www.ijarp.com ISSN 2456-9992 Page: 01-08
International Journal Advanced Research Publications
Review Article
Volume: 02
Issue: 05

FRAUDULENT ACTIVITIES ON ONLINE BANKING (CHENNAI)

*[1]Nila K. B., [2]Dr. S. Thirumal

[1]Com.LLB(Hons),The Tamilnadu Dr. Ambedkar Law University,SOEL,Chennai 600113.

2Assistant Pofessor of Commerce, The Tamilnadu Dr. Ambedkar Law University, SOEL, Chennai 600113.

Article Received: 31 March 2026, Article Revised: 21 April 2026, Published on: 11 May 2026

***Corresponding Author: Nila K. B.**

Com.LLB(Hons),The Tamilnadu Dr. Ambedkar Law University,SOEL,Chennai 600113.

DOI: https://doi-doi.org/101555/ijarp.4831

ABSTRACT

Online banking has significantly transformed the banking sector by enabling faster transactions, ease of access, and improved customer convenience. However, the rapid growth of digital banking services has also led to an increase in fraudulent activities, cyber threats, and system-related risks affecting both banks and users. This research paper focuses on fraudulent practices in online banking, with special reference to Chennai. The study evaluates customer awareness, common security threats, operational challenges faced by banks, and the effectiveness of existing regulatory measures. Using primary data, relevant academic sources, and a comparative review of international practices such as fraud control mechanisms implemented in Thailand, the paper identifies weaknesses in the current security framework. The study ultimately proposes measures to strengthen fraud prevention systems, enhance customer education, and improve trust and efficiency in online banking services.

KEYWORDS: Online Banking, Cyber Fraud, Digital Security and Financial Crime.

INTRODUCTION

The banking sector has undergone a major shift due to advancements in information technology and the development of digital infrastructure. One of the most notable outcomes of this transformation is the emergence of online banking, also known as internet or electronic banking. Online banking allows customers to perform a wide range of financial activities—such as transferring funds, paying bills, checking account balances, applying for loans, and managing investments—without visiting a bank branch. This shift has greatly enhanced customer convenience and improved the efficiency of banking operations.

In India, the expansion of online banking has been supported by increased internet access, widespread use of smartphones, and government-led initiatives encouraging digital payments. The introduction of systems like the Unified Payments Interface (UPI), mobile banking platforms, and web-based financial services has resulted in a substantial rise in digital transactions. The growing transaction volume reflects the increasing acceptance of online banking among Indian users.

The COVID-19 pandemic further accelerated this digital transition. Restrictions on physical movement and social distancing measures compelled customers to depend heavily on online platforms for banking needs. In response, banks expanded their digital services to include online account opening, digital lending, and remote investment services. While these developments improved accessibility and financial inclusion, they also introduced new security and operational risks.

A major concern associated with online banking is the increasing incidence of fraud. Cyber offenders use methods such as phishing scams, malicious software, identity misuse, and unauthorised account access to exploit technological weaknesses and customer ignorance. Such fraudulent activities lead to financial losses and seriously undermine public confidence in digital banking systems.

Apart from security-related threats, customers also face technical problems such as transaction failures, system downtime, delayed processing, and ineffective grievance redressal mechanisms. Although automation has improved speed and efficiency, limited human involvement in resolving complex issues often results in dissatisfaction among users. As a result, ensuring secure, reliable, and trustworthy online banking services has become aey priority for both banks and regulatory authorities.

This study examines fraudulent activities in online banking with specific reference to Chennai. It analyses customer perceptions, challenges faced by banking institutions, and the role of regulatory bodies in addressing online fraud. By incorporating both Indian and international perspectives, including fraud control measures adopted in countries like Thailand, the study aims to offer practical insights for strengthening online banking security in India.

Review of Literature

Haq and Khan (2013), in Internet Banking in India, examined the early stages of online banking adoption among Indian consumers. Their research indicated that factors such as

education and income significantly influenced usage. The study found that limited awareness and fear of fraud discouraged customers from adopting internet banking, highlighting the importance of financial education in reducing fraud-related risks.

Chauhan and Chaudhary (2015), in their article Internet Banking in India: Challenges and Opportunities, analysed the rapid growth of online and mobile banking services. While customers valued the convenience offered by digital platforms, concerns regarding security, privacy, and system reliability continued to affect trust. The authors emphasised the need for strong fraud prevention mechanisms and transparent security practices.

Manikyam (2014), in Banking Reforms in India, explored the effects of economic reforms on the Indian banking sector. The study noted that technological advancements enhanced efficiency and competition but also introduced new cyber and operational risks. The author stressed the necessity for continuous technological upgrades to address emerging fraud threats.

Seranmadevi (2012), in E-Banking Services in India, studied the accessibility of electronic banking services and observed that customers were reluctant to rely entirely on digital platforms due to concerns about fraud and misuse of personal data. The study concluded that improving customer awareness and strengthening security systems are essential for increasing trust in e-banking.

Driga and Isac (2014), in their work E-Banking Services – Features, Challenges and Benefits, examined global trends in electronic banking. Their research identified cyber fraud, identity theft, and system vulnerabilities as significant threats to online banking stability. The authors highlighted the role of regulatory supervision and advanced fraud detection technologies in managing these risks.

Research Gap

Although existing studies have extensively examined the growth and adoption of online banking, there is limited research focusing specifically on fraudulent activities and technical challenges at the city level in India. Empirical studies analysing customer perceptions of online fraud and institutional responses in metropolitan areas such as Chennai are scarce. Furthermore, comparative evaluations of international fraud prevention models, particularly those implemented in countries like Thailand, have not been sufficiently explored in Indian academic literature. This study seeks to fill these gaps by providing a focused and comparative analysis.

Statement of the Problem

The growing reliance on online banking services has been accompanied by a noticeable increase in cyber fraud and security-related incidents. Customers are frequently exposed to risks such as phishing scams, unauthorised fund transfers, and misuse of personal data, which weaken confidence in digital banking systems. In addition to security threats, technical problems like failed transactions, delayed processing, and ineffective grievance redressal mechanisms further contribute to customer dissatisfaction. Although regulatory authorities have introduced various measures to control online fraud, the continued rise in such incidents suggests shortcomings in existing security frameworks and limited user awareness. Addressing these concerns is essential to ensure the safe, reliable, and sustainable expansion of online banking services.

Objectives of the Study

1. To examine the key security risks involved in the use of online banking services.
2. To assess customer perceptions regarding the safety and reliability of online banking.
3. To recommend effective measures for minimising fraudulent activities in online banking systems.

RESEARCH METHODOLOGY

The research adopts both primary and secondary data sources. Primary data were collected through a structured questionnaire administered to 100 respondents residing in Chennai City. Secondary data were obtained from academic books, research journals, reports published by the Reserve Bank of India, National Crime Records Bureau statistics, and other relevant government publications. The collected data were analysed using percentage analysis for quantitative interpretation. In addition, qualitative methods were applied to study regulatory frameworks, policy measures, and selected case studies related to online banking fraud.

RESULTS AND DISCUSSION

Table 1: Socio-Economic Profile of Respondents.

S. No	Particular	Category	Number	Percentage
		Below 18	33	33
1.	Age	18-25	40	40
		More than 25 Years	27	27
		Total	100	100
		Male	37	37
2.	Gender	Female	63	63
		Total	100	100

		High school	13	13
3.	Occupation	Undergraduate	20	20
		Postgraduate	40	40
		Employee	27	27
		Total	100	100

Source: primary data

The table indicates that most respondents fall within the 18–25 age group, showing greater acceptance of online banking among young users. Participation decreases with increasing age, suggesting a digital gap among older individuals. Female respondents form a larger share of the sample, reflecting their growing involvement in digital financial activities. Educational status plays a key role, as postgraduates represent the highest proportion of users. Undergraduates and employees also contribute significantly, indicating regular use for academic and professional needs. School students account for a smaller share, yet their presence reflects early exposure to online banking. Occupational diversity shows wide adoption across social groups. Overall, demographic factors strongly influence online banking usage patterns.

Table 2: People's Perception Towards Online Banking Security

Statement	Agree	%	Neutral	%	Disagree	%	Total
Online banking is a secure mode of transaction	35	35	50	50	15	15	100
Banks compensate customers for losses due to online fraud	15	15	25	25	60	60	100
Incidents of online money theft are increasing	45	45	37	37	18	18	100
Online banking is more convenient than traditional banking	60	60	20	20	20	20	100
Customers are aware of phishing and fraudulent messages	40	40	38	38	22	22	100
Two-factor authentication enhances transaction safety	55	55	30	30	15	15	100
Delay in complaint resolution increases fear of fraud	58	58	27	27	15	15	100
Banks provide sufficient guidance on safe online banking practices	28	28	42	42	30	30	100

Source: Primary Data

The responses show a balanced yet cautious attitude towards online banking security. Half of the participants (50%) neither agree nor disagree that online banking is secure, while 35% consider it safe, indicating hesitation among users. A large proportion (60%) believe that

banks do not adequately compensate customers in cases of online fraud, reflecting weak confidence in institutional protection. At the same time, 45% feel that online money theft cases are rising, which may contribute to fear among users. However, convenience remains a major factor, as 60% state that online banking is easier than traditional methods. Awareness of phishing appears moderate, with 40% agreeing they are aware, while a considerable number remain neutral. More than half (55%) recognize that two-factor authentication improves safety, and 58% think delays in complaint handling increase anxiety. Only 28% feel banks provide enough guidance on secure usage, suggesting room for improvement in awareness programs. Overall, the findings indicate that although users appreciate convenience, concerns about fraud management and security support continue to exist.

Table 3: Opinion on Online Banking Fraud.

Statements	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Total
Phishing messages and fake links are major causes of online banking fraud	30	28	22	12	8	100
Fake customer care calls increase the risk of financial loss	25	32	20	15	8	100
Sharing OTP or PIN leads to unauthorised transactions	35	30	18	10	7	100
Banks respond promptly to online fraud complaints	10	18	30	25	17	100

Source: Primary Data

The responses indicate considerable awareness of common online banking fraud practices. Regarding phishing messages and fake links, 30% strongly agree and 28% agree (total 58%) that they are major causes of fraud, while 22% remain neutral and 20% disagree or strongly disagree. Similarly, 25% strongly agree and 32% agree (57% in total) that fake customer care calls increase financial risk, whereas 20% are neutral and 23% express disagreement. A clear majority also recognize the danger of sharing confidential details, as 35% strongly agree and 30% agree (65%) that sharing OTP or PIN results in unauthorised transactions; only 17% disagree and 18% remain neutral. However, confidence in banks' response to fraud complaints appears low. Only 10% strongly agree and 18% agree (28%) that banks respond promptly, while 30% are neutral and a larger share—25% disagree and 17% strongly disagree (42%)—express dissatisfaction. These figures show that although respondents are generally

aware of fraud risks, many lack confidence in the speed and effectiveness of banks' grievance redressal mechanisms.

Limitations of the Study

The study is limited to respondents from Chennai and does not cover rural areas. The sample size of 100 respondents restricts wider generalisation of the findings. A larger representation of younger respondents may have influenced the results. The study was conducted within a short time frame and may not capture long-term trends. Since the data is based on self-reported responses, the possibility of respondent bias cannot be ruled out. Limited availability of recent secondary data also acted as a constraint.

Findings of the Study

1. The highest number of respondents (40%) are aged 18–25, compared to 33.3% below 18 and 26.7% above 25, showing greater involvement of younger users.
2. Women form 63.3% of the sample, while men account for 36.7%, indicating stronger female representation in the study.
3. Postgraduates make up the largest occupational group (40%), followed by employees (27%), undergraduates (20%), and school students (13%).
4. About 50% remain neutral on the security of online banking, and only 35% consider it secure, suggesting hesitation among users.
5. Nearly 45% feel that online fraud cases are increasing.
6. A majority (60%) believe banks do not properly compensate fraud victims.
7. Even with these concerns, 60% find online banking more convenient, and many respondents (58%–65%) recognize phishing, fake calls, and OTP sharing as common causes of fraud.

SUGGESTIONS

1. Strengthen security measures to minimize online fraud.
2. Create regular programs to educate customers about digital safety.
3. Make grievance handling systems quicker and more efficient.
4. Offer clear instructions for safe online banking usage.
5. Enforce strict punishment to control cybercrimes.

CONCLUSION

Online banking has become a vital part of India's financial system by providing easy access and convenience to users. At the same time, the increasing incidence of online fraud and cyber security threats has raised serious concerns regarding the safety and reliability of digital banking platforms. Although various preventive measures have been introduced by the Government of India, the Reserve Bank of India, and banking institutions, customer confidence in online banking continues to remain uncertain. To ensure the sustainable growth of digital banking, there is a need to strengthen technological safeguards, enforce regulatory mechanisms more effectively, and enhance customer awareness regarding safe banking practices. Addressing these issues will help build stronger trust among users and support the long-term development of secure and efficient online banking services.

REFERENCES

1. Drigă, I., & Isac, C. (2014). E-Banking services: Features, challenges and benefits. Annals of the University of Petrosani, Economics, Vol. 14, Issue 1, pp. 49–58.
2. Ansari, S. J., & Han, N. A. (2017). E-Banking in India: Progress and challenges. International Journal of Innovative Research and Advanced Studies, Vol. 4, Issue 6.
3. Bank for International Settlements (BIS). (2003–2015). Management and supervision of cross-border electronic banking activities. BIS Publications, Basel.
4. Chauhan, V., & Chaudhary, V. (2015). Internet banking in India: Challenges and opportunities. Journal of Management Science and Technology, Vol. 2, Issue 3, pp. 29–40.
5. Dangwal, R. C., & Jan, K. S. (2010). The upcoming technology and associated innovation. ICFAI University Press.
6. Directorate of Enforcement vs Axis Bank & Ors. (2019). Reported Case Law.
7. Reserve Bank of India (RBI). Various years. Reports on digital payments and cyber security. RBI Publications, Mumbai.
8. National Crime Records Bureau (NCRB). Various years. Cyber Crime Reports**.** Ministry of Home Affairs, Government of India.