International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Exploring India's Digital Financial Landscape: A comprehensive study of Cyber Fraud Trends and Digital Literacy in India

*Vishal Singh Yadav[1], Prof. Anshuja Tiwari[2] , Prof. Mukesh Chansoriya[3] , Jasvinder Singh Aujla[4]*

Research Scholar, Faculty of Management, Lakshmi Narain College of Technology, Bhopal[1]
Professor, Department of Commerce, Barkatullah University, Bhopal[2]
Professor, Faculty of Management, Lakshmi Narain College of Technology, Bhopal[3]
Research Scholar, Faculty of Management, Lakshmi Narain College of Technology, Bhopal[4]

**ABSTRACT:**

The exponential growth of digital financial services in India presents a double-edged phenomenon of unprecedented opportunity and significant risk. This research critically examines the intricate landscape of digital financial fraud, exploring the multifaceted challenges emerging from India's rapid digital transformation. By analyzing digital connectivity, cyber financial crime patterns, and the complex interplay between technological adoption and fraud vulnerabilities, the study unveils critical insights into the nation's digital financial security ecosystem. Leveraging comprehensive secondary data and advanced statistical analysis, this research provides a nuanced understanding of digital fraud trends, geographical variations, and the pivotal role of digital literacy in shaping cybersecurity outcomes.

**Keywords:** Digital Financial Fraud, Digital Payments, Digital Financial Inclusion, Cybersecurity, Digital Literacy, Digital Financial Services

## Introduction:

In the last few years, especially post demonetisation in 2016 and the COVID-19 pandemic, there has been a major spike in the number of digital payments in India. Innovation in the payments landscape, regulatory support, the increase in smartphone penetration and cheaper mobile internet access have played a key role in the adoption of digital transactions and their rapid growth in India. Payment service providers, along with new players and additional investments, have been providing an enhanced seamless user experience at competitive prices, promoting wider adoption of digital payments.[1]

The rapid growth of digital financial services in India has brought about significant benefits in terms of financial inclusion and convenience. However, this expansion has also been accompanied by a rise in digital financial fraud. As India continues to embrace digital payments and online banking, understanding the nature, scale, and impact of digital financial fraud has become a crucial priority for policymakers, regulators, and financial institutions. India has witnessed a remarkable surge in the adoption of digital financial services in recent years. The launch of the Unified Payments Interface (UPI) in 2016, the proliferation of digital wallets, and the increasing penetration of internet and smartphone usage have all contributed to this trend. Retail digital payments in India growing from 162 crore transactions in FY2012-13 to over 14,726 crore transactions in 2023-24 (till February 2024) i.e., approximately 90-fold increase over 12 years. UPI is used at all levels from street vendors to large shopping malls. Today, among all countries in the world, India is the country with the highest digital transaction, accounting for nearly 46% share, as per the 2022 data. India is followed by Brazil, China, Thailand and South Korea. [2]

However, this rapid digitalization of the financial landscape has also opened the door to a wide range of fraudulent activities. Cybercriminals have been quick to exploit the vulnerabilities in the digital ecosystem, targeting unsuspecting consumers, financial institutions, and fintech providers. The evolving nature of these fraud techniques, coupled with the diverse socioeconomic and technological landscape of India, has made it challenging to effectively combat this growing menace.

## Types of Digital Financial Fraud in India:

The research has identified the following prevalent types of digital financial fraud in India:

**(a) Phishing and Social Engineering Attacks:** Cybercriminals use sophisticated techniques, such as fake emails, SMS messages, or social media posts, to trick users into divulging sensitive financial information, like login credentials or payment card details.

**(b) Unauthorized Access to Bank Accounts and Digital Wallets:** Fraudsters exploit security vulnerabilities to gain unauthorized access to user accounts, enabling them to make fraudulent transactions or steal funds.

**(c) Fraudulent Mobile Applications and Websites:** Malicious actors create fake mobile applications or websites that mimic legitimate financial services, aiming to lure unsuspecting users and steal their personal and financial information.

**(d) Card Skimming and Cloning:** Fraudsters use card skimming devices or compromised ATMs to capture payment card details, which are then used to create counterfeit cards for unauthorized transactions.

**(e) UPI-based Fraud and Transaction Hijacking:** Cybercriminals exploit vulnerabilities in the UPI ecosystem to initiate fraudulent transactions, often by impersonating legitimate users or hijacking ongoing transactions.

**(f) Investment Scams and Ponzi Schemes:** Fraudulent investment schemes and Ponzi scams, often promoted through online channels, have defrauded numerous Indian consumers, resulting in significant financial losses.

**(g) Identity Theft and Synthetic Fraud:** Fraudsters use stolen or fabricated personal identities to open new financial accounts, obtain loans, or conduct other fraudulent activities.

These fraud techniques continue to evolve, as cybercriminals adapt their methods to exploit new vulnerabilities and take advantage of the rapidly expanding digital financial ecosystem in India.

## Literature Review:

Digital fraud has emerged as a significant challenge in today's increasingly digitized world. Various studies and reports have been conducted to understand the scope, impact, and trends associated with this phenomenon, both globally and within specific regions like India. This overview provides insights from prominent sources, highlighting the gravity of the issue and the urgent need for effective countermeasures.

### (a) Global Perspective

1. The "LexisNexis Risk Solutions Cybercrime Report"[3] The LexisNexis Cybercrime Report for 2023 reveals a concerning upward trend in digital fraud, with global attack rates increasing by 19% year-over-year. North America experienced the most significant surge at 43%, while the ecommerce sector saw a 59% rise in attacks. The gaming and gambling industry faced a staggering 103% increase in bot volume. The report highlights evolving threats, including the emerging use of generative AI in fraud and continued exploitation of instant payment systems for scams. While attack patterns varied by region and industry, with APAC seeing a decline and North America experiencing sharp growth, the overall trend points to increasing sophistication and persistence of cybercriminals.

The report emphasizes the critical need for robust, multi-faceted fraud prevention strategies across all industries. Financial services, ecommerce, communications, and gaming sectors each face unique challenges, with attack rates and methods varying significantly. Mobile channels, particularly browsers, showed increased vulnerability. The report also notes positive developments in some countries, such as the UK and Singapore, where scam losses have stabilized due to implemented defenses. It underscores the importance of global collaboration, regulatory action, and advanced fraud detection technologies in combating the evolving cybercrime landscape. The report mentions the India's potential regulation of digital gaming services and its involvement in expanding cross-border instant payment schemes, both of which could impact future fraud patterns in the region. Additionally, it highlights the rising sophistication of fraud tactics, such as the use of synthetic identities and the exploitation of mobile channels.

2. The "Fraud Management Insights" report by SAS provides a comprehensive overview of fraud trends worldwide. The report by Javelin Strategy & Research and SAS examines global digital fraud trends in 2023, highlighting the ongoing evolution of the "global scam economy" that emerged during the COVID-19 pandemic. The study, which covers 12 countries, reveals that while the initial pandemic-related fraud schemes have subsided, they've been replaced by a diverse array of scams, including romance scams, fake employment opportunities, and investment schemes. The report notes significant regional variations in fraud trends, such as South Africa's efforts to formalize payments, Singapore's struggle with sophisticated phone-based scams, India's widespread adoption of biometric ID systems, and the growth of embedded lending and Buy Now, Pay Later (BNPL) services in the United States. The study emphasizes the need for robust, AI-driven fraud prevention strategies, including multifactor authentication, account-based alerts, and consolidated monitoring solutions. It also underscores the importance of consumer trust in the expanding global digital payment ecosystem, noting that U.S. consumers alone lost $8.8 billion to scams in 2022, a 30% increase from the previous year. The report concludes with eight expert strategies for combating fraud in the digital age, highlighting the critical role of advanced technologies like AI, machine learning, and biometrics in detecting and preventing fraud across various channels. The report also underscores the importance of advanced analytics and machine learning in combating digital fraud effectively.

### (b) India-Specific Perspective

i. Varalakshmi et al. (2024) examined cybersecurity challenges in digital payment systems. The research analyzes evolving threats like phishing attacks, malware infiltration, data breaches, and identity theft targeting digital payments. It explores the role of encryption, biometrics, tokenization, and regulatory frameworks in mitigating risks. The study employs a quantitative approach, using a structured questionnaire to collect data from 105 respondents. Analysis reveals modest positive correlations between digital payments and payment gateways (r=0.527), payment security and digital payments (r=0.655), and cybersecurity and digital payments (r=0.550). Findings emphasize the interconnected nature of security measures and digital payment platforms, highlighting the need for robust cybersecurity protocols, user education, and stakeholder collaboration to build a secure and trusted digital payment ecosystem.

(ii) Ameya, Lonkar et al. (2024) evaluated "Consumer Preparedness" (CP) against digital payment frauds in India by examining factors such as fraud awareness, protective measures, and response strategies. Through a literature review and analysis of data from 372 consumers using statistical methods like ANOVA and Chi-square, it identifies a moderate overall preparedness, characterized by low awareness, moderate protection, and high responsiveness. The study highlights the absence of a model to assess consumer readiness and suggests improvements, including the creation of a central fraud registry by Central Banks and enhanced customer authentication and awareness programs by financial institutions to improve consumer preparedness.

(iii) Dr, Selvi, S. (2024) examined the effects of digitalization on India's banking sector, especially following the demonetization event. It highlights how digital banking has enhanced transaction efficiency and accessibility, supported by government incentives for cashless payments. Despite these benefits, the increase in digital transactions has also led to a rise in cyber fraud within the banking industry. The study seeks to identify and categorize new types of cyber fraud that have emerged with digitalization and explore the underlying causes contributing to these fraudulent activities in the Indian banking sector.

(iv) Dahiya, K. (2023) explored trends in cybercrime in India, highlighting the country's growing digital landscape and associated risks. It discusses prominent trends like phishing attacks, ransomware, cyber fraud targeting financial transactions, and risks on social media platforms. The paper emphasizes the need for prioritizing cybersecurity measures, raising awareness, and establishing robust legal frameworks to combat cybercrime effectively. It provides an overview of different types of cybercrimes, including those against individuals, property, organizations, and society. The paper also outlines the Information Technology Act 2000 and its relevant sections addressing cyber offenses. Additionally, it offers strategies for cybercrime prevention and discusses various types of cybercriminals and their motivations. Overall, the paper underscores the urgent need for collaborative efforts between individuals, organizations, and the government to secure India's digital future (Dahiya, 2023).

These studies and reports underscore the pervasive nature of digital fraud, both globally and within India. They provide valuable insights into the evolving tactics employed by fraudsters, the potential impacts on businesses and individuals, and the need for proactive measures to combat this growing threat. By leveraging the findings and recommendations from these authoritative sources, stakeholders can develop effective strategies to safeguard against digital fraud and foster a more secure digital ecosystem.

## Methodology:

Doctrinal research method. The study is based on analytical and descriptive methods related to Digital Financial fraud in the banking sector. This study mainly uses secondary data, which are Books, Journals, Monthly magazines, Articles, Online sources like Research gate, Google Scholar and were used to gather relevant articles. Data from the Reserve Bank of India Report, National statistical surveys, Government reports and statistical databases, PIB, news stories, Articles, and a few reputable periodicals was also collected for the purpose.

***Objective and scope:***

The primary objective of this research is to provide a comprehensive, multidimensional analysis of digital financial fraud in India, addressing critical knowledge gaps and offering actionable insights for stakeholders across the digital financial ecosystem.

The scope of this study encompasses the following key aspects:

1. Systematically categorize and analyze prevalent digital financial fraud techniques

2. Investigate the spatial distribution of cyber financial crimes across different Indian states; Correlate digital literacy levels with fraud reporting patterns

3. Investigation of the underlying factors contributing to the rise of digital financial fraud.

4. Assessment of the financial and social impact of digital financial fraud on the broader economy.

## Analysis

The study comprises three key sections: an analysis of digital connectivity and the payment landscape in India, a geographical breakdown of cyber financial crime cases, and a Cross-sectional Analysis of State-level Data of Digital Literacy and Cyber Fraud Reporting Patterns in India. Each section aims to provide a comprehensive understanding of the respective topics.

## Digital connectivity and the payment landscape in India

**(a) Status of Digital Connectivity:** India is the world's second-largest telecommunications market. As of December 2023, tele-density stood at 85.23%. In India, the total telephone subscriber base stood at 1,190.33 million in December 2023. As of December 2023, the wireless subscribers base stood at 1,158.49 million. Delhi had the highest tele-density, while Bihar had the lowest, showing significant regional disparities in telecom penetration.

Total broadband subscriptions in the country grew from 149.75 million in FY16 to 904.54 million in FY23 (April-December). India is also the second-largest country in terms of internet subscribers. India is one of the biggest consumers of data worldwide. India was the second-largest market for Google Play in 2019 and was estimated to grow at a compound annual growth rate (CAGR) of 11% between 2018 to 2022. In 2020, India accounted for 14% of the global app installs. Indians downloaded over 28 billion apps on their mobiles in 2022 and accounted for 5% of the 625 billion downloads globally. App downloads in the country increased from 12.07 billion in 2017 to 19 billion in 2019[9][10].

This data indicates a mature mobile market with high urban penetration, growing rural adoption, and a shift towards broadband services, particularly mobile broadband.

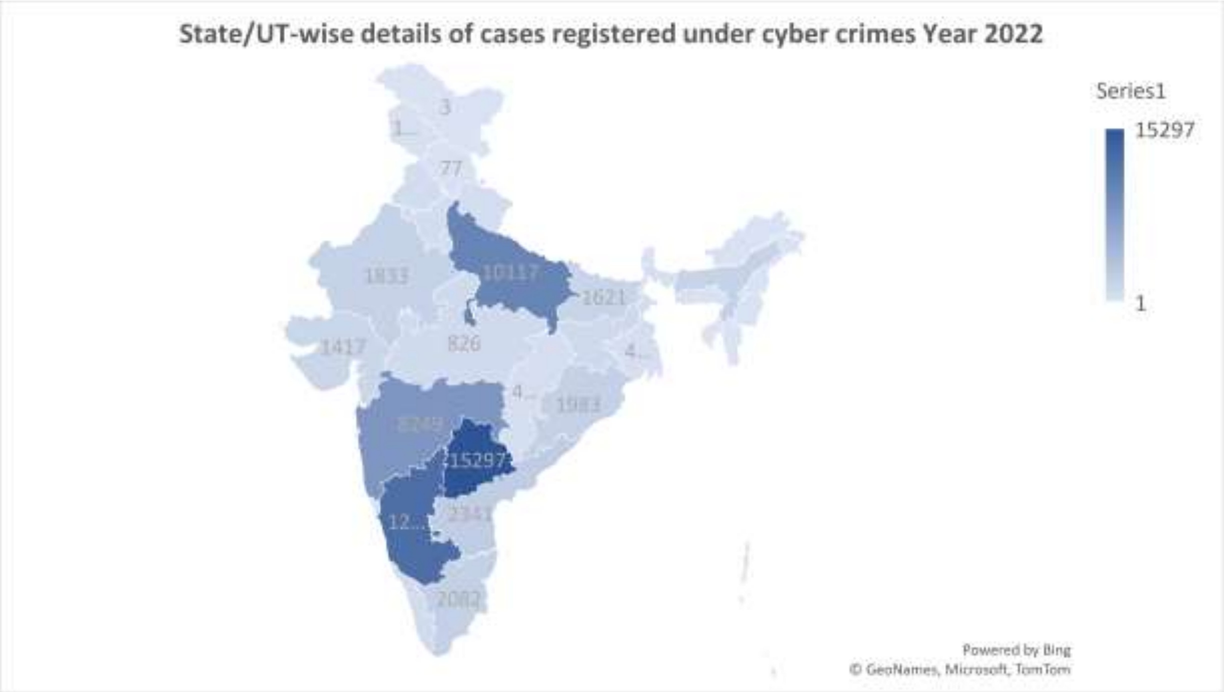
(**b) Status of Digital Payment Landscape:** As of March 2024, number of ATMs stand at 218,815, while PoS terminals at 8.90 million. QR code deployment increased substantially, with over 346 million UPI QR codes by 2024. Credit cards grew from 62 million in March 2021 to 101.8 million in March 2024, while debit cards slightly increased from 898 million to 964 million during the same period. During March 2021 to March 2024, Credit card PoS transactions increased from 62 million (value ₹188,726 crore) to 180 million (value ₹603,781 crore). While online credit card transactions jumped from 30.6 million to 163.9 million during the same period. UPI and QR-based payments showed explosive growth, with banks reporting millions of UPI QR codes deployed. From just one million transactions in 2016, UPI has since crossed the landmark 10 billion (1,000 crores) transactions. [11]

RBI-Digital Payments Index- The RBI-DPI comprises of 5 broad parameters that enable measurement of deepening and penetration of digital payments in the country over different time periods. These parameters are – (i) Payment Enablers (weight 25%), (ii) Payment Infrastructure – Demand-side factors (10%), (iii) Payment Infrastructure – Supply-side factors (15%), (iv) Payment Performance (45%) and (v) Consumer Centricity (5%). Each of these parameters have sub-parameters which, in turn, consist of various measurable indicators. The index for March 2024 stands at 445.50 as against 100 in March 2018 as base to capture the extent of digitisation of payments across the country. [12]

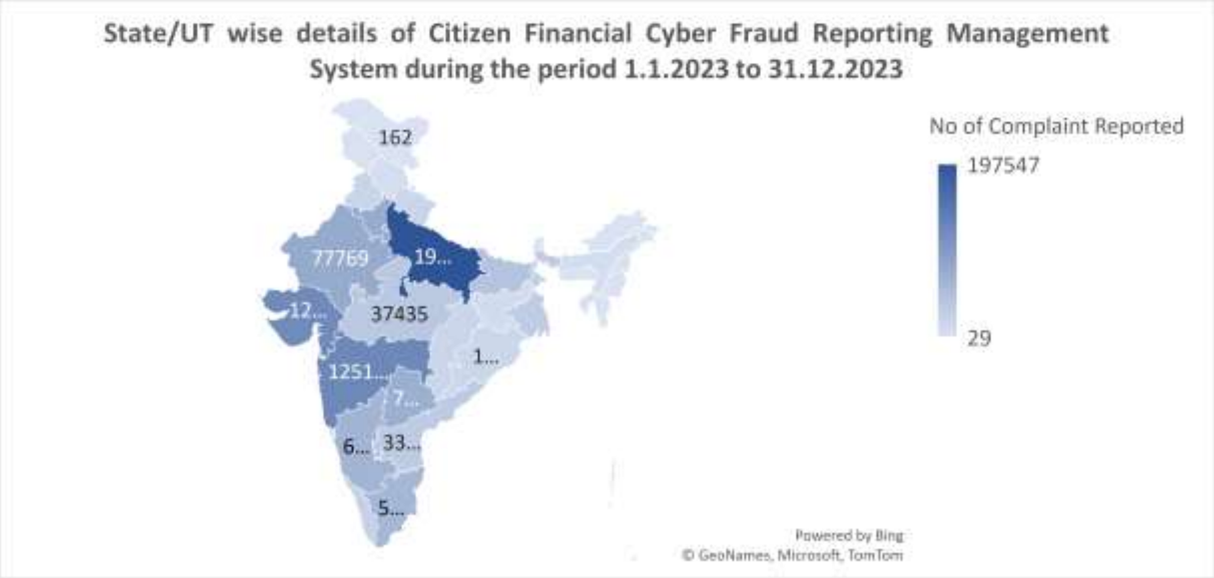
This data demonstrates India's rapid transition to digital payments, with consumers increasingly favoring electronic and mobile payment methods while maintaining access to traditional cash infrastructure.

## Geographical breakdown of cyber financial crime cases

**(a) Cyber-crime cases in India:** Total cyber-crime cases in India rose from 50,035 in 2020 to 65,893 in 2022, a 31.7% increase over three years.[13] Telangana (15,297), Karnataka (12,556), and Uttar Pradesh (10,117) reported the highest number of cyber-crime cases, accounting for about 57% of all cases nationwide. States with major tech hubs and metropolitan areas tend to report higher numbers of cases, likely due to greater internet penetration and digital transactions. Despite being home to Mumbai, a major financial and tech hub, Maharashtra reported 8,249 cases, significantly fewer than Telangana or Karnataka. Southern states (Telangana, Karnataka, Tamil Nadu, Kerala) collectively account for a large proportion of reported cases.


State/UT-wise details of cases registered under cyber crimes Year 2022
3
1...
77
1833
10117
1621
1417
826
4...
4...
1983
8249
15297
12...
2341
2082
Series1
15297
1
Powered by Bing
© GeoNames, Microsoft, TomTom

(b) Citizen Financial Cyber Fraud Reporting Management System during year 2023: In 2023, a total of 1,128,265 cyber fraud complaints were reported across India suggesting either a massive increase in cyber fraud or, more likely, improved reporting mechanisms through the Citizen Financial Cyber Fraud Reporting Management System.[14] Uttar Pradesh reported the highest number of complaints (197,547) in 2023, followed by Maharashtra (125,153) and Gujarat (121,701). This contrasts with the 2022 data where Telangana, Karnataka, and Uttar Pradesh were the top three states for cyber-crime cases. Major urban and tech-centric states like Maharashtra, Karnataka, and Delhi continue to report high numbers of cyber fraud cases, consistent with the 2022 cyber-crime data.

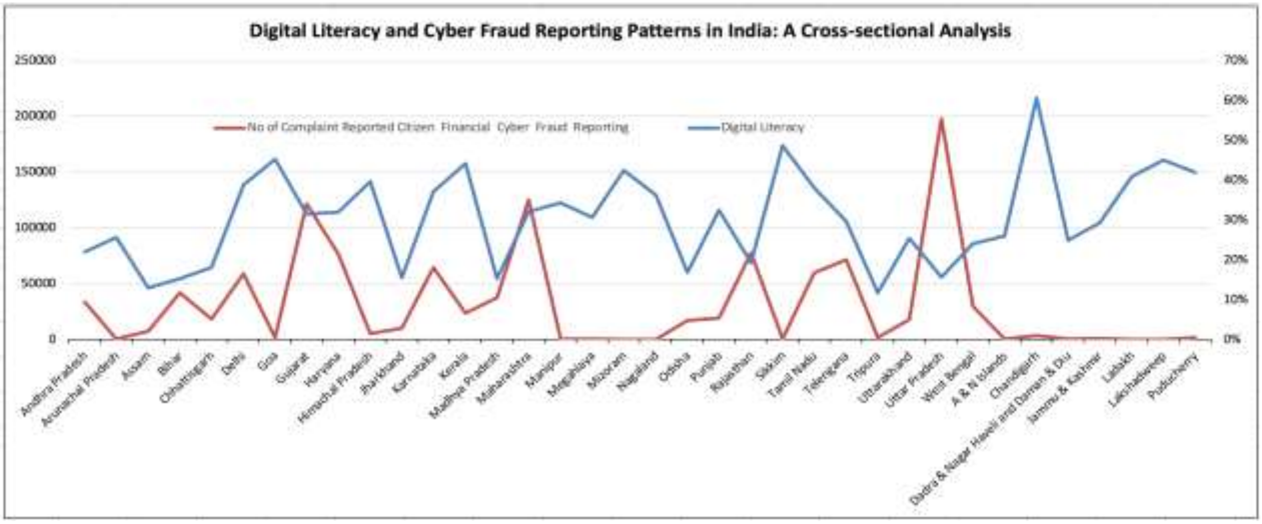

State/UT wise details of Citizen Financial Cyber Fraud Reporting Management System during the period 1.1.2023 to 31.12.2023
162
77769
19...
12...
37435
1...
1251...
7...
6...
33...
5...
No of Complaint Reported
197547
29
Powered by Bing
© GeoNames, Microsoft, TomTom

This comparison suggests that while the overall trend of increasing cyber incidents continues, the new reporting system for financial frauds has dramatically increased the number of reported incidents. It also highlights potential shifts in the geographical distribution of cyber crimes and frauds, possibly due to changes in reporting mechanisms or evolving patterns of cyber criminal activity.

## Digital Literacy and Cyber Fraud Reporting Patterns in India: A Cross-sectional Analysis of State-level Data

Digital Literacy is the ability of individuals and communities to understand and use digital technologies for meaningful actions within life situations. Simply it is the ability to access the computer/mobile/internet for our day-to-day activities and being connected with others through the internet. If at least one person in the household has the ability to operate a computer and use the internet (among individuals who are 5 years of age and older), it is defined as Digitally Literate Household. Only 38% of households in India are digitally literate. In urban areas, digital literacy is relatively higher at 61% as compared to just 25% in rural areas. [15]

The National Statistical Office (NSO) under the Ministry of Statistics and Programme Implementation conducted a Multiple Indicator Survey in India: Education & ICT Skills as part of the 78th round of National Sample Survey (NSS) from 2020– 2021(Report published in March 2023).[16] To ascertain the information and communication technology (ICT) skills of people, the survey asked respondents to self-report whether they could perform nine activities on a computer. In response to a set of questions, most participants indicated an inability to perform relatively routine tasks. Barely 25 per cent said they knew how to copy or move a file or folder, only 6 per cent said they could use basic arithmetic formulas in a spreadsheet, and a mere 5 per cent said they could create an electronic presentation using any software.



In order to explore the relationship between digital literacy (ability to copy or move a file or folder) and number of complaints reported through Citizen Financial Cyber Fraud Reporting Management System during year 2023 across different states and union territories in India, Pearson correlation coefficient was used as statistical tool.

Pearson correlation coefficient: The Pearson correlation coefficient is a measure of the linear correlation between two variables. It ranges from -1 to +1, where:

- +1 indicates a perfect positive linear correlation

- 0 indicates no linear correlation

- -1 indicates a perfect negative linear correlation

***Results:***

Pearson correlation coefficient is 0.2516 and P-value: 0.1390.

Mean Digital Literacy: 31.06%

Median Digital Literacy: 31.75%

Standard Deviation of Digital Literacy: 11.66

Mean Number of Complaints: 36,257

Median Number of Complaints: 17,958

Standard Deviation of Complaints: 49,593

***Interpretation:***

**a) Correlation:** The Pearson correlation coefficient of 0.2516 suggests a weak positive correlation between digital literacy rates and the number of complaints. This means that as digital literacy increases, there is a slight tendency for the number of complaints to increase as well, but the relationship is not strong.

**b) Statistical Significance:** The p-value of 0.1390 is greater than the conventional significance level of 0.05. This means that we cannot reject the null hypothesis that there is no correlation between digital literacy and the number of complaints. In other words, the observed weak positive correlation might be due to chance rather than a true relationship between the variables.

**c) Digital Literacy:** The standard deviation of 11.66 indicates considerable variation in digital literacy rates across different states/UTs.

**d) Complaints:** The mean number of complaints is 36,257, while the median is 17,958. The large difference between the mean and median suggests a right-skewed distribution, with some states having a very high number of complaints pulling the mean up. The high standard deviation (49,593) confirms the wide disparity in the number of complaints across different states/UTs.

**e) Additional Observations:** Some states/UTs have significantly higher numbers of complaints compared to others. For example, Uttar Pradesh has 197,547 complaints, while Lakshadweep has only 29. These outliers might be influencing the correlation results.

The analysis doesn't account for population differences between states/UTs. States with larger populations are likely to have more complaints simply due to their size, which might not necessarily correlate with digital literacy rates.

## Limitations:

**a) Non-linear Relationships:** The Pearson correlation only measures linear relationships. There might be non-linear relationships between digital literacy and complaints that are not captured by this analysis.

**b) Confounding Variables:** Factors such as population size, urbanization, economic development, and access to technology could be influencing both digital literacy rates and the number of complaints. A multiple regression analysis could help control for these factors.

**c) Time Series Data:** This analysis is based on a single snapshot. Analyzing how changes in digital literacy rates over time correlate with changes in complaint numbers could provide more insights.

It may be noted that while there is a weak positive correlation between digital literacy rates and the number of complaints across Indian states and UTs, this relationship is not statistically significant based on the available data. The analysis suggests that the relationship between digital literacy and cyber complaints is complex and likely influenced by various other factors not captured in this simple correlation analysis. Further, more comprehensive studies would be needed to draw definitive conclusions about the relationship between digital literacy and cyber complaint reporting in India.

## Conclusion

The analysis reveals several key insights about India's digital landscape and cyber fraud reporting patterns:

(a) Digital Infrastructure and Growth: India has emerged as a significant digital market with high tele-density (85.23%) and substantial broadband penetration (904.54 million subscriptions). There's a marked urban-rural divide in digital literacy (61% vs 25%). Digital payments have shown explosive growth, particularly in UPI adoption, with the RBI-DPI showing significant improvement (445.50 in March 2024 vs 100 in March 2018)

(b) Cyber Crime Patterns: Total cyber-crime cases increased by 31.7% from 2020 to 2022. Significant geographical variations exist, with tech-hub states reporting higher incidents.

(c) Digital Literacy and Fraud Correlation: A weak positive correlation (0.2516) exists between digital literacy rates and cyber fraud complaints. The relationship is not statistically significant (p-value: 0.1390). The relationship between digital literacy and cyber fraud reporting is complex and influenced by multiple factors beyond simple correlation.

These findings suggest the need for:

- Targeted interventions to bridge the digital literacy gap

- Enhanced cyber security awareness programs

- More comprehensive research incorporating multiple variables

- State-specific strategies considering local demographic and technological factors

The analysis underscores that while India is rapidly digitizing, there's a crucial need to balance digital adoption with adequate security measures and literacy programs to create a more resilient digital ecosystem.

**References:**

1. PricewaterhouseCoopers (PwC). (2023). "Combating Fraud in the Era of Digital Payments." Retrieved from https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/payments-transformation/combating-fraud-in-the-era-of-digital-payments.pdf

2. Reserve Bank of India (RBI). (2023). "Speech on Digital Payments Landscape." Retrieved from https://www.rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1422

Press Information Bureau (PIB). (2023). "Digital Payments Press Release." Retrieved from https://pib.gov.in/PressReleasePage.aspx?PRID=1973082

3. LexisNexis Risk Solutions. (2024). "Cybercrime Report 2024." Retrieved from https://risk.lexisnexis.com/global/en/about-us/press-room/press-release/20240522-cybercrime-report

4. Javelin Strategy & Research. (2023). "Global Digital Fraud Trends: Evaluating Past, Present, and Future." Retrieved from https://javelinstrategy.com/whitepapers/global-digital-fraud-trends-evaluating-past-present-and-future

5. Varalakshmi, D., Anusuyaa, S., Baheti, A., Dugar, P., Pentala, P., & Sethia, M. D. (2024). Cyber security in digital payments: An empirical study. Asian Journal of Management and Commerce, 5(1), 305-310.

6. Lonkar, A., Dharmadhikari, S., Dharurkar, N. V., Patil, K., & Phadke, R. A. (2024). Tackling digital payment frauds: A study of consumer preparedness in India. Journal of Financial Crime. https://doi.org/10.1108/jfc-01-2024-0029

7. Selvi, S. (2024). A Study on Cyber Frauds Post Digitalization in India. International Journal for Research in Applied Science and Engineering Technology. https://doi.org/10.22214/ijraset.2024.60191

8. Dahiya, K. (2023). Trends in Cyber Crime in India. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 11(5), 6393-6404. https://doi.org/10.22214/ijraset.2023.53073

9. India Brand Equity Foundation (IBEF). (n.d.). Indian Telecommunications Industry Analysis. Retrieved from https://www.ibef.org/industry/indian-telecommunications-industry-analysis-presentation

10. Telecom Regulatory Authority of India (TRAI). (n.d.). Telecom Subscriptions Reports. Retrieved from https://trai.gov.in/release-publication/reports/telecom-subscriptions-reports

11. Reserve Bank of India (RBI). (n.d.). ATM View. Retrieved from https://www.rbi.org.in/scripts/ATMView.aspx

12. Reserve Bank of India (RBI). (n.d.). Press Release Display. Retrieved from https://www.rbi.org.in/Scripts/ BS_PressReleaseDisplay.aspx?prid=58371

13. Lok Sabha. (n.d.). Questions Annex. Retrieved from https://sansad.in/getFile/loksabhaquestions/annex/1714/AU1432.pdf?source=pqals

14. Press Information Bureau (PIB). (n.d.). Press Release. Retrieved from pib.gov.in/PressReleaseIframePage.aspx?PRID=2003158

15. Central Board of Women Empowerment and Development (CBWED). (n.d.). Digital Literacy Report. Retrieved from https://dtnbwed.cbwe.gov.in/images/upload/Digital-Literacy_3ZNK.pdf

16. Ministry of Statistics and Programme Implementation. (2021). 78th Round of National Sample Survey: Multiple Indicator Survey in India. Retrieved from https://www.mospi.gov.in/sites/default/files/publication_reports/MultipleIndicatorSurveyinIndiaf.pdf

**Annex**

**Digital Literacy and Cyber Fraud Reporting Patterns in India**

| State/UT | Digital Literacy* | No of Complaint Reported Citizen Financial Cyber Fraud Reporting |
|---|---|---|
| Andhra Pradesh | 22.00% | 33507 |
| Arunachal Pradesh | 25.60% | 470 |
| Assam | 12.90% | 7621 |
| Bihar | 15.30% | 42029 |
| Chhattisgarh | 18.10% | 18147 |
| Delhi | 38.80% | 58748 |
| Goa | 45.30% | 1788 |
| Gujarat | 31.50% | 121701 |
| Haryana | 32.00% | 76736 |
| Himachal Pradesh | 39.60% | 5268 |
| Jharkhand | 15.50% | 10040 |
| Karnataka | 37.10% | 64301 |
| Kerala | 44.10% | 23757 |
| Madhya Pradesh | 15.30% | 37435 |
| Maharashtra | 32.10% | 125153 |
| Manipur | 34.30% | 339 |
| Megahlaya | 30.60% | 654 |
| Mizoram | 42.50% | 239 |
| Nagaland | 36.20% | 224 |
| Odisha | 16.80% | 16869 |
| Punjab | 32.50% | 19252 |
| Rajasthan | 19.30% | 77769 |
| Sikkim | 48.70% | 292 |
| Tamil Nadu | 38.00% | 59549 |
| Telengana | 29.60% | 71426 |
| Tripura | 11.70% | 1913 |
| Uttarakhand | 25.40% | 17958 |
| Uttar Pradesh | 15.60% | 197547 |
| West Bengal | 24.00% | 29804 |
| A & N Islands | 26.00% | 526 |
| Chandigarh | 60.60% | 3601 |
| Dadra & Nagar Haveli and Daman & Diu | 24.90% | 412 |
| Jammu & Kashmir | 29.30% | 1046 |
| Ladakh | 40.90% | 162 |

| | | |
|---|---|---|
| Lakshadweep | 45.00% | 29 |
| Puducherry | 42.00% | 1953 |
| All-India | 24.60% | 1128265 |

*- ability to copy or move a file or folder