Transaction

The frequency table presents the preferences for using UPI apps in making transactions. It provides insights into the percentage distribution of responses across different categories: "Not Preferred to Use," "Occasionally," "Sometimes," and "Often." Among the UPI apps mentioned, PhonePe is widely used, with 41.18% of respondents using it often. Gpay also enjoys popularity, with 44.12% of respondents using it often. In contrast, Amazon Pay is not preferred by a significant portion of respondents (35.29%), while Paytm and BHIM have a similar percentage of respondents who do not prefer to use them (37.25%). MobiKwik, Airtel UPI, iMobile Pay, Payzapp, and Freecharge face higher resistance, as more than 40% of respondents do not prefer to use them. Interestingly, a significant proportion of respondents (50.98%) do not prefer to use Payzapp and Freecharge. Similarly, more than half of the respondents (50.00%) do not prefer the "Others" category of UPI apps. Overall, the frequency table provides a comprehensive overview of the preferences for different UPI apps and highlights the varying levels of usage and acceptance among respondents. It offers valuable insights into the popularity and adoption of these apps in facilitating online transactions.

Variables	No of Items	Descriptive Statistics						Tests of Normality		Reliability
		Mean		Std. Deviation	Variance	Skewness	Kurtosis	Kolmogorov-Smirnov[a]	Shapiro-Wilk	
		Statistic	Std. Error	Statistic	Statistic	Statistic(SE = 0.121)	Statistic(SE = 0.241)	Statistic (df =408)	Statistic (df =408)	
Digital Banking Security Measures	10	3.837	0.033	0.663	0.439	-0.121	-1.006	0.107**	0.960**	0.822
User Experience and Digital Banking Security	7	3.815	0.035	0.702	0.493	0.077	-1.069	0.105**	0.952**	0.775
Enhancing Online Transaction Security in Digital Banking	6	3.632	0.042	0.846	0.717	-0.646	0.329	0.119**	0.953**	0.833
Assessing Vulnerabilities	9	3.548	0.044	0.888	0.789	-0.268	-0.108	0.074**	0.970**	0.869
Safeguarding Digital Banking Apps	9	3.417	0.041	0.830	0.689	-0.455	0.355	0.092**	0.972**	0.873
a. Lilliefors Significance Correction										

Table 3: Descriptive Statistics

The table presents the descriptive statistics, tests of normality, and reliability statistics for different variables related to digital banking empowerment and safeguarding online transactions from fraudulent activities. For each variable, the table provides the mean, standard deviation, variance, skewness, and kurtosis. The mean values range from 3.417 to 3.837, indicating the average response for each variable. The standard deviation values range from 0.033 to 0.044, indicating the variability or dispersion of responses around the mean. The variance values range from 0.663 to 0.888, representing the average squared deviation from the mean. The skewness values indicate the degree of asymmetry in the distribution. All variables have positive skewness values, ranging from 0.077 to 0.717, suggesting a slightly right-skewed distribution. The kurtosis values represent the degree of peakedness or flatness of the distribution. The values range from -1.069 to 0.789, indicating varying levels of peakedness. The normality tests are conducted using the Kolmogorov-Smirnov test and the Shapiro-Wilk test. The p-values for both tests are denoted as "**" in the table, indicating statistical significance. Therefore, the assumption of normality is violated for all variables. The reliability statistics are measured using Cronbach's alpha, which assesses the internal consistency of the items within each variable. The Cronbach's alpha values range from 0.775 to 0.873, indicating good to excellent reliability. In summary, the variables related to digital banking empowerment and security measures show slightly right-skewed distributions and varying levels of peakedness. The assumption of normality is violated for all variables. However, the variables demonstrate good to excellent internal consistency reliability based on Cronbach's alpha values.

The regression analysis aims to determine the factors that influence the usage and mitigation of online transaction frauds in digital banking. The dependent variable in this analysis is "Digital Banking Security Measures," while the independent variables include "User Experience and Digital Banking Security," "Assessing Vulnerabilities," "Enhancing Online Transaction Security in Digital Banking," and "Safeguarding Digital Banking Apps."

Variables	No of Items	R	R Square	Adjusted R Square	Std. Error of the Estimate	ANOVA			Durbin-Watson	Unstandardized Coefficients		Standardized Coefficients	t-Value (Sig.)	Collinearity Statistics	
						F-Value	df	Sig.		B	Std. Error	Beta		Tolerance	VIF
Dependent Variable															
Digital Banking Security Measures	10	0.734	0.538	0.535	0.452	156.9847	3,404	0	1.625	***					

Independent Variables								
(Constant)			0.761	0.144	5.268 (0.000)**			
User Experience and Digital Banking Security	7		0.523	0.035	0.554	15.155 (0.000)**	0.855	1.170
Assessing Vulnerabilities	9		0.210	0.027	0.281	7.694 (0.000)**	0.856	1.168
Enhancing Online Transaction Security in Digital Banking	6		0.093	0.030	0.118	3.069 (0.002)**	0.769	1.301
Safeguarding Digital Banking Apps	9		.037[d]	0.878	0.380	0.044 (0.634)	1.576	0.586
a. Dependent Variable: Digital Banking Security Measures								
d. Predictors in the Model: (Constant), User Experience and Digital Banking Security, Assessing Vulnerabilities, Enhancing Online Transaction Security in Digital Banking, Safeguarding Digital Banking Apps								

Table 4: Determinants of Usage and Mitigation Online Transaction Frauds (Regression)

The results show that the regression model has a moderate level of explanatory power, as indicated by the coefficient of determination (R-square) of 0.538. This means that approximately 53.8% of the variability in the dependent variable can be explained by the independent variables included in the model. The adjusted R-square, which takes into account the number of predictors in the model, is 0.535. The analysis also indicates that the overall model is statistically significant, as evidenced by the significant F-value of 156.9847 ($p < 0.001$). This suggests that at least one of the independent variables has a significant relationship with the dependent variable.

Examining the individual independent variables, the "User Experience and Digital Banking Security" variable has a significant positive impact on "Digital Banking Security Measures" ($p < 0.001$). This indicates that as the user experience and security in digital banking improve, the adoption of digital banking security measures also increases. Similarly, "Assessing Vulnerabilities" and "Enhancing Online Transaction Security in Digital Banking" have significant positive effects on "Digital Banking Security Measures" ($p < 0.001$). This implies that assessing vulnerabilities and enhancing online transaction security are important factors in promoting the implementation of security measures in digital banking.

However, the variable "Safeguarding Digital Banking Apps" does not have a significant effect on "Digital Banking Security Measures" ($p = 0.634$), suggesting that safeguarding digital banking apps may not be a strong determinant of security measures adoption in this analysis.

Overall, the results of the regression analysis provide insights into the factors that contribute to the usage and mitigation of online transaction frauds in digital banking. They highlight the importance of user experience, assessing vulnerabilities, and enhancing transaction security in promoting the adoption of digital banking security measures. The regression results provide several unique implications for enhancing digital banking security measures and mitigating online transaction frauds. Firstly, it is crucial for banks to prioritize user experience, as improving the user interface and simplifying processes can encourage customers to prioritize security measures. Secondly, regular vulnerability assessments should be conducted to identify and address any weaknesses in digital banking systems. Thirdly, banks should continuously enhance online transaction security through measures like two-factor authentication and fraud detection systems. Additionally, while safeguarding digital banking apps did not show a significant impact, it is important for banks to evaluate and strengthen app security regularly. Lastly, continuous monitoring and adaptation are essential to stay proactive in addressing

emerging threats. By considering these implications, banks can enhance security, protect customer data, and foster trust in the digital banking ecosystem.

Suggestions

- To encourage customers to use online banking and other digital platforms for banking services, the Reserve Bank of India (RBI) and Government of India (GOI) should take into consideration, adopt, and execute the model for online banking fraud prevention measures.
- Bank employees should educate their clients about the many sorts of internet banking scams using examples and demonstrations to help them avoid fraudulent transactions and financial loss.
- In accordance with client needs and capabilities, banks should enhance their policies relating to threshold values and transaction limits for online banking, and they should also assume liability for unauthorised online transactions.
- To increase client acceptance and adoption of online banking transactions in their daily life, banks should concentrate on protection, prevention, privacy, safety, and security measures.
- To increase the usage and adoption of online banking transactions in India, banks should enhance their services by offering sufficient connectivity, design, maintenance, technology, and convenience elements.

Conclusion

Fraudsters have always targeted banking and financial institutions due to the nature of their business. However, the introduction of technology in banking services has made these institutions even more susceptible to fraud threats. Over the past decade, there has been a significant increase in reported fraud incidents, especially since the demonetization in 2017 and the onset of the Covid-19 pandemic, as evident from data published by RBI and NCRB. This surge is primarily attributed to the growing reliance on electronic banking services, which have been found to carry higher security risks compared to traditional banking methods. The aim of this study is to examine the adoption of digital banking and its role in mitigating online transaction fraud in India. The study focuses on various factors such as perceived benefits, internal and external attacks on apps, and the ease of app usage, all of which contribute to reducing fraud in digital banking within India. By shedding light on these aspects, this study emphasizes the need for the banking industry to set comprehensive goals to combat fraud in India, promoting a cashless economy through the nation's digital transformation while ensuring freedom from fraudulent activities.

Reference

Ali, L. Ali, F. Surendran, P. and Thomas, B. (2017) “The Effects of Cyber Threats on Customer’s Behaviour in e-Banking Services”, *International Journal of e-Education, e-Business, eManagement and e-Learning,* 7(1).

Ali, M. A., Hussin, N., & Abed, I. A. (2019). E-banking fraud detection: a short review. *Int. J. Innov. Creat. Chang*, *6*(8), 67-87.

Bharatial, A. B. and Alim, A. K. (2016) Legal control of cyber crimes against ebanking in India.

Chandrika, G. D. P and Aggarwala, A. C. (2018) E- Banking Frauds a Critical Study of the Legislative Meausres.

Goel, S. (2016) “Cyber-Crime: A Growing Threat to Indian Banking Sector”, *International Journal of Science Technology and management,* .5(12).

Hoskote, L. S. (1996) “Crime and Security in Electronic Banking”, *CBI Bulletin*, 4

https://www.inform-software.com/riskshield/online-and-mobile-banking-fraud-prevention

Karishma, B. and Soni, H (2016) “Indian Banking Sector: Then, Now & the Road Ahead”, *International Research Journal of Engineering and Technology (IRJET),* 3(4).

Khanna, A. and Arora, B. (2009) “A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry” *International Journal of Business Science and Applied Management,* 4(3).

Lal, R. and Saluja, R. (2012) “E-Banking: The Indian Scenario”, *Asia Pacific Journal of Marketing & Management Review*, 1(4).

Monica, Y., Bhatt, Kumar, A and Singh, S. K. (2022) Frauds in the Banking Sector a Detailed Study of Insider Risks in E-Banking and Legislative Framework in India.

Palchenla, S. and Nidhi, S. (2022) Legal and regulatory issues of cyber fraud in transnational banking with special reference to European Union.

Ranjith, P. V., Kulkarni, S., & Varma, A. J. (2021). A Literature Study Of Consumer Perception Towards Digital Payment Mode In India. *PSYCHOLOGY AND EDUCATION*, *58*(1), 3304-3319.

Shree, S. and Gurusamy, s. (2021) Online Banking Frauds A Study woth reference to Perception of Bank Customers.

Yazdanifard, R., WanYusoff, W. F., Behora, A. C., & Sade, A. B. (2011). Electronic banking fraud: The need to enhance security and customer trust in online banking. *Advances in Information Sciences and Service Sciences*, *3*(10), 505-509.

Zahoor, Z. MoinUd-din and Karuna, (2016) "Challenges in Privacy and Security in Banking Sector and Related Countermeasures", *International Journal of Computer Applications*, 144(3)

