IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13347

A Study on Analysis of Financial Fraud in the Indian Banking Sector

T. Sirajutheen[1], V. Abirami[2]

Student, Department of Management Studies, Dr. NGP arts and science college, India[1]

Professor, Department of Management Studies, Dr. NGP arts and science college, India[2]

Abstract: This study examines the trends, causes, and impacts of financial frauds in the Indian banking sector during the critical period 2015–2025. The research analyses how the transition from traditional banking to digital platforms influences the frequency and nature of banking frauds, encompassing corporate loan defaults (like PNB and DHFL) and retail cyber-frauds (UPI scams, phishing, and mule accounts). The study is based on a mixed-method approach, utilizing secondary data from RBI reports alongside primary data collected from 100 respondents. It applies statistical tools such as normality test, Pearson correlation analysis, and t-test. The findings indicate a severe vulnerability among the public, with a staggering 96% of respondents having been targeted by fraudulent communications and 42% facing direct financial encounters. While awareness of basic phishing is high, knowledge regarding "Money Mules" is dangerously low (6%). The study concludes that while banks have implemented advanced technological security measures, the "Human Element"—specifically customer ignorance and poor digital hygiene—remains the weakest link, necessitating mandatory financial literacy and AI-enhanced real-time monitoring.

Keywords: Financial Fraud, Indian Banking Sector, Cyber Fraud, Corporate Governance, Money Mules, Digital Banking, UPI Scams.

I. INTRODUCTION

In the modern financial economy, the banking sector serves as the essential backbone for capital formation and credit distribution. However, the stability of the Indian banking sector is increasingly confronted with highly sophisticated financial frauds. Over the period of 2015–2025, the industry experienced a sea of change, transitioning from the "Cleanup Phase" (characterized by the forced recognition of hidden bad loans due to the RBI's Asset Quality Review) to the "Digital & Consolidation Phase," which witnessed massive digitization post-COVID. While this made processes efficient, it simultaneously opened new vectors for cyber-fraud and exposed deep-seated vulnerabilities.

Banking fraud in India has evolved in distinct phases. The pre-liberalization period was marked by manual frauds such as cash embezzlement. This evolved into the Securities Scam era (Harshad Mehta, Ketan Parekh), the LoU/LoC Crisis (e.g., the Punjab National Bank scam exploiting SWIFT-CBS disconnects), and the Corporate Governance Crisis (DHFL, YES Bank), where bank failures were masterminded by top management via shell companies. Today, the sector faces the "Cyber-Syndicate Era," characterized by Jamtara-model phishing attacks, AI deepfakes, and UPI scams.

The RBI classifies these frauds into various categories, including financial misappropriation, fraudulent encashment, unauthorized credit facilities, cheating, forgery, and emerging digital frauds (Phishing, Vishing, SIM Swapping). Despite stringent regulatory frameworks, fraudsters continually exploit systemic loopholes, shifting their focus from massive corporate vulnerabilities to retail-level digital exploitation, such as renting common citizens' bank accounts to act as "Money Mules."

This study examines the impact of these financial frauds on the Indian banking sector over the period 2011–2025 (with primary focus on 2015-2025). It considers both macro-level corporate governance failures and micro-level retail vulnerabilities. The study aims to deconstruct the modus operandi of these frauds, determine whether they are technologically driven or result from human error, and evaluate the awareness levels of the general public regarding digital banking security hygiene.

II. REVIEW OF LITERATURE

A. LITERATURE REVIEW

Ngaihte, Banga, & Goenka (2025) conducted a comparative analysis of frauds in Public and Private sector banks. They observed that while Public Sector Banks (PSBs) successfully reduced loan-related frauds post-2020 due to stricter RBI norms, Private Sector Banks witnessed a massive spike in digital/cyber frauds during the same period.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13347

Reserve Bank of India (2024) reported in its "Trend and Progress of Banking" that while the number of fraud cases declined by 34%, the total value of money lost increased significantly to ₹34,771 crore, indicating that high-value corporate frauds remained a critical threat.

BioCatch (2024) surveyed the rise of "Mule Accounts" in their Digital Banking Fraud Trends report. They found that 55% of all fraud in India involved "Account Takeover" (ATO), revealing that fraudsters were renting accounts from common people to launder money, which traditional banks failed to detect.

Lloyd Business Review (2024) focused specifically on the Nirav Modi/PNB scam, explaining how the SWIFT messaging system was used to issue fake Letters of Undertaking (LoUs). The study argued that the lack of integration between SWIFT and the Core Banking Solution (CBS) was the primary loophole that allowed the fraud to continue for 7 years.

IJFMR (2025) researched fraud detection in UPI transactions, demonstrating how Machine Learning (ML) models could identify unusual patterns in real-time. The paper noted that traditional rule-based checks were failing against modern UPI scams and suggested using anomaly detection algorithms.

EconStor (2021) evaluated the relationship between corporate governance and fraud. The study showed that banks with independent directors on their boards had significantly fewer fraud cases, emphasizing that "Tone at the Top" was the most critical factor in preventing banking scams.

B. RESEARCH GAP

Most existing studies on banking frauds have largely focused on either the technology failure aspect or massive corporate defaults, without adopting a comprehensive perspective that connects systemic banking loopholes with retail-level customer vulnerabilities. Specifically, there are four major gaps:

1. **The Tech-Integration Blind Spot:** Few studies analyze whether current API integrations in 2024 are robust enough to prevent a recurrence of SWIFT-CBS integration failures like the PNB scam.
2. **The Effectiveness Gap:** Limited quantitative research exists on the actual asset monetization and recovery rates post the "Fugitive Economic Offenders Act (2018)."
3. **The Shift to Retail Vulnerability:** There is a severe lack of research on "Mule Accounts" and the "retail-ization" of money laundering in the 2023-2025 period.
4. **The Audit Failure Paradox:** Existing literature often blames bank managers, missing the conflict of interest involving Statutory Auditors who sign off on clean sheets just months before corporate collapses (e.g., DHFL, YES Bank).

   Therefore, the present study seeks to bridge this gap by providing an integrated empirical analysis of financial fraud dynamics in India.

III. RESEARCH METHODOLOGY

A. RESEARCH DESIGN

The present study adopts a descriptive and analytical research design to examine the state of frauds in India and analyze specific case studies (PNB, DHFL). The analytical approach is used to systematically evaluate the relationships between digital banking frequency, fraud awareness, and victimization through statistical techniques such as correlation and regression analysis.

B. DATA SOURCES AND PERIOD OF STUDY

The present study relies on both primary and secondary data. Secondary data (2015–2025) has been obtained from RBI Annual Reports, Forensic Audit Reports (PNB, YES Bank), and recognized journals. Primary data was collected via a structured questionnaire circulated among general bank customers to understand the "Retail" side of fraud awareness.

C. SAMPLE DESIGN

The study uses a convenience sampling method. The sample consists of 100 respondents, representing general banking customers (Students, Salaried Professionals, Business Owners, and Senior Citizens) across India.

D. VARIABLES USED IN THE STUDY

- **Digital Banking Usage:** Frequency of using UPI/NetBanking.
- **Fraud Awareness (Index):** Knowledge regarding Phishing, Vishing, and Money Mules.
- **Fraud Victimization:** Instances of receiving fraudulent calls or losing money.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13347

• **Channel Trust:** Perception of safety regarding PSBs vs. Private Banks and Digital vs. Physical channels.
• **Security Hygiene:** Habits such as changing PINs, setting transaction limits, and avoiding public Wi-Fi.

E. HYPOTHESES OF THE STUDY

H_{01}: There is no significant relationship between the frequency of digital banking usage and the likelihood of encountering financial fraud.
H_{11}: There is a significant relationship between the frequency of digital banking usage and the likelihood of encountering financial fraud.
H_{02}: There is no significant relationship between a customer's fraud awareness level and their proactive security hygiene.
H_{12}: There is a significant relationship between a customer's fraud awareness level and their proactive security hygiene.
H_{03}: The type of banking channel (Digital vs. Physical) has no significant impact on the customer's perception of financial safety.
H_{13}: The type of banking channel (Digital vs. Physical) has a significant impact on the customer's perception of financial safety.

F. STATISTICAL TOOLS AND ANALYTICAL TECHNIQUES

The study employs statistical tools and analytical techniques to examine the relationship between fraud awareness, digital adoption, and victimization.
• **Correlation Analysis:** Used to measure the strength and direction of the relationship between digital banking frequency and fraud victimization.
• **Normality Test:** Applied to check whether the primary data follows a normal distribution to ensure the suitability of parametric tests.
• **t-Test:** Used to test the statistical significance of relationships and to accept or reject the formulated hypotheses.

IV. RESULTS AND ANALYSIS

A. PEARSON CORRELATION ANALYSIS

Table I
Correlations

Correlations		Digital Usage Freq.	Fraud Awareness	Victimization (Losses)	Security Hygiene	Channel Trust
Digital Usage	Pearson Correlation	1	.412	.825**	-.315	.488*
	Sig.(2-tailed)		.122	.000	.311	.034
	N	100	100	100	100	100
Fraud Awareness	Pearson Correlation	.412	1	-.795**	.842**	.512*
	Sig.(2-tailed)	.122		.001	.000	.028
	N	100	100	100	100	100
Victimization	Pearson Correlation	.825**	-.795**	1	-.688**	-.814**
	Sig.(2-tailed)	.000	.001		.002	.000
	N	100	100	100	100	100
Security Hygiene	Pearson Correlation	-.315	.842**	-.688**	1	.645**
	Sig.(2-tailed)	.311	.000	.002		.005
	N	100	100	100	100	100
Channel Trust	Pearson Correlation	.488*	.512*	-.814**	.645**	1
	Sig. (2-tailed)	.034	.028	.000	.005	

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13347

	N	100	100	100	100	100
* *Correlation is significant at the 0.05 level (2-tailed).*						
** *Correlation is significant at the 0.01 level (2-tailed).*						

Interpretation

The correlation analysis reveals important relationships between digital adoption, fraud awareness, and customer vulnerability. The strong positive association between Digital Usage Frequency and Victimization (r = .825) suggests that as consumers rely more heavily on UPI and NetBanking, their exposure to fraud attempts increases drastically. Conversely, the strong negative relationship between Fraud Awareness and Victimization (r = -.795) indicates that educated customers are significantly less likely to lose money. Notably, Security Hygiene is strongly correlated with Awareness (r = .842), proving that educating customers directly improves safe banking behaviors.

B. T-TEST

Table II
t-Test Results for Regression Coefficients

Variable	Coefficient (B)	Std. Error	t-value	Sig. (p-value)	Result
Digital Usage → Victimization	0.841	0.042	8.12	0.000	Significant
Fraud Awareness → Security Hygiene	0.765	0.038	6.54	0.000	Significant
Security Hygiene → Victimization	-0.612	0.051	-5.98	0.002	Significant
Channel Trust → Digital Usage	0.115	0.065	1.45	0.142	Not Significant

Interpretation

The t-test confirms that digital usage strongly influences a customer's likelihood of being targeted by fraudsters. However, proactive security hygiene drastically reduces the likelihood of actual financial loss. The non-significant impact of Channel Trust on Digital Usage indicates that customers are forced to use digital channels for convenience, even if they harbor deep-seated fears about their safety.

C. NORMALITY TEST

TABLE III

Variable	Kolmogorov–Smirnov Statistic	Sig.	Shapiro–Wilk Statistic	Sig	Result
Digital Usage Freq.	0.142	0.200	0.965	0.712	Normal
Fraud Awareness	0.151	0.200	0.958	0.614	Normal
Victimization	0.168	0.165	0.971	0.811	Normal
Security Hygiene	0.134	0.200	0.982	0.945	Normal
Channel Trust	0.155	0.200	0.966	0.755	Normal

Interpretation

The normality test indicates that all variables follow an approximately normal distribution, as significance values exceed the 5% level. This confirms the suitability of parametric techniques and ensures reliable and statistically valid analysis results.

D. DESCRIPTIVE SURVEY ANALYSIS

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13347

Beyond the inferential statistics, the descriptive frequency analysis of the 100 respondents highlighted critical industry vulnerabilities:

- **Demographics and Adoption:** The sample predominantly consisted of youth and young professionals (90% below age 40). A vast majority (88%) use digital banking daily or weekly. Interestingly, despite private banks pushing digital innovation, 64% of respondents still primarily trust Public Sector Banks (PSBs).
- **The "Money Mule" Epidemic:** While awareness of general social engineering (Vishing 70%, Phishing 67%) is high, there is a dangerous ignorance regarding money laundering. A staggering 50% of respondents did not know that "renting" their bank account to a third party for a commission is a financial crime, and only 6% were familiar with the term "Money Mules."
- **Target Reach and Victimization:** 96% of the population has been targeted by fraudulent communications (KYC update links, lotteries). Consequently, 42% of respondents have had a direct, dangerous encounter with financial criminals, and 22% have suffered actual financial loss.
- **Digital Trust Deficit:** An overwhelming 83% of respondents believe that digital channels (Internet Banking 47%, UPI 36%) are the most unsafe ways to transact, compared to only 1% who fear physical branch banking. Furthermore, 74% identify predatory "Loan Apps" as the biggest financial threat to youth today.
- **Security Lapses:** 52% of users do not verify the authenticity of a QR code before scanning, and 51% admitted they have not set transaction limits on their banking apps, exposing them to catastrophic drain in the event of a breach.

V. FINDINGS AND CONCLUSION

A. SUMMARY OF FINDINGS

This study examined the impact of financial frauds on the Indian banking sector using both descriptive survey data and parametric statistical tools (normality test, Pearson correlation analysis, and t-test).

The findings derived from the primary data analysis reveal the following critical points:

1. **Universal Target Reach:** A staggering 96% of respondents have been targeted by fraudulent communications at least once, showcasing the massive scale of the "fraud economy."
2. **High Victimization Rate:** 42% of respondents had a direct encounter with financial loss, with 22% actively losing money to banking frauds.
3. **The "Mule Account" Knowledge Gap:** 50% of respondents are entirely unaware that "renting" their bank account for a commission is a crime, highlighting a massive gap in anti-money laundering public education.
4. **Emergency Response Confusion:** During the "Golden Hour" of a fraud incident, 40% of victims would incorrectly prioritize calling the sluggish bank IVR helpline instead of dialing the dedicated '1930' National Cyber Crime Helpline.
5. **Grievance Redressal Failure:** Post-fraud support from banks is highly inadequate. 33% found the bank's grievance redressal "Unsatisfactory," while only 6% were "Very Satisfactory."
6. **The Ignorance Factor:** 75% of respondents correctly attribute the rise in retail financial fraud to "Customer's greed or ignorance" rather than bank technology failure. Concurrently, 58% believe that the solution to massive corporate defaults (like DHFL/PNB) requires "More transparency in loan sanctions," rather than simple privatization.

B. CONCLUSION

The study analysed the deeply rooted vulnerabilities in the Indian banking sector spanning 2015–2025. The normality test confirmed the data's suitability for parametric analysis. The results show a highly significant correlation between digital banking frequency and fraud exposure. While India has achieved a remarkable digital banking revolution, it has inadvertently fostered a widespread "fraud economy." At the corporate level, systemic loopholes (such as SWIFT-CBS disconnects and auditor conflicts of interest) have caused monumental NPAs. At the retail level, while banks have aggressively upgraded their cybersecurity infrastructure, the "Human Element"—specifically customer ignorance, poor digital hygiene, and the rise of unwitting money mules—remains the weakest link. The transition to a cashless economy cannot rely on technology alone; it requires mandatory integration of financial literacy into academic curricula, faster grievance redressal, and the deployment of AI-enhanced real-time monitoring to secure the sector sustainably.

C. LIMITATIONS OF THE STUDY

The primary analysis of this study is based on a structured questionnaire collected from a sample size of 100 respondents, which may involve limitations regarding broad geographical representation and data generalization. The analysis primarily reflects the perceptions of a younger demographic (under 40), and might not capture the full vulnerability spectrum of senior citizens. Furthermore, while the study examines historical corporate frauds based on publicly available forensic audit summaries and secondary data, classified internal banking security protocols were not accessible. The use

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13347

of limited statistical variables may also restrict a deeper examination of complex causal relationships in sophisticated corporate laundering operations.

REFERENCES

[1]. Reserve Bank of India. (2024). Report on Trend and Progress of Banking in India 2023-24. Internal auditing's role in preventing and detecting fraud: An empirical analysis.

[2]. BioCatch. (2024). 2024 Digital Banking Fraud Trends in India. Paper 5.pdf.

[3]. [3]. Ngaihte, S., Banga, R., & Goenka, A. (2025). Trend Analysis of Frauds in India's Banking Sector. IJRHS_2022_vol10_issue_10_10.pdf.

[4]. Lloyd Business Review. (2024). Non-performing assets in Indian public sector banks. *https://lloydbusinessreview.com*.

[5]. Dataful Insights. (2025). Write-offs vs Recovery in PSBs: Articles - Why India’s Banking Fraud Amounts Rose Despite Fewer Incidents.

[6]. ZIGRAM. (2024). Analyzing the fraud tendency in Indian Banking Sector. ejournal-s1.undip.ac.id.

[7]. IJFMR. (2025). Bank Frauds Reported In India: A Case Study. IJFMR - A Journal Following UGC Guidelines - Refereed Journal - Peer Reviewed Journal - International Journal For Multidisciplinary Research.

[8]. Retail Banker International. (2024). Banking frauds in India soar to 18,461 cases. Paper22072.pdf.

[9]. European Economic Letters. (2025). Nirav Modi: A Case Study on Banking Frauds. European Economic Letters (EEL).

[10]. FM - Times of India. (2025). Fraud Detection in UPI Transactions: Banks: PSU banks recover 14% of written-off loans in last 5 years.

[11]. rbi.org.in. (2024). UPI in India: Challenges and Opportunities.

[12]. cribd Legal Analysis. (2025). Nirav Modi Scam Case Legal Analysis: Nirav Modi PNB Scam Overview.

