INTERNATIONAL DEVELOPMENT PLANNING REVIEW
ISSN:1474-6743 | E-ISSN:1478-3401

THE HIDDEN COST OF CYBER FRAUDS ON FINANCIAL INCLUSION IN INDIA

***Dr.S.Subbulakshmi,** Abirami. B**
*ORCID ID: 0000-0002-6821-9776, Associate Professor, P.G. Department of Commerce, SDNB Vaishnav College, for Women, Chromepet, Chennai44
** II-M.COM, P.G. Department of Commerce, SDNB Vaishnav College for Women, Chromepet, Chennai–44

Abstract
India's digital economy has boosted financial access, especially in rural and low-income communities. Yet, with 15.9 lakh cyber incidents in 2023, digital fraud now poses a serious threat to financial inclusion. Beyond financial loss, it leads to fear, mistrust, and exclusion—especially among women, elderly, and rural users. This paper explores these hidden impacts, analyzes policy and behavioral gaps, and proposes inclusive, community-level responses. Real financial inclusion demands not just access—but safety, trust, and support.

Keywords: Digital Economy, Cyber Frauds, safety, support Financial Inclusion, policy and behavioral gaps

1. A. Introduction: A Double-Edged Growth

India's fintech revolution is deep and fast. Over 750 million smartphone users and 49% of global real-time digital payments make India a global leader. Initiatives like UPI, PMJDY, and Digital India have pushed access to the remotest corners. The RBI's Financial Inclusion Index stood at 60.1 in 2023, showing steady progress.

But rising access comes with rising threats. CERT-In reported **15.9 lakh cyber incidents in 2023**, many affecting first-time or vulnerable users—daily wagers, women, small vendors. For them, one fraud can erase years of trust and savings. The loss is personal and long-lasting.

1. B. Statement of the problem:

The purpose of the study is to learn more about the frequency of fraud episodes, the monetary losses resulting from fraudulent activity, and the underlying causes of this trend. Organisations can more effectively manage the risk of fraud in the post-digital age by being aware of these factors. Due to lack of availability and the gestation period, all of the frauds that were started were in rural areas, primarily in the northern states of the country, namely Bihar, Odisha, and Uttar Pradesh, where the initiator's shared documents were located. This gave people the opportunity to properly utilize digitalization.

1. C. Importance of the study:

Impact of digitalization on cyber frauds:

Determining the precise effects of India's digitalization is one of the main research challenges. Due to a lack of currency notes and coins in the economy, demonetization sparked a new wave of cyber frauds that were only occurring in a small number of places. With the advent of flexible payment gateways, fraudsters began to take a chance and turn these activities into their main source of income, running the risk of facing legal repercussions.

1. **D. Scope of the Study:**

The study focuses on the incidence of cybercrime in India and the tactics employed by scammers after banking operations were digitalized. This study was carried out in the Chennai City.
This study is entirely dependent on the target population, which is the population size of the 18–60 age range. The instances that victims of cyber frauds in Chennai have experienced are discussed with working class individuals, business owners and college students being the most affected groups. Primary research design with a well structured questionnaire used in the month of June 2025

1. **E. Review of Literature:**

In order to provide consumers with online access to nearly all banking products, the majority of Indian banks have developed their mobile and net banking websites. Internet banking / net-banking or online banking, is a digital tool that enables clients of banks or other financial Institutions have to conduct its business / non-business through online. Interesting user / Customer ID‘s and passwords are used to access net financial gateways.

This study sheds light on the banking sector's digitization and how it affects e-banking frauds. It also detects security flaws and highlights the technology that banks utilize to protect their e-banking systems.
Cybercrime, fraud, and the **RBI scams** more than doubled in value between 2019 and 20. From Rs 71,543 crore in 2018–19 to Rs 1.85 lakh crore now, the overall number of fraud cases has increased by 159%. Data released by the Reserve Bank of India (RBI) in its annual report indicates that the number of frauds increased by 28% from 6,799 instances in 2019–20 to 8,707 incidents in 2019–20. The performance of online banking was investigated by Balasubramanian et al. (2014). 52 participants in the study voiced concerns about the insecurity of the information they submit online and the possibility of their bank's website being hijacked. Clients are concerned about malware risks as well.

a. Bharat Reddy (2024),”Digital financial frauds in India: a call for improved investigation strategies”. According to a recent report, over the past three years, digital financial scams in India have cost the country an astounding 1.25 lakh crores. This study highlights the necessity of better research techniques.

b. Soni R R, Soni Neena “An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks” “2024”

The safety and dependability of financial operations are seriously threatened by the use of technology in financial services as well as by the excessive reliance on electronic and digital tools to conduct business and payment activities. The frequency of banking frauds has increased in tandem with the expanding trend of online and cyber transactions, impacting an increasing number of individuals who use financial technology tools. Fraud involving electronic cards, net banking transactions, ATMs, and internet payments has grown to be a significant problem. Even with strict security measures in place for electronic transactions, these cyber scams in financial firms result in a significant loss of money for both individuals and institutions each year.

c. Dr Rakhi Tiwari Digital Banking: A Study of Fraudulent Practices in Indian Banks "2024"-This research paper focuses on the impact of digitalization on banking frauds. It examines fraudulent practices within Indian banks.

d. Priyanka Datta, Surya Narayana Panda, Sarvesh Tanwar "A Technical Review Report on Cyber Crimes in India" "2023"

Users of social networking sites have recently seen a variety of social-networking attacks. Technical assistance scams and Internal Revenue Service (IRS) impersonation scams are the most prevalent forms of deception that attackers employ on gullible victims in an attempt to profit financially. India's cybercrime rate is steadily increasing for a number of reasons. Scammers take full advantage of the difficulty in tracking down cybercriminals. Cybercrime in India has been thoroughly examined. According to this study, the number of fraud cases is rising, and the victims are primarily between the ages of 20 and 29. Women and children are primarily impacted. Therefore, awareness campaigns are necessary to stop or prevent cybercrime in India.

2. Hidden Costs: What Numbers Don't Show

Beyond money, cyber fraud takes a human toll:

- **Trust Breakdown:** 40% of rural users stop using digital tools after fraud.
- **Fear-Driven Withdrawal:** Women and elderly often quit UPI or wallets out of fear.
- **Social Silence:** Shame and self-blame prevent many from reporting.
- **Credit Freeze:** Fraud leads to credit reluctance; some face CIBIL issues.
- **MSME Barriers:** 51% of MSMEs are rural, yet many avoid digital finance.
- **Gender Divide:** Though 22.24% of MSMEs are woman-led, many lack digital confidence.

Each incident deepens digital fear. Financial access becomes financial trauma.

3. Institutional Responses: Progress with Gaps

India has taken several key steps:

- **DPIP (Digital Payment Intelligence):** AI-based fraud detection.
- **Bank.in / Fin.in:** Domain naming to avoid phishing.
- **CPFIR:** Central fraud registry.
- **Cyber Campaigns:** Awareness by RBI and MeitY.
- **Grievance Tools:** Helpline (1930), portals, and Lok Adalats.
- **Counseling Centres:** Support in cities like Jaipur and Mumbai.

Yet, many solutions are urban and technical. Victims—especially in rural or low-literacy areas—struggle to access or even understand them.

4. Behavioral Gaps: Why Trust Fails

Access is not enough. Usage needs confidence. Data reveals:

- **Only 61.4%** of rural people have basic financial literacy (RBI 2023).
- **Only 36%** of rural women feel confident using digital banking.
- **<50%** of fraud money is recovered.

- **1 in 3 SHG women** refuse to use UPI out of fear.
- **43% of rural MSMEs** avoid online credit fearing fraud.

Digital distrust is rising, silently.

5. Building Resilience: Six Human-Centered Solutions

A. Emotional Recovery & Peer Support

- **Victim Groups:** Use SHGs and NGOs for shared healing.
- **Counseling Help:** Expand Maharashtra's model nationwide.
- **Storytelling:** Promote survivor stories to reduce stigma.

B. Cyber Literacy through Community

\

- **SHG & MSME Focus:** Add cyber safety in training.
- **Local Languages:** Visual/audio tools in Tamil, Hindi, etc.
- **Peer Trainers:** Trusted locals as digital guides.

C. Safer, Simpler Platforms

- **Human UI:** Use icons, colors, and voice support.
- **AI Warnings:** Flag risky transactions simply.
- **One-Click Help:** Complaint buttons in regional languages.

D. Inclusive Monitoring

- **Dormant Account Tracking:** Spot dropout after fraud.
- **Redress Timelines:** Publish average complaint resolution time.
- **Confidence Surveys:** Track post-fraud recovery.

E. More Accountability

- **Cyber Audits:** Mandatory yearly checks.
- **Grievance Scorecards:** Rate banks/platforms on complaint handling.
- **Fraud Case Repository:** Share anonymized examples for learning.

F. Secure Rural Entrepreneurship

- **Train Bank Mitras:** Add fraud awareness.
- **Microloan Protection:** Link loans with basic cyber safety.
- **Certification Tags:** "Cyber Safe" badges for MSMEs.

These aren't just tools. They rebuild confidence.

6. Conclusion: Trust is the Real Currency

India's digital growth is promising but fragile. When fear outweighs access, inclusion fails. Cyber fraud breaks not just wallets, but trust and dignity.

Real solutions need empathy, not just technology. By supporting victims and building safer systems, India can lead in digital trust—not just transactions.

Financial inclusion must be safe to be real. Trust is essential, not optional.

Research Gaps & Future Directions:

Contextual rural studies should be given priority in future research on digital payment fraud in India, with a focus on empirical assessments that examine the effects of fraud on vulnerable and rural populations. Furthermore, assessing the success of public marketing and awareness efforts like DigiKavach (2023) can reveal how well these activities inform users and discourage fraud. Evaluating scalable fraud recovery measures, such as liability caps, insurance models, or auto-reversals, to determine how well they safeguard users is equally crucial. Lastly, thorough cost-benefit assessments are necessary to weigh the benefits of financial inclusion against the expenses of preventing fraud and provide evidence-based recommendations for policymakers.

References:

- **RBI Financial, Annual Report 2024–25,23**
- **MSME, NPCI, CERT Annual Report.**

Websites:

- **www.google.co.in**
- **www.wikipedia.com**
- **www.ijrcm.com**
- **www.scribd.com**
- **www.slideshare.com**
- https://www.hindustantimes.com/business/financial-fraud-top-cyber-crime-in-india- upi-e-banking-most-targeted-study-101695036325725

Journals:

- Priyanka Datta, Surya Narayana Panda, Sarvesh Tanwar, (2024), "A Technical Review Report on Cyber Crimes in India"
- Bharat Reddy (2024) Digital financial fraud in India: a call for improved investigation strategies
- Priyanka Datta, Surya Narayana Panda, Sarvesh Tanwar, (2024), "A Technical Review Report on Cyber Crimes in India"
- Dr. Rakhi Tiwari, (2024), "Digital Banking: An Examination of Fraudulent Activities in Indian Banks"
- R.R. Soni and Neena Soni (2013),An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks