JOURNAL: PRIMAX INTERNATIONAL JOURNAL OF COMMERCE AND MANAGEMENT RESEARCH
ISSN: Print ISSN: 2321-3604 Online ISSN: 2321-3612, Impact Factor: 7.184
(A DOUBLE-BLIND PEER REVIEWED, OPEN ACCESS REFEREED QUARTERLY JOURNAL)
PRIMAX IJCMR VOLUME NO.13, ISSUE NO-1, APRIL – JUNE, 2025
Research Article

A STUDY ON DIGITAL BANKING SECURITY CHALLENGES: LEVERAGING AWARENESS AS A SHIELD AGAINST FRAUD

Anusha H.G*
Lecturer, Department of Commerce
Sri J.C.B.M College, Sringeri

***Corresponding author | Received: 01/03/2025 | Accepted: 15/04/2025 | Published: 30/04/2025**

Abstract

Digital banking is the practice of conducting financial transactions and providing services online through the technologies in digital platforms. It provides convenience by allowing customers to access banking services at any time and any location. Customers can manage accounts, invest and transfer money. Traditional banking has undergone an evolution because of digital banking, which makes it convenient and accessible to people all over the world. However, it also comes with new hazards. A crucial strategy to mitigate these security issues is effectively utilizing awareness as a shield against fraud. Educating users about possible risks and secure banking procedures can considerably decrease the threat. This strategy gives customers the ability to identify fraud activities and take preventative action to safeguard their financial assets. These awareness programs can encourage users to adopt safer online banking practices. This study aims to evaluate the level of awareness among digital banking users regarding cyber threats and to identify the primary security challenges digital banking systems face in the current technological landscape. It also analyses the role of emerging technologies in strengthening digital banking. This study is based on primary data collection, with additional internet-based information. This analysis employs quantitative methods that focus on digital banking and identify the key security challenges faced by digital banking systems. This study emphasizes the role of customer education in mitigating digital banking fraud. Leveraging user awareness as a proactive shield is essential in combating these risks effectively. Both users and financial organizations could reduce threats by strengthening customer education and encouraging safe banking transactions. Ultimately, fostering a culture of awareness is key to safeguarding the integrity and trust of digital banking systems.

Keywords: Traditional banking, investing, financial assets, Technologies.

Introduction

The banking sector has undergone an evolution attributable to digital banking, which offers consumers across the world quick, easy, and effective services. Digital banking systems with recent updates have resulted in increased use of artificial intelligence for personalized services; improved security with biometric authentication; streamlined online account opening; blockchain integration for secure transactions; adoption of robo-advisors for automated investment advice; and the creation of "one-stop shop" platforms that offer comprehensive financial services through a single app.There are serious security risks associated with the quick digitization of banking activities, such as identity theft, data breaches, cyber threats, phishing scams, account hijacking, and fraudulent transactions. These issues erode confidence in digital banking systems in addition to endangering consumers' financial security.

To reduce these hazards and protect consumers from possible fraud, it is essential to be aware of digital security procedures. Digital banking has emerged as an essential element of the modern period. It provides financial transactions with outstanding efficiency and convenience. However, providing a secure and reliable digital banking experience requires resolving security issues and raising user knowledge.

Objective of the study

1. To assess the extent of digital transformations in banking and their role in enhancing customer convenience through streamlined services.
2. To evaluate the level of awareness among digital banking users regarding cyber threats and fraud prevention.
3. To identify the primary security challenge of digital banking services in current technological landscape.
4. To analyses the role of emerging technologies in strengthening digital banking.

Literature Review

"A Study on the Customer Awareness of Security Issues and Threats in Digital Banking in Chennai", Dr. Sankararaman, Dr. Suresh S, Dr. Thirumagal PG, Priyadharshini V and Dr. Rengarajan (2024) - This study focuses on the way programs like 'Digital India,' which encourage cashless transactions, have fuelled the swift expansion of digital banking in India. It draws attention to the security issues the industry is facing as it moves from traditional to digital banking. To improve security in digital banking, the study investigates new cyber threats, weaknesses, and regulatory actions. Ultimately, it seeks to improve every individual's dependability and security of digital financial systems.

Instances of Digital Banking Security Fraud- In India, digital fraud has increased in recent years.

1. Account Takeover Frauds: Using malware or phishing attacks, fraudsters obtained unauthorized access to victim's bank accounts and carried out illegal transactions.
2. Digital Arrest Scams: Using online platforms, scammers posed and accused, forced the victims of money laundering. They force people to transfer money to evade false lawsuits.
3. SIM Swap Frauds: To gain unauthorized access to bank accounts, attackers copied a victim's SIM card and intercepted banking notifications and one-time passwords.
4. Phishing and Vishing Attacks: Scammers used deceptive emails (phishing) or phone calls (vishing) to trick individuals into revealing sensitive banking information, leading to unauthorized transactions.

5. Ghost Tap Scams: Cybercriminals used these scams to duplicate digital payment methods connected to mobile devices without having physical access. In the fiscal year 2024, the losses resulting from cyber fraud activity in India reached a record high of over 1.7 billion Indian rupees. These were specifically linked to fraud involving credit cards, debit cards, and online banking. With over 740,000 cases registered between January and April 2024 cybercrime in India has increased at an alarming rate.

Scope of the study

This study is intended to examine the security issues with online banking and the vital role that user awareness plays in hindering fraud. The study emphasizes how educated individuals can serve as a barrier against cybercrime by analyzing current potential hazards.

Limitations of the study

1. The study may be impacted by discrepancies in information availability, especially in rural least technologically advanced locations.
2. The study's insights could be soon rendered obsolete by continuing technology developments and shifting fraud strategies due to the rapid way of digital banking security measures are evolving.

Research Methodology

The research aims to assess "A Study on Digital Banking Security Challenges: Leveraging Awareness as a Shield Against Fraud". To evaluate the extent of digital banking and its security challenges in the Chikkmagaluru region, the present circumstance is being examined by gathering the opinions of locals and students. A closed-ended questionnaire is used to get the opinions of the individuals.

Data collection

The primary data was collected using a well-written questionnaires. A sample of 110 respondents was selected for the research. A realistic sampling technique was used in the study to effectively collect data from the chosen participants. Cross tabulation and Chi-Square analysis were used in the study, together with an estimate of Cronbach's alpha value, to determine the questionnaire's reliability.

Testing of the Data Using Chi-Square Hypothesis Testing Reliability Statistics

Reliability Statistics

Cronbach's Alpha	N of Items
.899	7

Cronbach's Alpha reliability test was conducted on the data collected from primary sources of the questionnaire has produced a value of 0.899, indicating excellent internal consistency and demonstrating the instrument's high reliability for measuring the intended construct. Good dependability implies that the survey's questions accurately reflect respondents' knowledge and opinions about the security risks associated with digital banking as well as fraud prevention techniques. It proves that the questions were consistently comprehended by the respondents, offering reliable data for research. The survey concludes that respondents have accurately identified significant areas of security challenges and assessed awareness levels which was supported by excellent reliability.

Testing between frequent usage of digital banking services and reason for the frequent use of services based on features.

1. How often do you use digital banking services? * 2. What do you consider the most important feature of digital banking? Crosstabulation

Count

		2. What do you consider the most important feature of digital banking?					
		1	Convenience and accessibility	Customer support	Security measures	Speed of transactions	Total
1. How often do you use digital banking services?	1	2	0	0	0	0	2
	Daily	0	18	4	6	40	68
	Option	0	2	0	0	2	4
	Rarely	0	2	2	0	2	6
	Weekly	0	8	2	8	12	30
Total		2	30	8	14	56	110

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	125.482[a]	16	<.001
Likelihood Ratio	33.311	16	.007
Linear-by-Linear Association	.067	1	.795
N of Valid Cases	110		

We assumed that H_0 (Null Hypothesis) as there is no significant relationship between the frequency of digital banking services and the most important features of digital banking (convenience and accessibility, customer support, security measures, or speed of transactions) and H_1 (Alternative Hypothesis) as there is a significant relationship between the frequency of using digital banking services and the most important feature of digital banking.Interpretation of Chi-Square Test Results: Chi-Square Value during the study - 125.482, Degrees of Freedom/df = 16, p-value = 0.001. So the study concludes that since the p-value (0.001) is

less than 0.05, we failed to accept the null hypothesis (H_0), hence H_1 is accepted. This indicates a significant relationship between the frequency of digital banking services and the most important feature of digital banking.

Testing between the services of digital banking with the characteristics made to utilize digital banking services.

3. Which of the following digital banking services do you use most frequently? * 2. What do you consider the most important feature of digital banking? Crosstabulation

Count

		2. What do you consider the most important feature of digital banking?				
		Convenience and accessibility	Customer support	Security measures	Speed of transactions	Total
3. Which of the following digital banking services do you use most frequently?	Bill payments	8	0	10	10	28
	Bill payments, Checking account balances	0	0	2	2	4
	Bill payments, Investment and savings management	0	0	0	2	2
	Checking account balances	2	0	0	8	10
	Fund transfers	14	4	2	18	38
	Fund transfers, Bill payments	0	0	0	6	6
	Fund transfers, Bill payments, Checking account balances	6	0	0	2	8
	Fund transfers, Bill payments, Investment and savings management	0	0	0	4	4
	Fund transfers, Checking account balances	0	2	0	0	2
	Fund transfers, Checking account balances, Investment and savings management	0	0	0	2	2
	Fund transfers, Investment and savings management	0	4	0	2	6
Total		30	10	14	56	110

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	96.061[a]	30	<.001
Likelihood Ratio	81.185	30	<.001
Linear-by-Linear Association	.049	1	.825
N of Valid Cases	110		

We assumed that H_0 (Null Hypothesis) as there is no association between the most frequently used digital banking services and the perceived most important feature of digital banking and H_1 (Alternative Hypothesis) as there is an association between the most frequently used digital banking services and the perceived most important feature of digital banking.

Interpretation of Chi-Square Test Results: Chi-Square Value during the study - 96.061, Degrees of Freedom/df - 30, p-value = < .001. So, the study concluded that since the p-value (0.001) is less than 0.05, we failed to accept the null hypothesis (H_0). This indicates strong evidence against the null hypothesis. Hence H_1 is accepted. There is a statistically significant association between the most frequently used digital banking services and the perceived most important feature of digital banking. The data suggests that people's preferences for different digital banking services are not randomly distributed across the different perceived important features of these services.

Testing the assessment of awareness and experience with issues in digital banking services

9.Have you experienced or heard of the following issues in digital banking systems? * 10. If YES, Have you experienced or heard of the following issues in digital banking systems? (Select the one you perceive as most critical) Crosstabulation

Count

		10. If YES, Have you experienced or heard of the following issues in digital banking systems? (Select the one you perceive as most critical)									
		1	Data breaches exposing sensitive information	Data breaches exposing sensitive information, Difficulty in resolving issues	Difficulty in resolving issues	Fraudulent transactions or identity theft	Fraudulent transactions or identity theft, Data breaches exposing sensitive information	Unauthorized access to accounts	Unauthorized access to accounts, Data breaches exposing sensitive information	Unauthorized access to accounts, Fraudulent transactions or identity theft	Total
9.Have you experienced or heard of the following issues in digital banking systems?	No	14	4	2	4	4	0	4	0	0	32
	Yes	0	8	2	18	20	2	20	2	6	78
Total		14	12	4	22	24	2	24	2	6	110

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	44.041[a]	8	<.001
Likelihood Ratio	47.714	8	<.001
Linear-by-Linear Association	26.410	1	<.001
N of Valid Cases	110		

We assumed the Null Hypothesis (H_0) as there is no significant relationship between whether individuals have experienced or heard of digital banking issues and their perception of the most critical digital banking issues and the Alternative Hypothesis (H_1) as there is a significant relationship between whether individuals have experienced or heard of digital banking issues and their perception of the most critical digital banking issues.

Interpretation of Chi-Square Test Results: Pearson Chi-Square Value: 44.041, Degrees of Freedom /df – 8. The p-value (< 0.001) is much lower than 0.05. we failed to accept the null hypothesis (H_0), hence H_1 is accepted. Hence it can be concluded that there is a statistically significant relationship between whether individuals have experienced or heard of digital banking issues. This indicates that personal experience or awareness of digital banking issues influences the perception of which issue is most critical.

Testing the assessment of the most impactful emerging technology on strengthening the digital banking and its association with the frequently used digital banking services.

5. Which emerging technology do you think has the most significant impact as a boon on strengthening digital banking security? * 3. Which of the following digital banking services do you use most frequently? Crosstabulation

Count

		3. Which of the following digital banking services do you use most frequently?											
		Bill payments	Bill payments, Checking account balances	Bill payments, Investment and savings management	Checking account balances	Fund transfers	Fund transfers, Bill payments	Fund transfers, Bill payments, Checking account balances	Fund transfers, Bill payments, Investment and savings management	Fund transfers, Checking account balances	Fund transfers, Checking account balances, Investment and savings management	Fund transfers, Investment and savings management	Total
5. Which emerging technology do you think has the most significant impact as a boon on strengthening digital banking security?	1	0	0	0	0	2	2	0	0	0	0	0	4
	Artificial Intelligence (AI) for fraud detection	18	0	2	2	20	2	4	2	2	2	2	56
	Biometric authentication (e.g., facial or fingerprint recognition)	10	4	0	6	6	0	2	2	0	0	0	30
	Blockchain for secure transactions	0	0	0	2	4	2	2	0	0	0	0	10
	Cloud computing for data storage and scalability	0	0	0	0	6	0	0	0	0	0	4	10
Total		28	4	2	10	38	6	8	4	2	2	6	110

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	87.273[a]	40	<.001
Likelihood Ratio	77.733	40	<.001
Linear-by-Linear Association	4.785	1	.029
N of Valid Cases	110		

We have assumed the Null Hypothesis (H_0) as there is no association between the perceived most significant emerging technology for strengthening digital banking security and the most frequently used digital banking service. Alternative Hypothesis (H_1) as there is an association between perceived most significant emerging technology for strengthening digital banking security and most frequently used digital banking service.

Interpretation of Chi-Square Test Results: Chi-Square Value: 87.273, Degrees of Freedom /df - 40, P-value: <0.001. Since the p-value (<0.001) is much smaller than the commonly used significance level of 0.05, we failed to accept the null hypothesis (H_0), hence (H_1) is accepted. This means that there is strong evidence to conclude that there is a statistically significant association between the perceived most significant emerging technology for strengthening digital banking security and the most frequently used digital banking service. The data suggests that people's views on this emerging technology are most important for enhancing security which is related to the digital banking services they use most often.

Analysing And Interpretation of Data with Data Visualisation

Emerging technology in the banking sector has a most significant impact as a boon on strengthening the digital banking sector, respondents prefer AI as an emerging technology. It can control E-banking fraud and threats, and its algorithms adapt to threats, enabling proactive fraud prevention, by analyzing vast transaction data in real time and identifying anomalies and suspicious activities

The biggest security challenges for the digital banking system

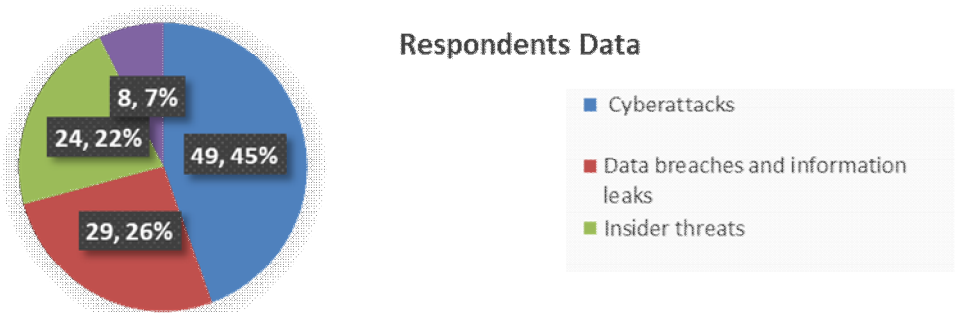

Figure i The chart represents the biggest security challenges for digital banking services.

In the study, most of the respondents believe that Cyberattacks (e.g., phishing, malware) are identified as the biggest security challenge for digital banking systems, with 45% of respondents highlighting this issue. Data breaches and information leaks (26%) and insider threats (22.2%) are also major concerns. Weak user authentication systems (7.4%) are considered the least significant challenge.

The measures that the digital banking system should prioritize the enhanced security to reduce digital banking frauds and cyber threats

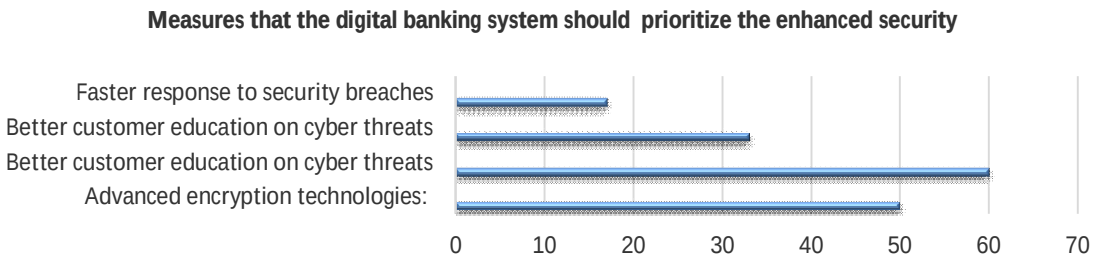

Figure ii The chart represents measures that should be prioritized to enhance security to reduce digital fraud threats

In the study, most of the respondents believe that better customer education on cyber threats is the top priority for enhancing digital banking security. Advanced encryption technologies and stronger multi-factor authentication methods were also significant preferences as measures that digital banking adopts.

Finding of the Study

1. In the study, most consumers make use of digital banking services daily, underscoring its significance in everyday financial tasks. Usage that occurs once a week or less suggests varying reliance according to user demands.
2. The study reveals that many respondents believe that the most crucial aspects are thought to be accessibility and convenience, which are the main characteristics of digital transactions then security precautions. Transaction speed and customer service are not given as much priority.
3. During the study, the most frequently used services are fund transfers, which are followed by bill payments. Less frequently used services include investment management and account balance checking.
4. The main aspect of the study is to identify the primary challenges in Digital Banking, where respondents find that the largest obstacle is the possibility of fraud or illegal access, which is followed by technical difficulties or system outages. Lack of awareness and personalization are small issues.

5. The study reveals that the most significant emerging technology under digitalized banking transactions is security which acts as a shield against fraud the technological advancement for enhancing security is thought to be artificial intelligence. Biometrics and blockchain are also useful, although cloud computing is comparatively less significant.
6. The respondents think that improving the security of digital banking requires educating customers about cyber threats. Biometric, advanced encryption technologies are also seen as significant security improvements, strengthening multi-factor authentication techniques less important.
7. From the study it finds that most respondents have not experienced the problems, but they heard cybercrime and digital banking fraud as unauthorized account access is cited as a top concern by people who have encountered problems. Identity theft and fraudulent transactions also account for a significant percentage of serious problems. Another major obstacle that users have is data breaches.

Suggestions From the Study

Banks should prioritize offering excellent daily-use services that emphasize easy accessibility and convenience while maintaining strict safety standards to increase the productivity of digital banking. Significant security issues can be resolved by implementing advanced encryption technologies like blockchain and boosting fraud detection systems with artificial intelligence. Frequent consumer education regarding system features and related hazards will raise awareness and decrease fraud. The findings will enhance user understanding which indicates a focused awareness campaign as a defence against fraud in online banking systems. Enhancing system performance and downtime can also reduce technical problems and guarantee an excellent user experience.

Customers are satisfied with increased tailored services in addition to convenient choices for bill payment and fund transfers. For frequent users, investing in biometric authentication will also provide an additional degree of security. Users should always use strong, unique passwords and enable two-factor authentication to protect themselves from online banking scams. Avoid disclosing personal information through unprotected channels and be constantly aware of being protected from phishing efforts.

Conclusion

In conclusion, protecting personal financial information requires a thorough understanding of security issues as digital banking develops. To remain alert, users should change their passwords frequently, enable two-factor authentication, and keep an eye out for any unusual activity on their accounts. One must have the proper knowledge to stay alert and protected from digital financial crimes, educating people on how to spot phishing efforts and stay away from unprotected networks can significantly lower the possibility of fraud.

Utilizing safe, reliable hardware and software is also crucial, as is being aware of the most recent risks. Assessing bank information regularly regarding security evolves and fraud prevention strategies also contributes to protection. When it comes to preventing digital financial fraud, the strongest protection is knowledge and initiative.

References

1. Dr. Sankararaman G “A Study on the Customer Awareness on Security Issues and Threats in Digital Banking in Chennai”- European Economic Letters ISSN 2323-5233 Vol 14, Issue 4 (2024) - https://www.eelet.org.uk/index.php/journal/article/download/2179/1957/2388
2. The cyber fraud in India in fiscal year 2024 - https://www.statista.com/statistics/1499770/india-cyber-fraud-losses/#statisticContainer
3. The Digital banking frauds - https://www.aubank.in/blogs/8-different-types-of-digital-banking-frauds?utm_source