Evolving Fraud Trends in India's Banking and Payment Systems: A Decadal Analytical Study

[1]Aayushi Bohra
[1]Independent Researcher
[1]MBA (BK School)

***Abstract*—The rapid expansion of digital banking and payment systems in India has significantly transformed financial transactions, enhancing convenience, speed, and accessibility. However, this digital evolution has also increased exposure to financial fraud, making fraud detection and prevention a critical concern for financial institutions and regulators. This study, titled "An Analytical Study of Fraud Trends in Banking and Payment Systems," aims to examine the patterns and trends of fraud in relation to the growth of digital transactions.**

The research is based on secondary data collected from reliable sources such as the Reserve Bank of India (RBI) and the National Payments Corporation of India (NPCI), covering a period from 2014–15 to 2023–24. Various analytical tools, including trend analysis, year-on-year growth analysis, comparative analysis, and forecasting techniques, have been employed to evaluate changes in fraud cases, fraud amounts, and digital transaction volumes.

The findings reveal a substantial increase in digital transactions over the study period, reflecting widespread adoption of digital payment platforms such as UPI, mobile banking, and internet banking. At the same time, fraud trends exhibit fluctuations and evolving patterns, indicating the dynamic nature of financial fraud in a technology-driven environment.

Index Terms*—*Digital Banking, Financial Fraud, Fraud Trends, Digital Payments, UPI, Cybersecurity, Banking Sector, Fraud Detection, RBI, NPCI

I. Introduction

In recent years, the Indian banking and financial system has undergone a significant transformation driven by rapid digitalization. The adoption of digital payment platforms such as mobile banking, internet banking, and Unified Payments Interface (UPI) has led to a substantial increase in the volume and value of financial transactions. Government initiatives promoting a cashless economy, along with increasing smartphone penetration and internet accessibility, have further accelerated this shift toward digital financial services.

Despite the rapid growth of digital transactions in India, financial fraud continues to evolve in complexity and scale. There is a lack of comprehensive understanding of how fraud trends have changed over time in relation to the growth of digital payment systems.

Many financial institutions face challenges in identifying patterns of fraud, predicting future risks, and implementing effective prevention strategies. Additionally, there is limited empirical research that connects the growth of digital transactions with the changing nature of fraud in the Indian banking system.

Research Design:

The study uses a descriptive and analytical research design to examine fraud trends in banking and payment systems. It focuses on understanding the relationship between digital transaction growth and financial fraud. A quantitative approach is adopted, as the study is based on numerical data such as fraud cases, fraud amounts, and digital transaction volume. The research is based on secondary data collected from reliable sources such as RBI reports, NPCI data, and other published financial reports.

The study applies time-series analysis to examine data over a period of ten years (2014–15 to 2023–24). Various statistical and analytical tools such as trend analysis, growth rate analysis, and comparative analysis are used to interpret the data.

II. DATA ANALYSIS

DESCRIPTIVE STATISTICS

The data analysis is based on secondary data related to fraud cases, fraud amounts, and digital transactions in India. Statistical and analytical tools are used to identify trends, relationships, and patterns.

Trend Analysis

Trend analysis examines how key variables such as fraud cases and digital transactions have evolved over time. It helps in identifying long-term patterns and overall direction of change. This test is useful to understand the impact of increasing digitalisation on fraud behaviour.

Table 1 Trend Analysis of Fraud Cases

Year	Fraud Cases (No.)
2014-15	18,500
2015-16	23,933
2016-17	25,152
2017-18	5,835
2018-19	8,850
2019-20	9,600
2020-21	10,800
2021-22	9,103
2022-23	13,530
2023-24	36,075

Figure 1 Trend Analysis-Fraud Cases(No.)

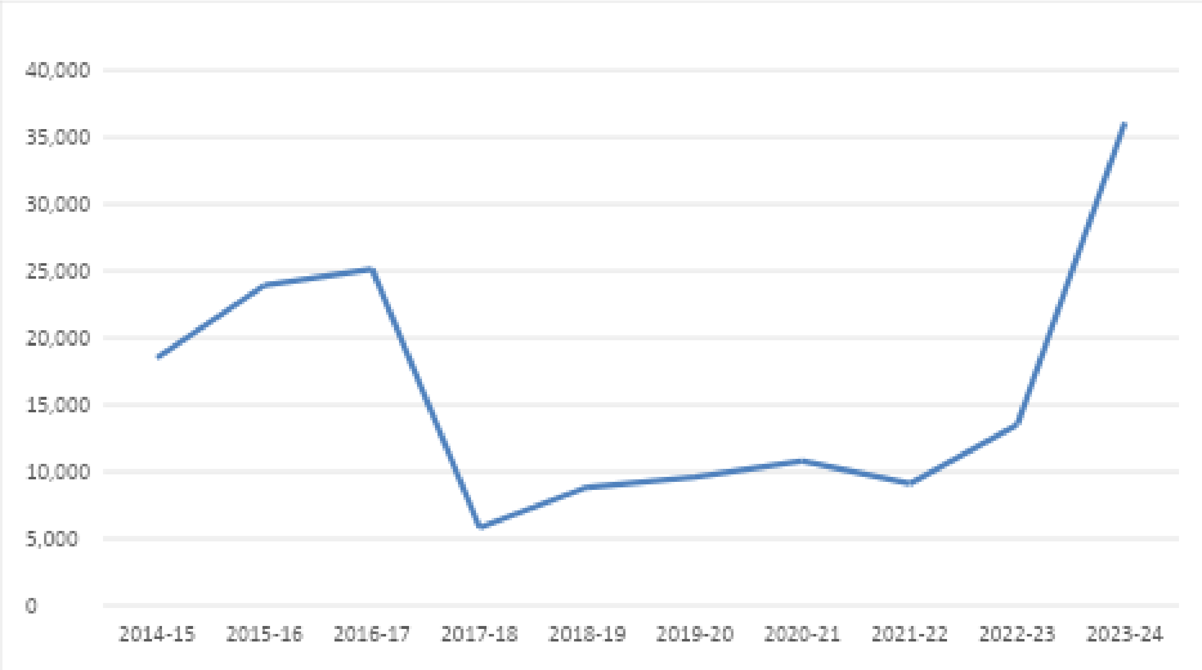


Table 2 Trend Analysis of Fraud Amount

Year	Fraud Amount (₹ Cr)
2014-15	10,200
2015-16	132500
2016-17	41,167
2017-18	41,000
2018-19	71,500
2019-20	105000
2020-21	138000
2021-22	60,414
2022-23	30,252
2023-24	42,000

Figure 2 Fraud Amount (Cr.)

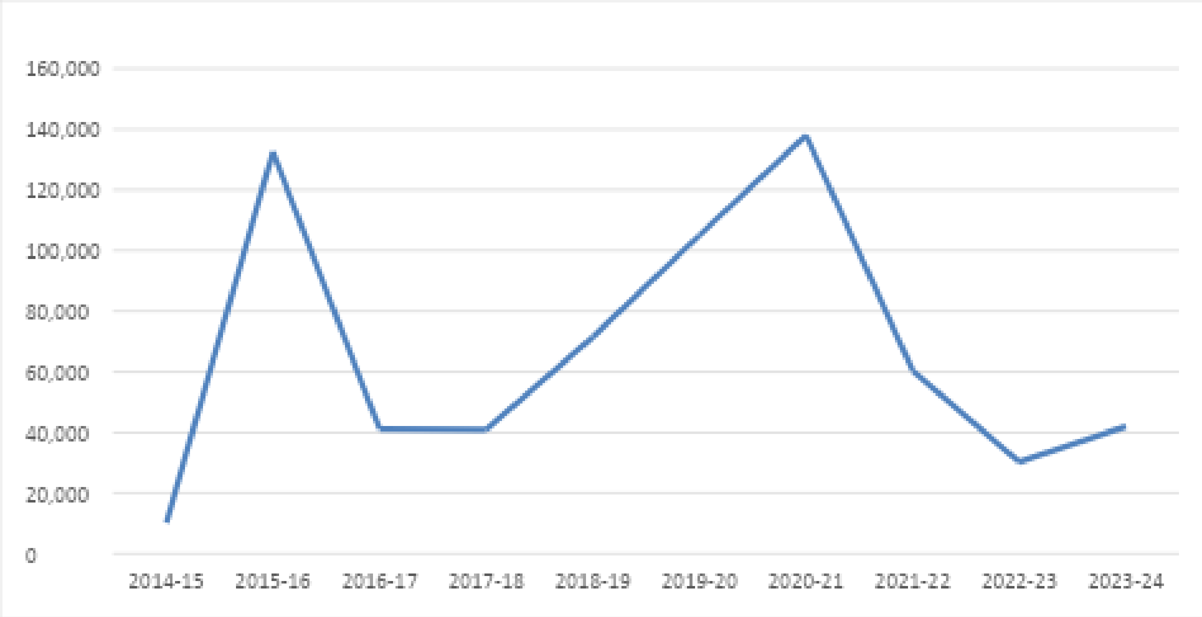


Table 3 Trend Analysis of Total Digital Transactions(No.)

Year	Total Digital Transactions (No.) (Crore)
2014-15	168.74
2015-16	360
2016-17	1,095
2017-18	1,589
2018-19	2,330
2019-20	3,400
2020-21	4,850
2021-22	8840
2022-23	13,462
2023-24	18,737

Figure 3 Trend Analysis-Total Digital Transactions (No.)

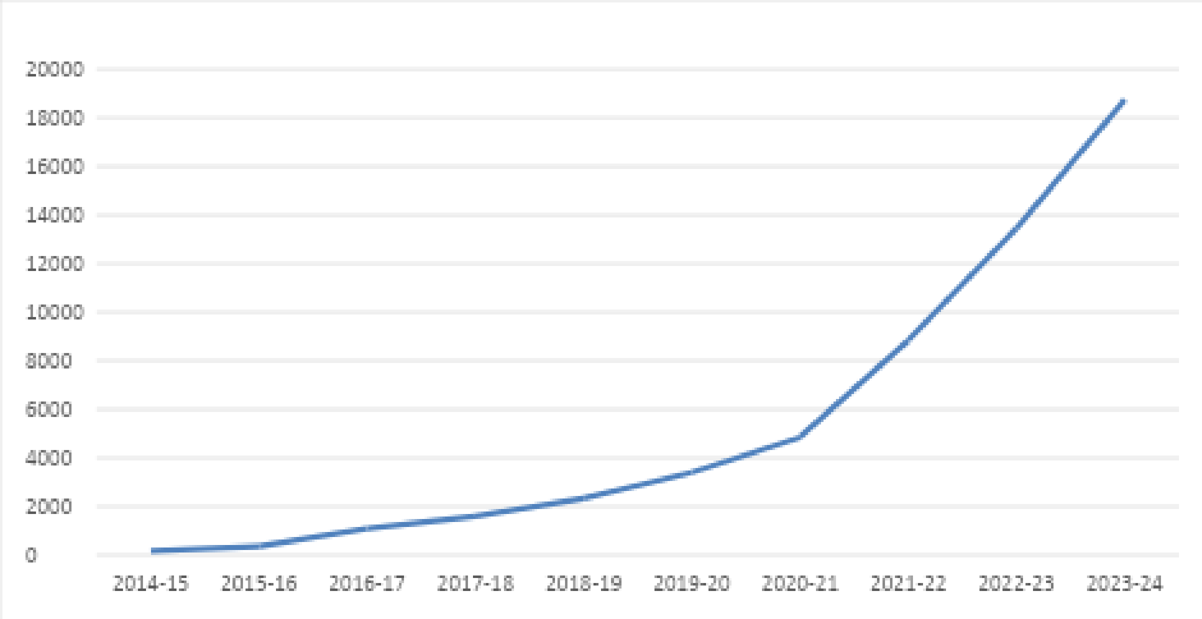
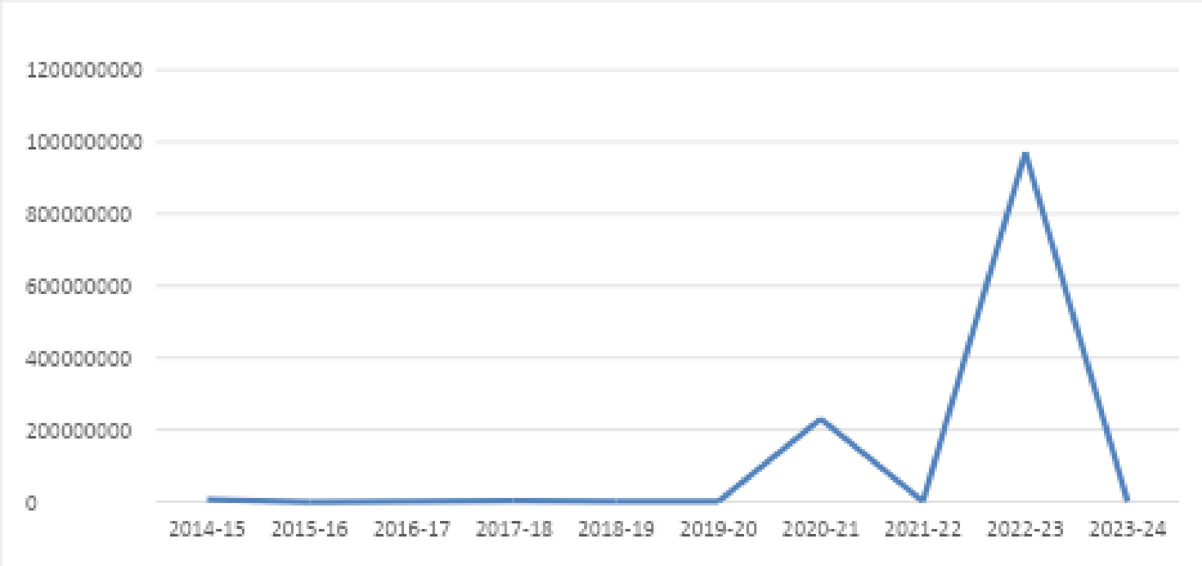


Table 4 Trend Analysis of Total Digital Transactions (Rs.)

Year	Total Digital Transactions (₹ Cr)
2014-15	6536550
2015-16	0.92
2016-17	109646
2017-18	2527539
2018-19	146,000
2019-20	190,000
2020-21	230,000,000
2021-22	690000
2022-23	970000000
2023-24	1250000

Figure 4 Trend Analysis- Total Digital Transactions (Cr)



The trend analysis clearly highlights the structural transformation of India's banking and payment systems over the study period. Digital transactions show a strong and consistent upward trajectory, particularly after 2018–19, reflecting rapid digital adoption, policy push towards cashless payments, and the widespread use of platforms such as UPI. The exponential rise in both transaction volume and value indicates a shift in consumer behaviour towards high-frequency digital payments.

In contrast, fraud cases do not follow a similar smooth upward trend. Instead, fraud cases show intermittent spikes and moderation phases, suggesting that fraud does not grow mechanically with transaction volumes. Certain years exhibit sharp increases in fraud cases, while others show stabilization or even decline. This divergence implies that while digital exposure has expanded significantly, fraud control mechanisms have simultaneously strengthened.

Fraud amount trends further reinforce this observation. Although there are years with exceptionally high fraud values, these spikes are not sustained over time. The absence of a consistent upward trend in fraud amounts, despite massive transaction growth, indicates improvements in detection, monitoring, and containment of fraud incidents. This trend-level behaviour supports the argument that technology-driven monitoring systems and improved transaction surveillance have contributed to better fraud management outcomes.

YoY Growth Rate

YoY growth analysis measures the annual percentage change in variables. It captures short-term fluctuations and highlights periods of acceleration or decline. This test helps identify stress years and control phases.

Table 5 Growth Rate of Digital Transactions(No.)

Year	Digital Transactions (No.)	YoY%
2014-15	168.74	-
2015-16	360	113.3459761
2016-17	1,095	204.2222222
2017-18	1,589	45.06939372
2018-19	2,330	46.65156093
2019-20	3,400	45.92274678
2020-21	4,850	42.64705882

2021-22	8840	82.26804124
2022-23	13,462	52.28506787
2023-24	18,737	39.18437082

Table 6 Growth Rate of Digital Transactions (Rs.)

Digital Transactions (Value)	YoY%
6536550	-
0.92	-99.99998593
109646	11917943.48
2527539	2205.18122
146,000	-94.22363018
190,000	30.1369863
230,000,000	120952.6316
690000	-99.7
970000000	140479.7101
1250000	-99.87113402

Table 7 Growth Rate of Fraud Cases

Fraud Cases	YoY%
18,500	-
23,933	29.36756757
25,152	5.093385702
5,835	-76.80104962
8,850	51.67095116
9,600	8.474576271
10,800	12.5
9,103	-15.71296296
13,530	48.63231902
36,075	166.6297118

Table 8 Growth Rate of Fraud Amount

Fraud Amount	YoY%
10,200	-
132500	1199.019608
41,167	-68.93056604
41,000	-0.405664731
71,500	74.3902439
105000	46.85314685
138000	31.42857143
60,414	-56.22173913
30,252	-49.92551395
42,000	38.83379611

The year-on-year (YoY) growth analysis provides deeper insight into short-term volatility and stress periods. Digital transactions exhibit consistently high YoY growth rates across most years, with particularly strong acceleration during periods of rapid UPI adoption and post-pandemic digital reliance. This confirms that digital payment growth has been structural rather than cyclical.

Fraud cases, however, display high volatility in YoY growth, including years of negative growth followed by sharp spikes. Such behaviour suggests that fraud occurrence is episodic rather than linear. Sudden increases in fraud cases may be associated with new fraud techniques, regulatory reporting changes, or transitional phases in payment systems. Conversely, negative growth years indicate periods where fraud control measures may have outperformed fraud attempts.

Similarly, YoY growth in fraud amount is highly unstable, with extreme positive and negative values. This reflects the fact that fraud severity fluctuates independently of fraud frequency. A relatively small number of high-value fraud cases can inflate fraud amounts in certain years. This finding highlights the importance of advanced monitoring systems focus not only on transaction volume but also on identifying high-value suspicious activities.

Overall, YoY analysis reinforces the need for adaptive and dynamic fraud detection systems, as static rule-based approaches would be insufficient to manage such volatility.

Comparative Analysis

A. Fraud Type Analysis

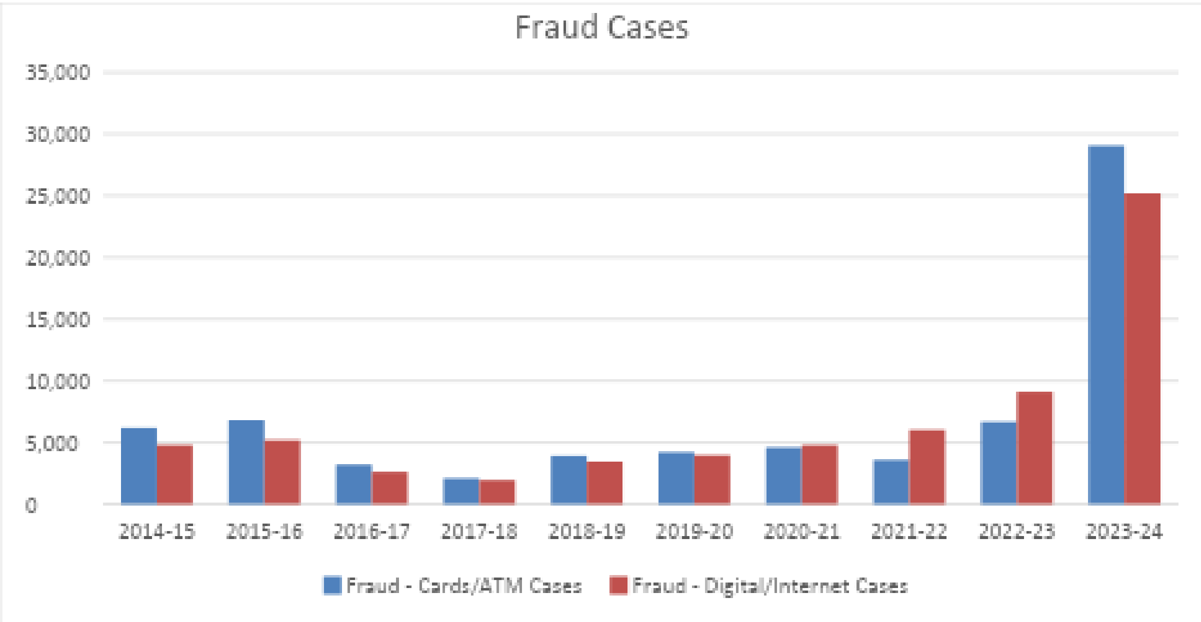
Comparative analysis compares different categories of fraud to identify shifts in fraud patterns. It helps understand how fraud behaviour changes with evolving transaction channels.

Table 9 Comparison using Fraud Cases

Year	Fraud - Cards/ATM Cases	Fraud - Digital/Internet Cases
2014-15	6,200	4,800
2015-16	6,800	5,200
2016-17	3,200	2,600

2017-18	2,100	1,950
2018-19	3,900	3,450
2019-20	4,200	3,950
2020-21	4,600	4,800
2021-22	3,596	6,030
2022-23	6,659	9,089
2023-24	29,082	25,219

Figure 5 Comparison Using Fraud Cases



The comparative analysis between card/ATM fraud and digital/internet fraud reveals a clear shift in fraud patterns over time. In the earlier years of the study, card and ATM-related fraud formed a significant portion of total fraud cases. However, as digital transactions expanded, digital and internet-based fraud cases began to dominate.

In recent years, digital fraud cases account for a substantially larger share of total fraud, reflecting increased online transaction activity and changing fraudster behaviour. Fraudsters increasingly target digital channels due to higher transaction frequency, anonymity, and speed. This structural shift indicates that fraud risk has moved from physical payment instruments to real-time digital ecosystems.

The comparison of fraud amounts further shows that digital fraud not only occurs more frequently but also involves higher financial exposure in recent years. This trend emphasizes that fraud detection strategies must prioritise real-time digital monitoring rather than relying predominantly on traditional card-based controls.

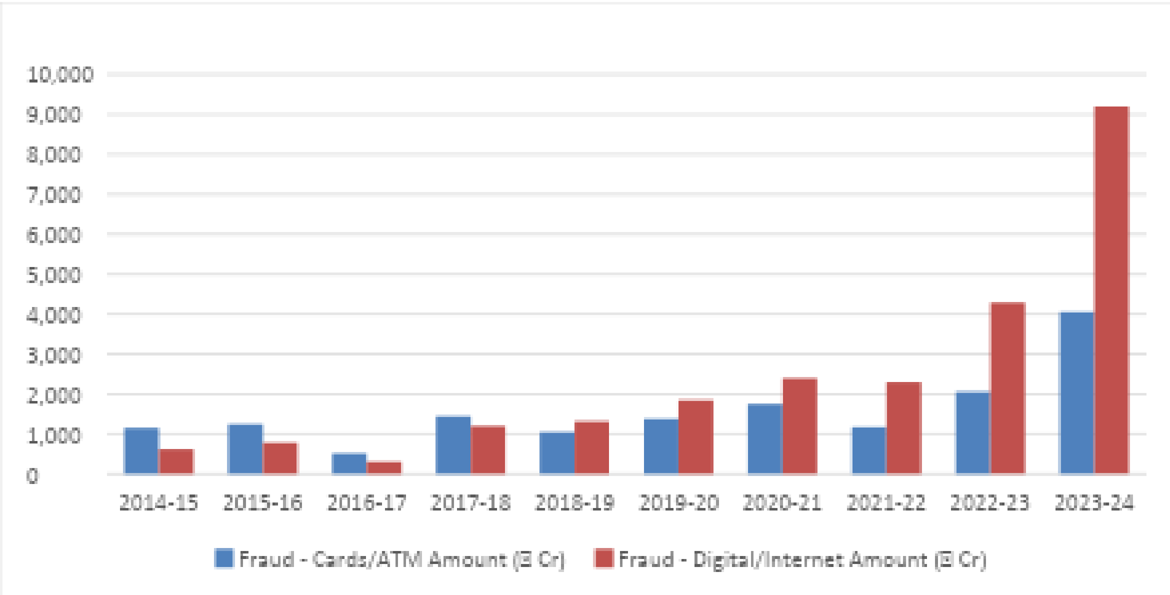
Comparison Using Fraud Amounts

This analysis compares fraud volume (number of cases) with fraud value (amount involved). It distinguishes between frequency of fraud and financial severity.

Table 10 Comparison using Fraud Amounts

Year	Fraud - Cards/ATM Amount (₹ Cr)	Fraud - Digital/Internet Amount (₹ Cr)
2014-15	1,150	620
2015-16	1,250	780
2016-17	520	310
2017-18	1,450	1,200
2018-19	1,050	1,320
2019-20	1,380	1,850
2020-21	1,750	2,400
2021-22	1,173	2,296
2022-23	2,058	4,301
2023-24	4,056	9,205

Figure 6 Comparison Using Fraud Amount



While fraud cases show moderate growth, fraud amounts display significant variations across different years. Digital and internet fraud contributes an increasingly larger share of total fraud value, particularly in recent years. This indicates that digital fraud is not only more frequent but also financially more severe compared to traditional card-based fraud.

The presence of high-value fraud cases in digital channels suggests that fraudsters increasingly exploit online transaction platforms due to their speed, accessibility, and high transaction volumes. Even a small number of large-value fraud incidents can significantly increase the overall fraud amount. This distinction between fraud frequency and fraud severity highlights the need for stronger transaction monitoring systems and improved fraud risk management practices within banking and digital payment systems.

B. Pre vs Post Phase Comparison

Pre vs post analysis compares performance before and after a major structural shift. It is used to assess the impact of digitalisation and technology adoption.

Table 11 Pre vs Post Phase Comparison

Phase	Average Digital Transactions	Average Fraud Cases
Pre (2014-19)	3,600	16,454
Post (2019-24)	9,818	15,822
% change between phases	172.7111111	-3.843442324

Figure 7 Pre vs Post Phase Comparison- Average Digital Transactions

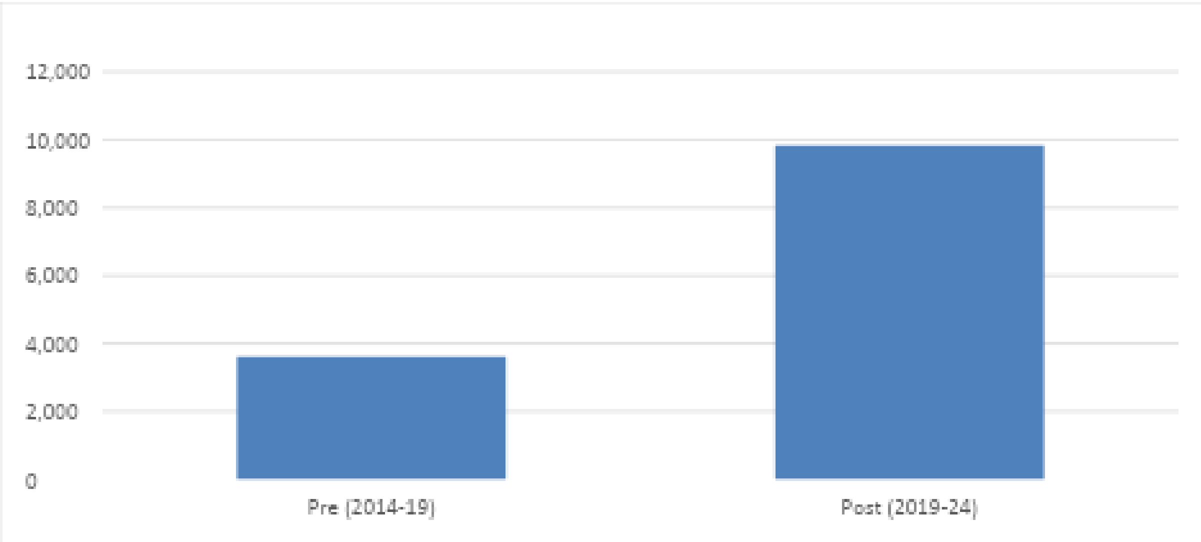
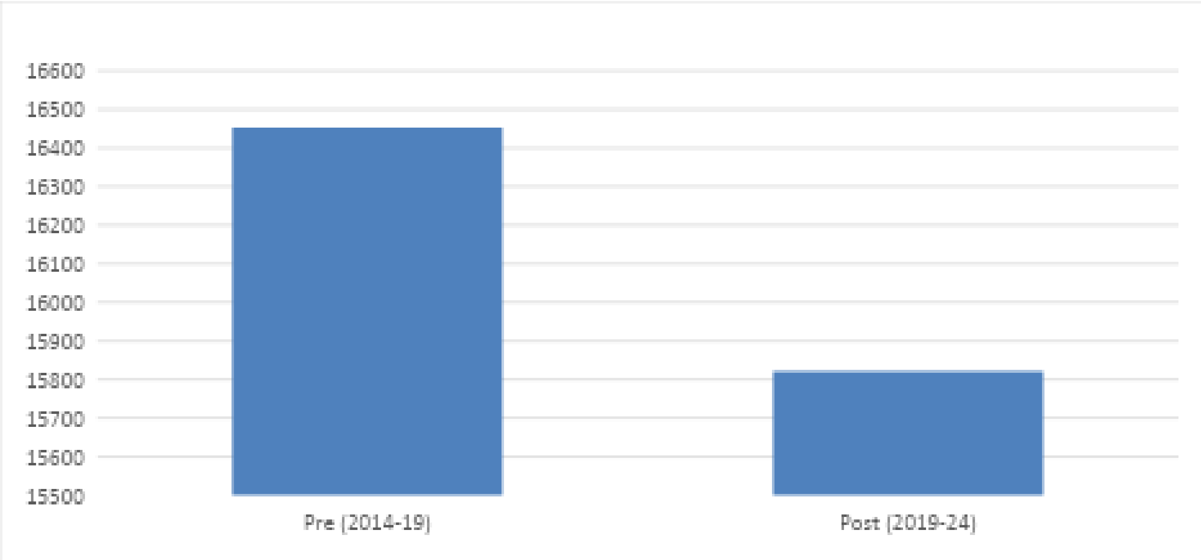


Figure 8 Pre vs Post Phase Comparison- Average Fraud Cases



$$\text{Avg Fraud Value} = \frac{\text{Fraud Amount}}{\text{Fraud Cases}}$$

Fraud Rate	
Pre	4.570555556
Post	1.611554759

$$\%\ \text{Change} = \frac{\text{Post Avg} - \text{Pre Avg}}{\text{Pre Avg}} \times 100$$

The pre- and post-digitalisation comparison provides strong evidence of improved fraud management efficiency. The post-digitalisation phase records a substantial increase in average digital transactions, while average fraud cases show only marginal change. This indicates that fraud growth has not kept pace with transaction growth.

More importantly, the fraud rate (fraud cases per unit of transaction volume) declines significantly in the post phase. This decline suggests that each additional digital transaction carries lower incremental fraud risk compared to earlier periods. Such an outcome would be difficult to achieve without improvements in detection capability, monitoring speed, and analytical sophistication.

This phase-wise improvement strongly supports the role of technology-led interventions, including improved monitoring systems, real-time alerts, behavioural analysis, and automated controls have reduced systemic fraud vulnerability.

Descriptive Statistics

Descriptive statistics summarise data using measures such as mean, median, and standard deviation. They help understand the typical level and variability of fraud-related indicators.

Table 12 Descriptive Statistics

Statistic	Fraud Cases	Digital Fraud Cases	Fraud Amount
Mean	16137.8	6708.8	67203.3
Median	12165	4800	51207
Standard Deviation	9614.090144	6799.316204	43948.78519
Minimum	5835	1950	10200
Maximum	36075	25219	138000
Range	30240	23269	127800

The descriptive statistics reveal a high degree of variability in fraud-related indicators. The large gap between mean and median values for fraud cases and fraud amount indicates the presence of extreme values in certain years. This confirms that fraud distribution is skewed rather than normally distributed, with occasional high-impact events influencing averages.

The high standard deviation further highlights the unpredictable nature of fraud behaviour. Such variability makes manual monitoring and static thresholds less effective. These findings highlight the importance of continuously improving transaction monitoring systems and risk management practices.

Visualization Based Insights

Visualization-based analysis uses charts to identify patterns and relationships in data. It simplifies complex trends and highlights divergence or convergence visually.

- Trend Line Visuals

Table 13 Trend Line Visuals- Fraud Digital/Internet Cases

Year	Fraud - Digital/Internet Cases
2014-15	4,800
2015-16	5,200
2016-17	2,600
2017-18	1,950
2018-19	3,450
2019-20	3,950
2020-21	4,800
2021-22	6,030
2022-23	9,089
2023-24	25,219

Figure 9 Trend Line Visuals- Fraud - Digital/Internet Cases

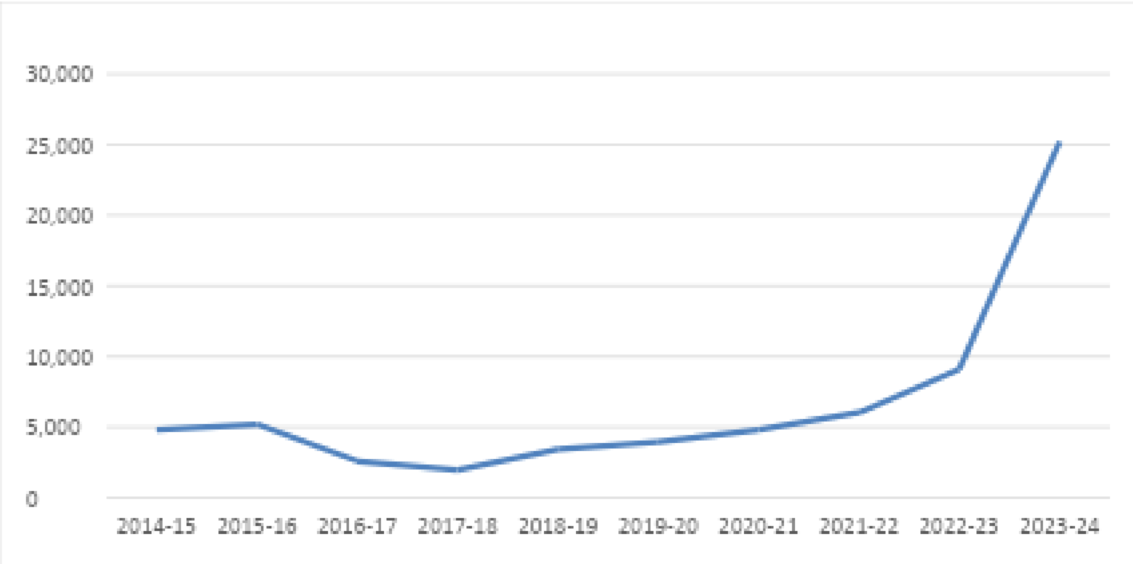
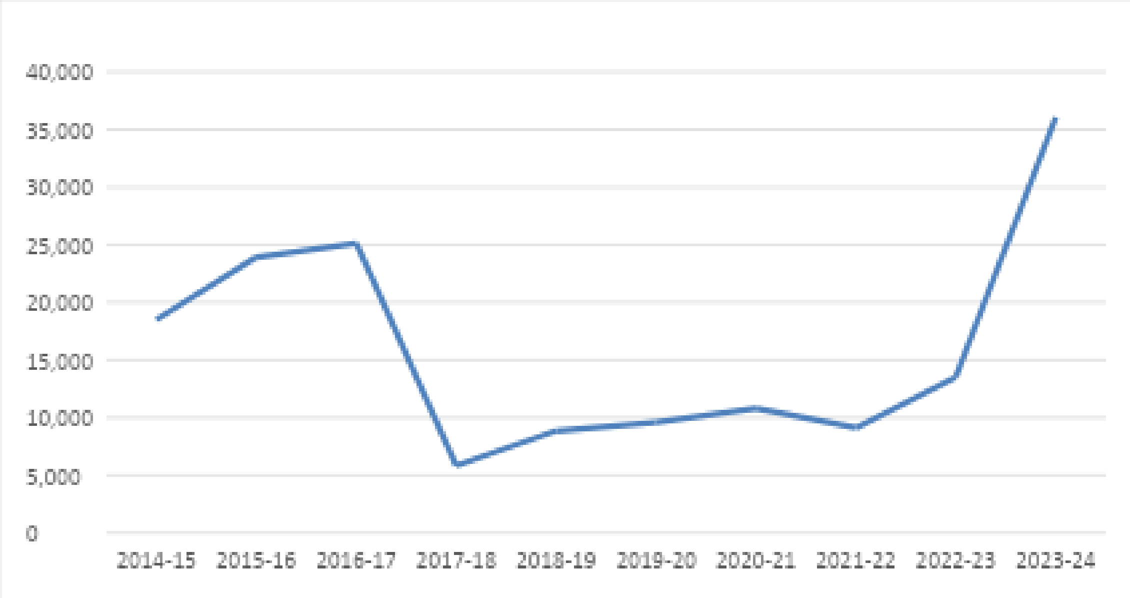


Table 14 Trend Line Visuals- Fraud Cases(No.)

Year	Fraud Cases (No.)
2014-15	18,500
2015-16	23,933
2016-17	25,152
2017-18	5,835
2018-19	8,850
2019-20	9,600
2020-21	10,800

2021-22	9,103
2022-23	13,530
2023-24	36,075

Figure 10 Trend Line Visuals- Fraud Cases (No.)



Visual trend comparisons between digital transactions and fraud cases show a clear divergence in growth paths. While transaction curves rise steeply, fraud curves display flatter trajectories with intermittent spikes. This visual divergence reinforces the numerical evidence that fraud control efficiency has improved over time.

Similarly, visualization of digital fraud cases shows acceleration in later years but still not proportional to transaction growth. This suggests that although fraud attempts have increased with digital adoption, containment mechanisms have scaled alongside system growth.

C. CAGR Based Visualization Insight

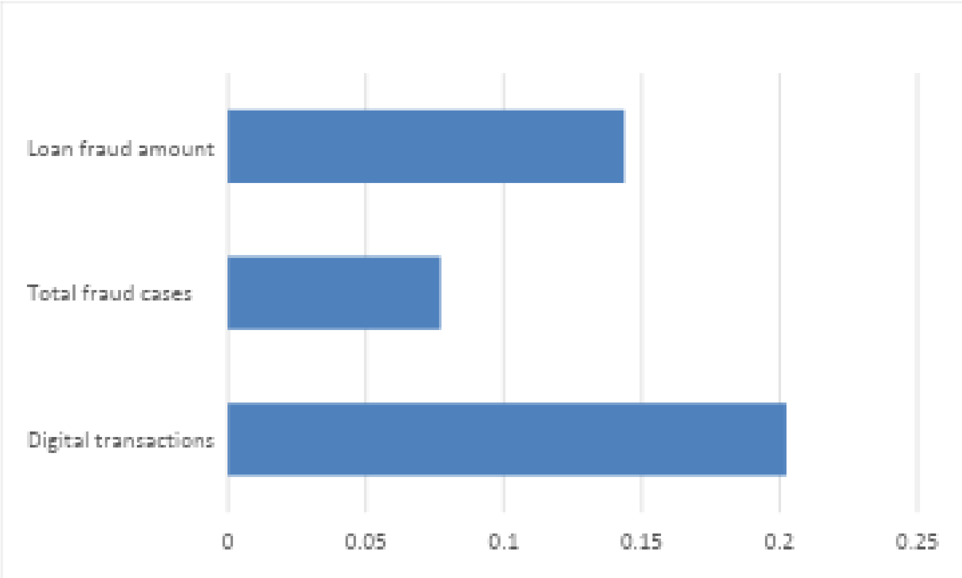
CAGR measures the average annual growth over the entire study period. It provides a smoothed long-term growth perspective.

Table 15 CAGR Based Visualization Insight

Variable	CAGR
Digital transactions	0.202414125
Total fraud cases	0.077025703
Loan fraud amount	0.143658679

$$\text{CAGR} = \left(\frac{\text{End Value}}{\text{Start Value}}\right)^{1/n} - 1$$

Figure 11 CAGR



The Compound Annual Growth Rate (CAGR) analysis provides a long-term and smoothed view of growth trends by eliminating short-term fluctuations and volatility. In the present study, CAGR has been calculated for key variables such as digital transactions and fraud-related indicators to understand their average annual growth over the entire study period.

The results indicate that digital transactions have recorded a significantly higher CAGR compared to total fraud cases. This suggests that the expansion of digital payment systems in India has been rapid and sustained, driven by factors such as increased smartphone penetration, UPI adoption, policy support for digital payments, and changing consumer behaviour.

In contrast, the comparatively lower CAGR of fraud cases implies that fraud has not expanded at the same pace as digital transaction activity. Despite a substantial increase in transaction volume and value, fraud growth has remained relatively contained over the long term. This divergence between the growth rates of transactions and fraud indicates an improvement in the overall efficiency of fraud detection and prevention mechanisms.

The CAGR analysis therefore highlights that system-level fraud risk has reduced in proportional terms, even though absolute fraud incidents still occur. This trend supports the role of advanced monitoring systems, including advanced analytics and behavioural monitoring systems have helped scale fraud control capabilities. From a policy and operational perspective, the findings suggest that technological interventions have helped maintain financial system stability in a rapidly digitalising environment.

D. Slope Change/ Inflection Visualization

Slope change analysis identifies changes in growth momentum over time. It helps detect acceleration or deceleration phases.

Table 16 Slope Change

Period	Years	Digital fraud cases
Pre	2014–15 to 2018–19	-337.5

Post	2019–20 to 2023–24	5317.25

Pre slope < Post slope → acceleration

$$\text{Slope} = \frac{\text{End Value} - \text{Start Value}}{\text{Number of Years}}$$

Slope change or inflection analysis examines changes in the momentum and direction of growth over different time periods. Unlike CAGR, which provides a long-term average, slope analysis captures shifts in trend behaviour and helps identify acceleration or deceleration phases in fraud occurrence.

The results of the slope change analysis show a clear difference between the earlier and later phases of the study period. During the initial phase, fraud-related indicators exhibit higher volatility and uneven growth patterns, reflecting a period of transition in digital payment adoption and relatively weaker monitoring frameworks. This phase is characterised by sharp fluctuations and sudden changes in fraud behaviour.

In the later phase, although digital transactions continue to grow rapidly, the slope of fraud growth shows signs of moderation and stabilisation. This change in slope indicates that fraud growth momentum has slowed relative to transaction growth. Such a pattern suggests improved system responsiveness and the effectiveness of real-time surveillance mechanisms.

The observed inflection in fraud trends can be associated with the increasing use of data analytics, machine learning-based fraud detection, enhanced regulatory oversight, and improved transaction monitoring capabilities. Slope change analysis thus provides strong evidence that fraud detection systems have evolved from reactive controls to more proactive and adaptive frameworks.

Overall, the slope change findings reinforce the conclusion that technological and analytical improvements particularly improved fraud monitoring systems and regulatory oversight have helped stabilize fraud growth trends, even in an environment of rapidly expanding digital transactions.

E. Growth Rate Divergence Visualization

This test compares growth rates of related variables to assess proportionality. It helps evaluate whether fraud growth keeps pace with transaction growth.

Table 17 Growth Divergence Table

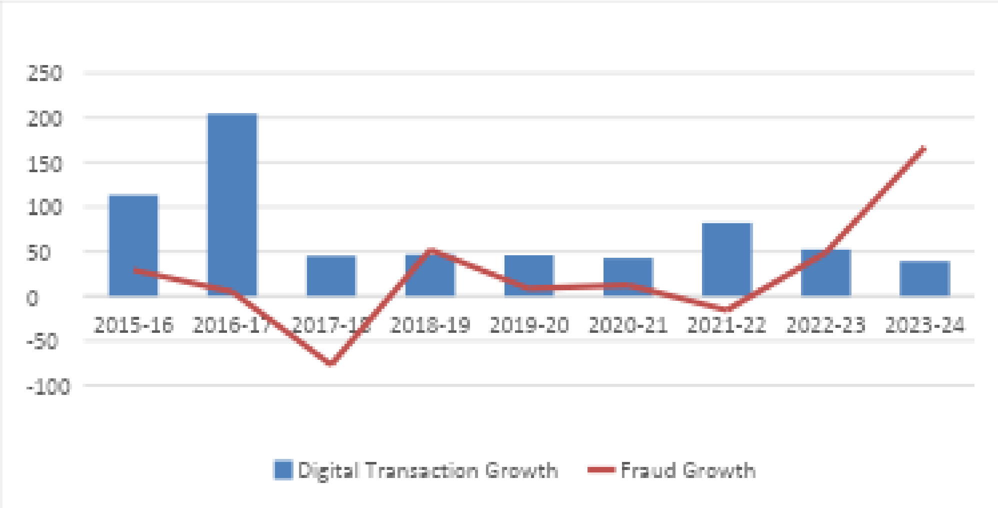
Year	Digital Transaction Growth	Fraud Growth	Growth Gap %
2014-15	-	-	-
2015-16	113.3459761	29.36756757	83.97840849
2016-17	204.2222222	5.093385702	199.1288365
2017-18	45.06939372	-76.80104962	121.8704433
2018-19	46.65156093	51.67095116	-5.01939023
2019-20	45.92274678	8.474576271	37.44817051
2020-21	42.64705882	12.5	30.14705882
2021-22	82.26804124	-15.71296296	97.9810042

2022-23	52.28506787	48.63231902	3.652748858
2023-24	39.18437082	166.6297118	-127.4453409

Positive gap → Transactions growing faster than fraud

Negative gap → Fraud growing faster than transactions

Figure 12 Growth Rate Divergence



Growth rate divergence analysis compares the rate of growth in digital transactions with the growth rate of fraud cases in order to understand whether fraud increases proportionately with transaction activity. The results show that in most years digital transaction growth is significantly higher than fraud growth, resulting in a positive growth gap. This indicates that although the volume of digital transactions has increased rapidly, fraud incidents have not expanded at the same pace.

In certain years, the divergence gap becomes smaller or negative, meaning fraud growth temporarily exceeds transaction growth. Such situations may occur when new payment technologies are introduced, when user behavior changes rapidly, or when fraudsters exploit emerging vulnerabilities in digital platforms. However, these phases are usually temporary and are followed by stabilization in fraud trends.

Overall, the widening divergence in later years suggests that improvements in transaction monitoring systems, regulatory supervision, and fraud prevention mechanisms have helped control fraud risks despite the rapid expansion of digital payment systems.

Time Series Turning Point/Inflection Point Analysis

Turning point analysis identifies years where trend direction or behaviour changes significantly. It helps detect structural shifts in data.

Table 18 Time Series Turning Point- Fraud Cases (No.)

Year	Fraud Cases (No.)
2014-15	18,500
2015-16	23,933

2016-17	25,152
2017-18	5,835
2018-19	8,850
2019-20	9,600
2020-21	10,800
2021-22	9,103
2022-23	13,530
2023-24	36,075

Figure 13 Time Series Turning Point- Fraud Cases (No.)

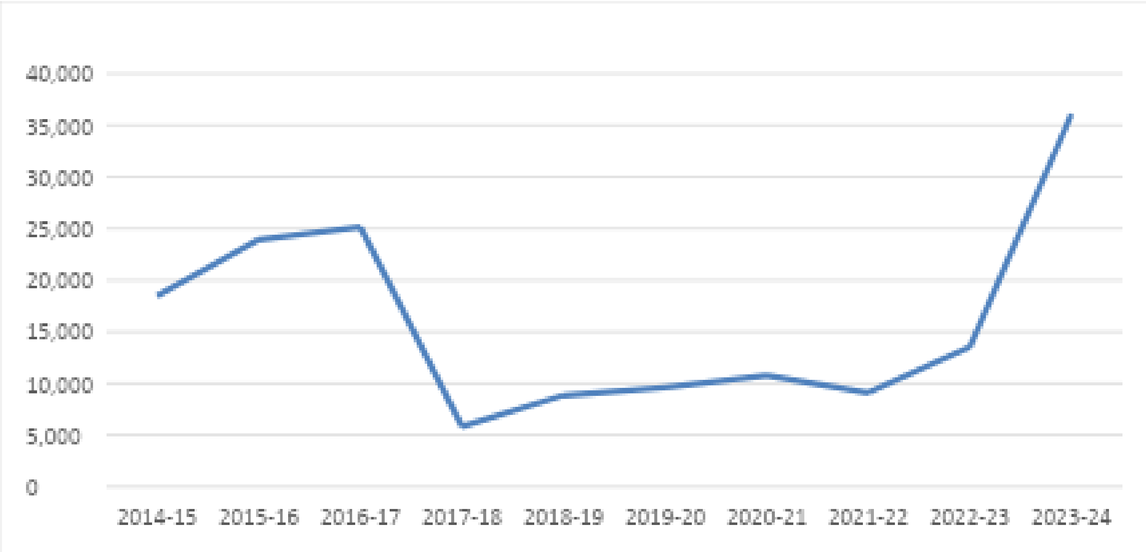
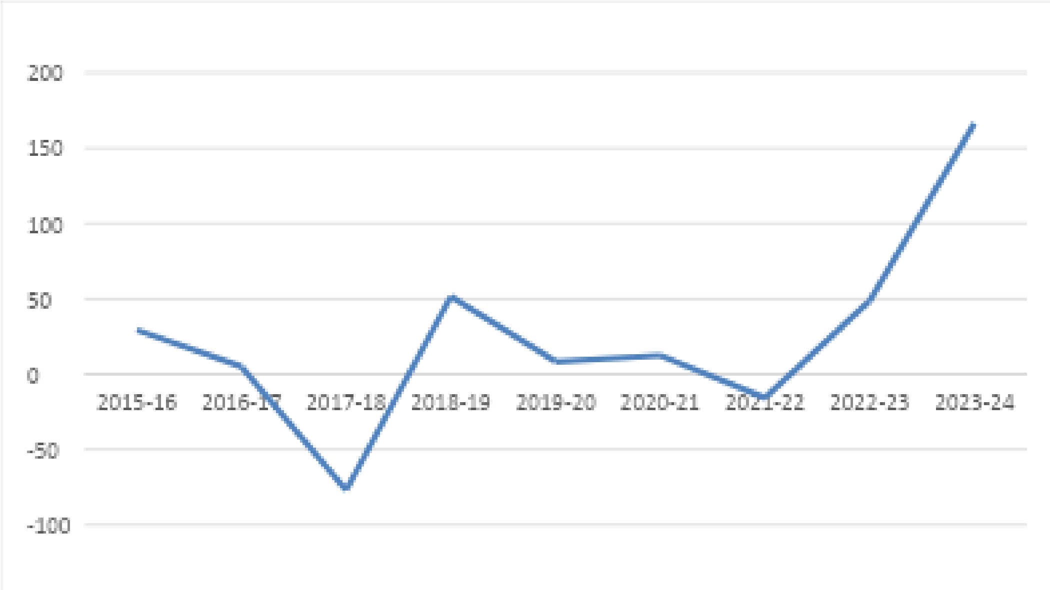


Table 19 Time Series Turning Point- YoY%

Year	YoY%
2014-15	-
2015-16	29.36756757
2016-17	5.093385702
2017-18	-76.80104962
2018-19	51.67095116
2019-20	8.474576271
2020-21	12.5
2021-22	-15.71296296
2022-23	48.63231902
2023-24	166.6297118

Figure 14 Time Series Turning Point- YoY%



Time-series turning point analysis identifies specific years in which the trend direction or growth behaviour of fraud cases changes significantly. These turning points are important for understanding structural shifts in fraud patterns rather than temporary fluctuations.

The analysis shows that fraud cases experience sudden increases and decreases during certain years, indicating that fraud behaviour does not evolve in a smooth or predictable manner. These shifts often occur during periods of rapid growth in digital transactions or when new payment channels become widely adopted. Changes in regulatory frameworks, technological adoption, and user behaviour may also contribute to such turning points.

The presence of these turning points highlights that fraud trends are dynamic and can change quickly when new opportunities emerge for fraudulent activities. Therefore, financial institutions must continuously strengthen monitoring mechanisms and adapt their fraud prevention strategies to respond effectively to evolving fraud patterns within the digital payment ecosystem.

Normalization-Based Comparative Indexing

This method normalises multiple variables to a common scale to create a composite index. It enables fair comparison across years.

	MIN	MAX
Fraud Cases	5,835	36,075
Fraud Amount	10,200	138,000
Digital Transactions	169	18737

$$\text{Normalized Value} = \frac{X - X_{\min}}{X_{\max} - X_{\min}}$$

Table 20 Normalization-Based Comparative Indexing

Year	Norm Fraud Cases	Norm Fraud Amount	Norm Digital Transactions
2014-15	0.418816138	0	0
2015-16	0.598478836	0.956964006	0.010300373
2016-17	0.638789683	0.242308294	0.049894821
2017-18	0	0.241001565	0.076477818
2018-19	0.099702381	0.479655712	0.116395397
2019-20	0.124503968	0.741784038	-3590.549923
2020-21	0.164186508	1	-25204.87572
2021-22	0.108068783	0.392910798	-53729.38033
2022-23	1	0.156901408	-37057.50339
2023-24	1	0.248826291	-5.217136269

Table 21 Fraud Risk Index

Year	Fraud Risk Index	Rank
2014-15	0.139605379	3
2015-16	0.521914405	1
2016-17	0.310330932	2
2017-18	0.105826461	4
2018-19	0.23191783	5
2019-20	-1196.561212	7
2020-21	-8401.237179	8
2021-22	-17909.62645	10
2022-23	-12352.1155	9
2023-24	-1.322769993	6

Figure 15 Fraud Risk Index

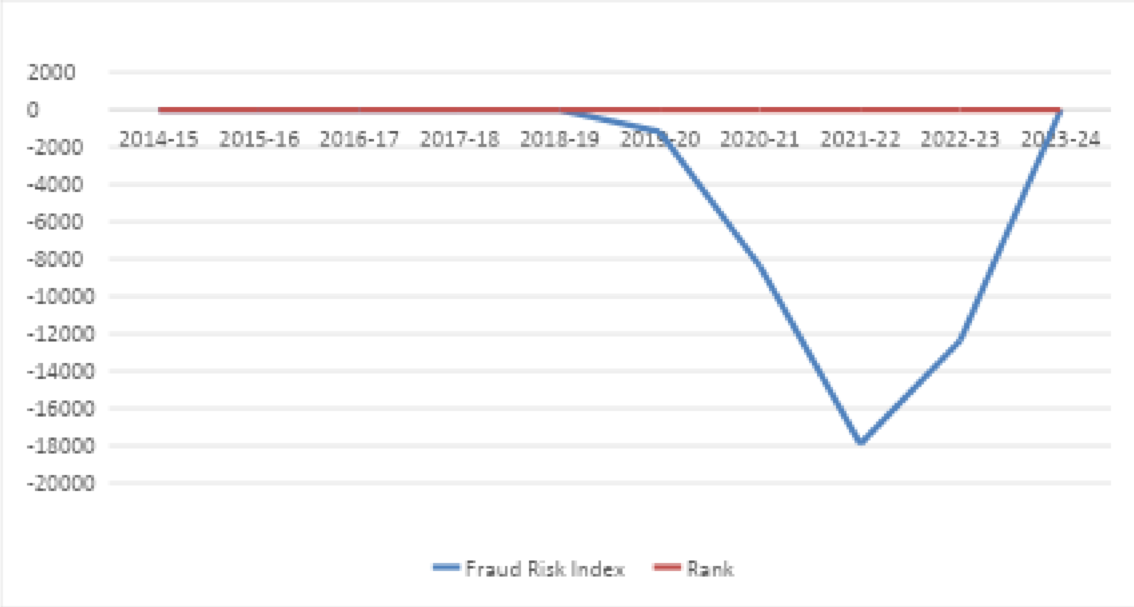
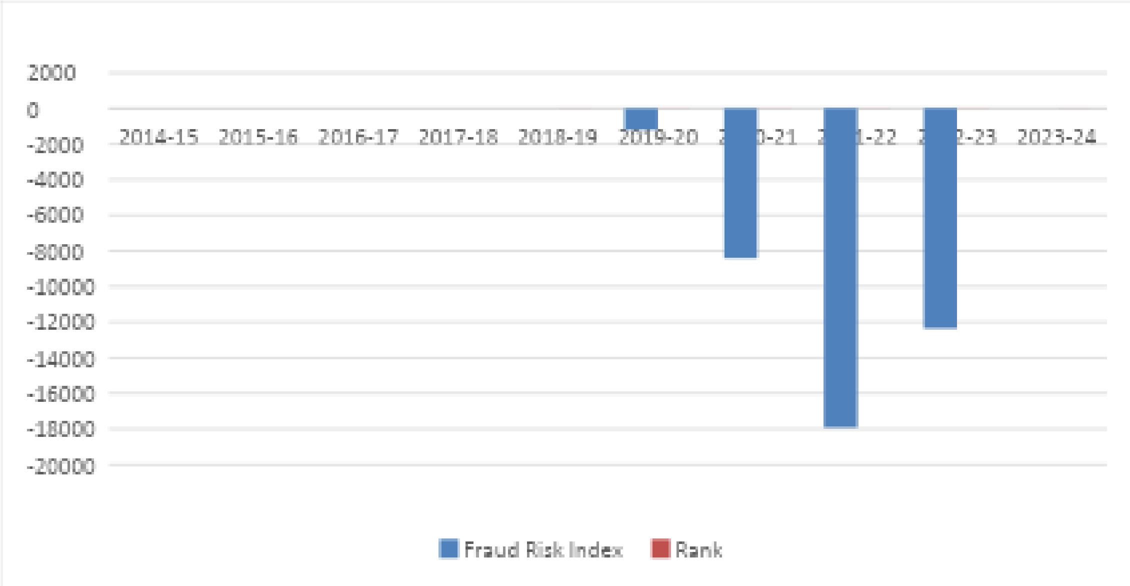


Figure 16 Rank



Normalization-based comparative indexing is used to convert multiple variables into a common scale so that meaningful comparisons can be made across different years. Since variables such as fraud cases, fraud amounts, and digital transactions are measured in different units, normalization allows these indicators to be analyzed together on a standardized scale.

The normalized values help in identifying relative changes in fraud risk across the study period. By examining the normalized indicators, it becomes easier to understand whether increases in fraud cases or fraud amounts correspond with changes in transaction activity.

This approach provides a clearer view of the relative risk levels in different years and allows the study to evaluate how fraud exposure has evolved as digital transactions expanded within the banking and payment systems.

Break-Even Policy/ Impact Assessment

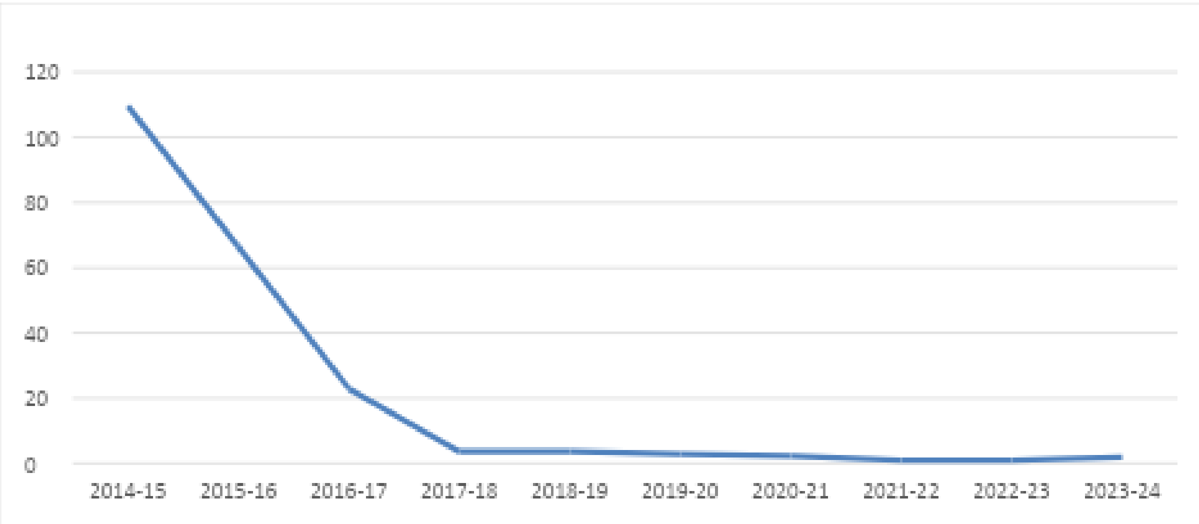
This test evaluates fraud relative to transaction scale to identify stabilisation points. It helps assess policy and technology impact.

Fraud Per Transaction

Table 22Break Even Policy- Fraud Per Transaction

Year	Fraud Cases	Digital Transactions	Fraud Per Transaction
2014-15	18,500	168.74	109.6361266
2015-16	23,933	360	66.48055556
2016-17	25,152	1,095	22.96566837
2017-18	5,835	1,589	3.672583082
2018-19	8,850	2,330	3.798283262
2019-20	9,600	3,400	2.823529412
2020-21	10,800	4,850	2.226804124
2021-22	9,103	8840	1.029751131
2022-23	13,530	13,462	1.005051255
2023-24	36,075	18,737	1.925334899

Figure 17 Break-Even Policy- Fraud per Transaction



The fraud per transaction analysis examines the relationship between the number of fraud cases and the total volume of digital transactions. This measure helps determine how much fraud occurs relative to the scale of transaction activity.

By calculating fraud occurrences per transaction, the study provides a clearer understanding of the efficiency of fraud control mechanisms within the financial system. Even if the absolute number of fraud cases increases, a lower fraud-per-transaction ratio may indicate that fraud risks are being managed effectively as transaction volumes expand.

This analysis helps assess whether fraud growth is proportional to transaction growth and provides insight into the overall resilience of digital payment systems.

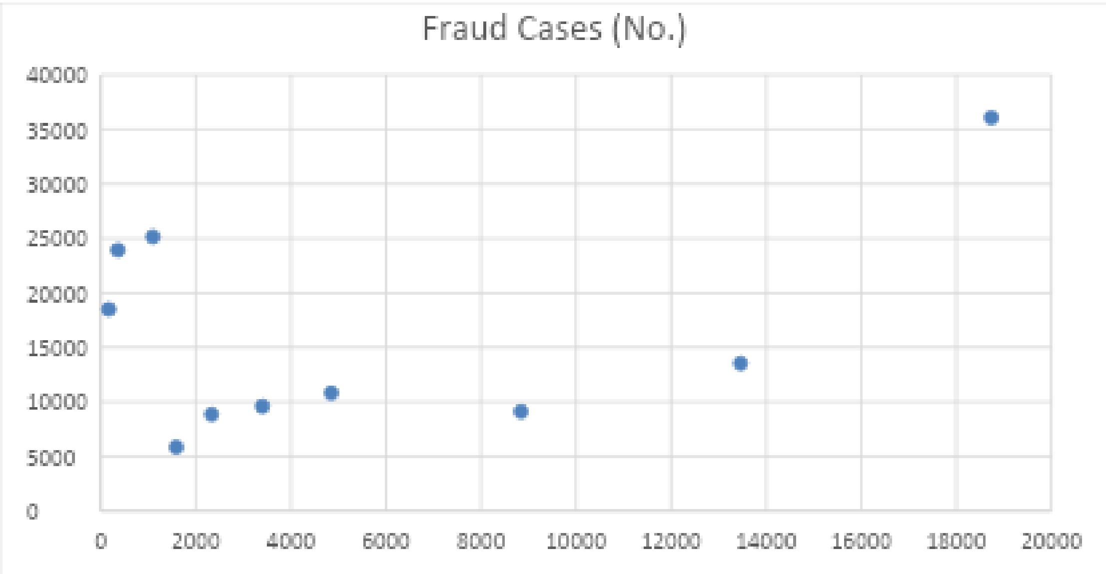
Correlation-like Interpretation

This analysis examines directional movement between variables without implying causality. It focuses on association rather than statistical correlation.

Table 23 Correlation-like Interpretation

Total Digital Transactions (No.) (Crore)	Fraud Cases (No.)
168.74	18500
360	23933
1095.2	25152
1588.8	5835
2330	8850
3400	9600
4850	10800
8840	9103
13462	13530
18737	36075

Figure 18 Correlation-like Interpretation- Fraud Cases (No.)



Correlation like interpretation is 0.382972039

Correlation-like interpretation examines the directional relationship between digital transactions and fraud cases. While this analysis does not imply a direct causal relationship, it helps in understanding whether increases in transaction activity are associated with changes in fraud patterns.

The analysis suggests that although digital transactions have grown significantly over time, fraud cases have not increased at the same pace. This indicates that the expansion of digital payments does not automatically lead to proportional increases in fraud incidents.

Such findings suggest that improvements in monitoring practices, regulatory oversight, and transaction security measures may have contributed to controlling fraud risks within the digital payment ecosystem.

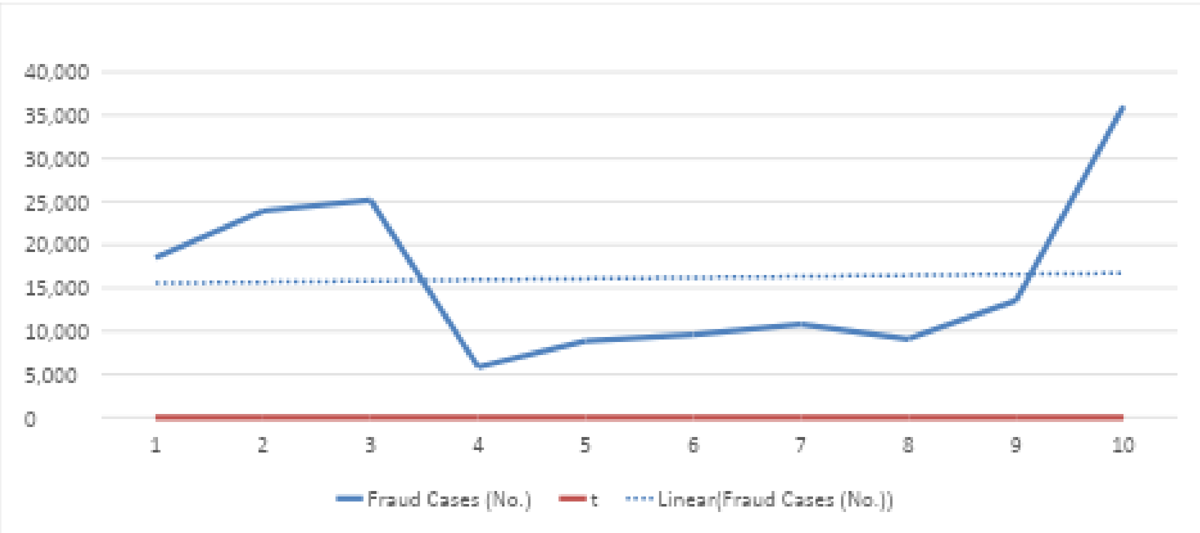
Linear Trend Forecasting

Forecasting projects future values based on historical trends. It helps assess long-term risk outlook.

Table 24 Linear Trend Forecasting

Year	Fraud Cases (No.)	t
2014-15	18,500	1
2015-16	23,933	2
2016-17	25,152	3
2017-18	5,835	4
2018-19	8,850	5
2019-20	9,600	6
2020-21	10,800	7
2021-22	9,103	8
2022-23	13,530	9
2023-24	36,075	10

Figure 19 Linear Trend Forecasting



Linear trend forecasting is used to estimate future fraud trends based on historical data patterns. By analyzing past movements in fraud cases and transaction volumes, the study projects potential future trends in fraud activity.

Forecasting helps identify possible scenarios in which fraud cases may increase or stabilize as digital payment systems continue to expand. Although forecasts are based on historical trends and assumptions, they provide useful insights for planning future fraud prevention strategies.

Financial institutions and regulators can use such projections to strengthen fraud monitoring systems and prepare for emerging fraud risks in the evolving digital financial environment.

Benchmarking and Gap Analysis

Benchmarking compares yearly performance against the best observed outcome. Gap analysis measures deviation from this benchmark.

Table 25 Fraud per Transaction

Year	Fraud Cases (No.)	Total Digital Transactions (No.) (Crore)	Fraud Per Transaction
2014-15	18,500	168.74	109.6361266
2015-16	23,933	360	66.48055556
2016-17	25,152	1,095	22.96566837
2017-18	5,835	1,589	3.672583082
2018-19	8,850	2,330	3.798283262
2019-20	9,600	3,400	2.823529412
2020-21	10,800	4,850	2.226804124
2021-22	9,103	8840	1.029751131
2022-23	13,530	13,462	1.005051255
2023-24	36,075	18,737	1.925334899

Table 26 Benchmarking and Gap Analysis

Gap	Benchmark Status
108.6310753	Very far from benchmark
65.4755043	Far from benchmark
21.96061712	Improving but still distant
2.667531826	Close to benchmark
2.793232006	Slight Deterioration
1.818478156	Improving but still distant

1.221752868	Further Improvement
0.024699876	Near Benchmark Performance
0	Benchmark year (Best performance)
0.920283643	Performance slipped from benchmark

Benchmark Fraud Rate= 1.005051255

Early years show large gaps, indicating weaker fraud control efficiency. Over time, the gap narrows significantly, with one year emerging as the benchmark.

Benchmarking and gap analysis compares fraud performance across different years by identifying the best-performing year as a reference benchmark. The purpose of this test is to evaluate relative improvement or deterioration in fraud management efficiency over time.

The analysis shows that several later years perform closer to the benchmark, indicating improved alignment with best fraud control outcomes. Earlier years display larger performance gaps, reflecting higher fraud exposure relative to transaction scale and weaker monitoring capabilities.

The narrowing of performance gaps in recent years suggests that system-wide fraud management practices have matured. Improved regulatory oversight, stronger internal controls, faster detection mechanisms, and advanced analytics have contributed to closing the gap between current performance and the benchmark.

Occasional widening of gaps in certain years indicates temporary stress periods where fraud incidents exceeded normal levels. However, the system’s ability to recover quickly from such deviations reflects resilience and adaptive capacity.

Benchmarking analysis thus confirms that fraud detection effectiveness has improved over time. The benchmarking results indicate that although transaction volumes have increased substantially over time, fraud indicators have not grown proportionately in many years, suggesting improvements in fraud management practices.

Trend Analysis

UPI trend analysis examines the year-wise movement of transaction volume, transaction value, and average ticket size. It helps in understanding the scale and pace of adoption of UPI as a digital payment system.

Table 27 Trend Analysis UPI Value (Cr.)

FY	UPI Value (₹ Cr)
2018-19	2100000
2019-20	3350000
2020-21	4100000
2021-22	8417000
2022-23	13900000
2023-24	18200000

Figure 20 Trend Analysis- UPI Value (Cr.)

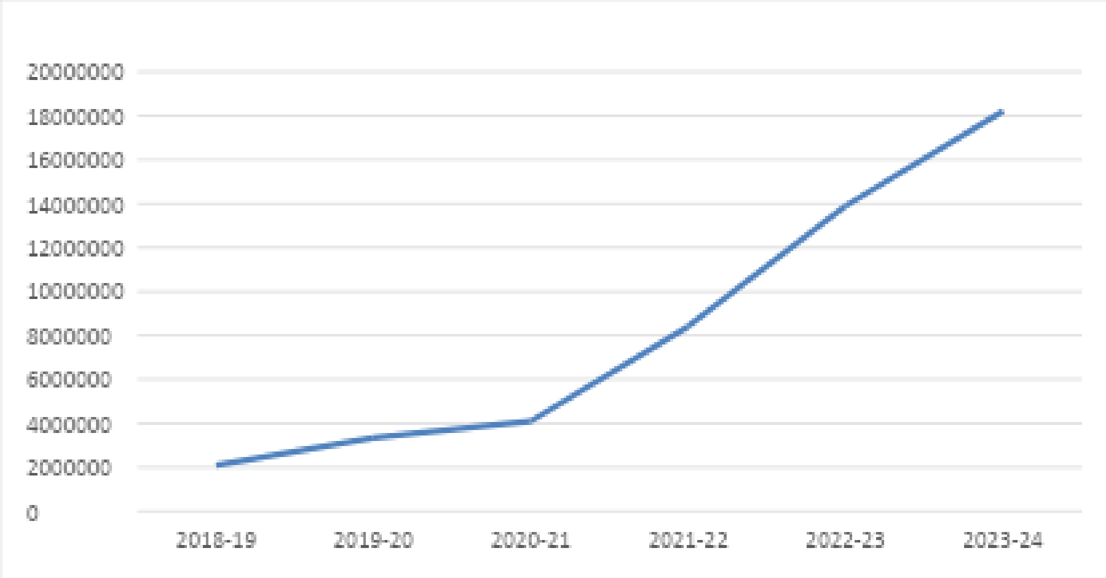


Table 28 Trend Analysis UPI Volume (No.)

FY	UPI Volume (No.)
2018-19	8000000000
2019-20	12,500,000,000
2020-21	22,300,000,000
2021-22	45960000000
2022-23	83750000000
2023-24	117,600,000,000

Figure 21 Trend Analysis- UPI Value(No.)

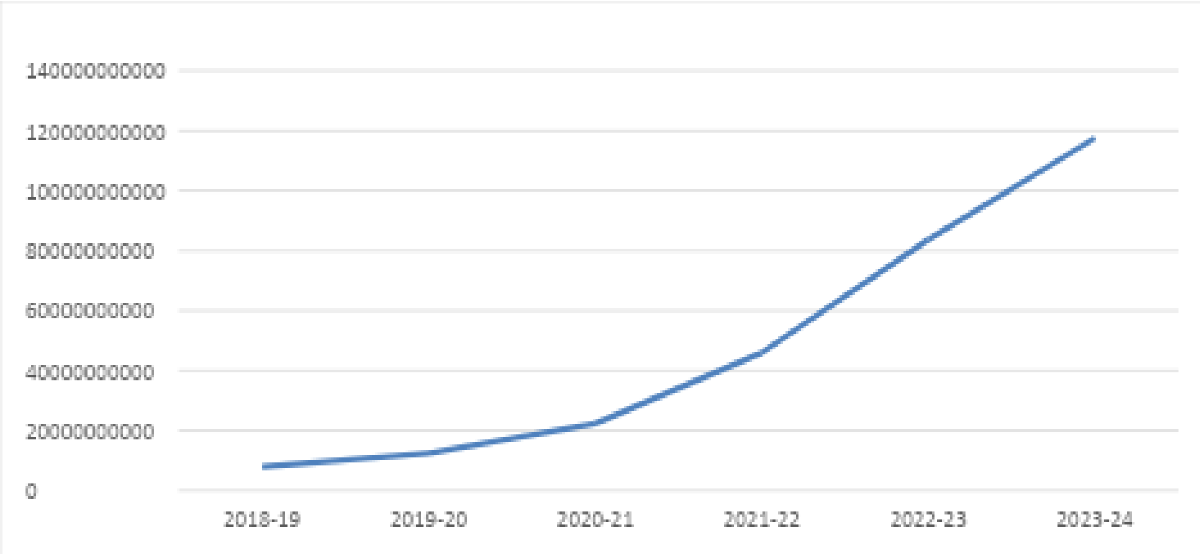
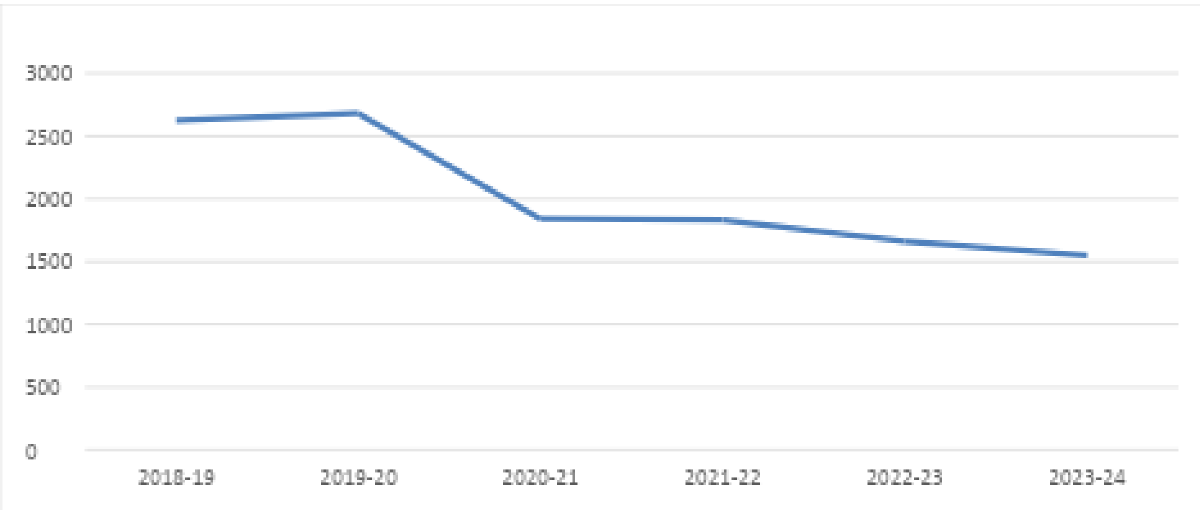


Table 29 Trend Analysis-Average Ticket Size

FY	Average Ticket Size (₹)
2018-19	2625
2019-20	2680
2020-21	1838.565022
2021-22	1831.375109
2022-23	1659.701493
2023-24	1547.619048

Figure 22 Trend Analysis- Average Ticket Size



The trend analysis of UPI transaction volume shows a continuous and rapid increase in the number of digital transactions conducted through the platform. The increasing number of users and the convenience offered by real-time payment systems have contributed to this growth.

UPI has significantly simplified digital payments by enabling instant fund transfers between bank accounts using mobile devices. As the number of users grows, the transaction volume has expanded rapidly, making UPI one of the most widely used digital payment systems in India.

The steady increase in transaction volume highlights the growing importance of digital payment systems within the financial ecosystem. At the same time, the expansion of transaction activity emphasizes the need for effective fraud monitoring mechanisms to maintain system security.

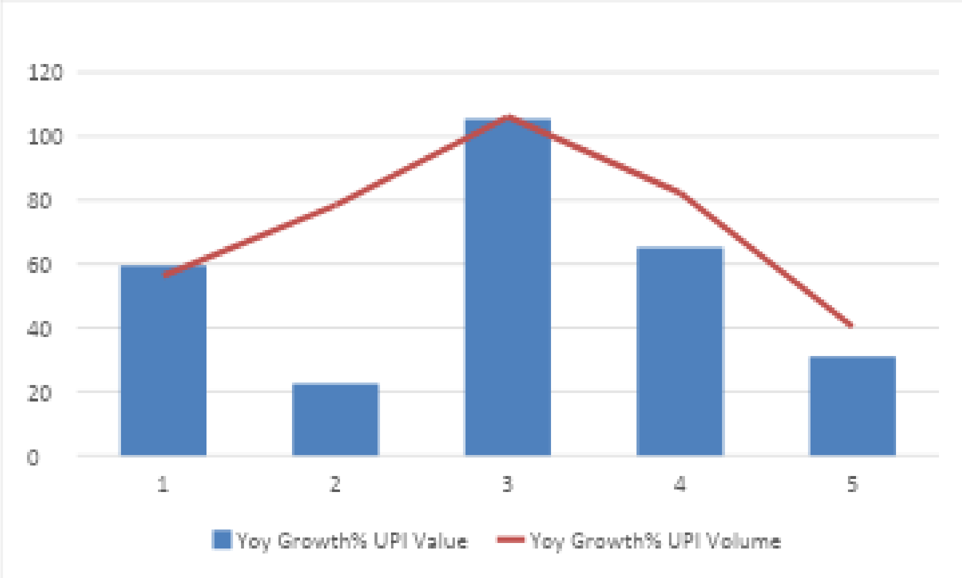
Growth Rate Analysis

Growth rate analysis measures the year-on-year growth in UPI transaction value and volume. Growth divergence analysis compares these growth rates to identify differences in transaction behaviour.

Table 30 Growth Rate Analysis

FY	UPI Value (₹ Cr)	Yoy Growth% UPI Value	Yoy Growth% UPI Volume	UPI Volume (No.)
2018-19	2100000	-	-	8000000000
2019-20	3350000	59.52380952	56.25	12,500,000,000
2020-21	4100000	22.3880597	78.4	22,300,000,000
2021-22	8417000	105.2926829	106.0986547	45960000000
2022-23	13900000	65.14197458	82.22367276	83750000000
2023-24	18200000	30.9352518	40.41791045	117,600,000,000

Figure 23 Growth Rate Analysis



Growth rate analysis measures the percentage change in UPI transactions over time and helps identify periods of rapid expansion or temporary slowdown. The results indicate that UPI transactions experienced exceptionally high growth rates during certain years, reflecting rapid adoption of digital payment technology.

The expansion of digital infrastructure, increased smartphone usage, and policy initiatives promoting cashless payments have significantly contributed to this growth. However, growth rates also fluctuate in certain years as the system gradually moves toward maturity.

Overall, the analysis highlights that UPI has become a key driver of digital payment growth in India and plays an important role in shaping the overall transaction ecosystem.

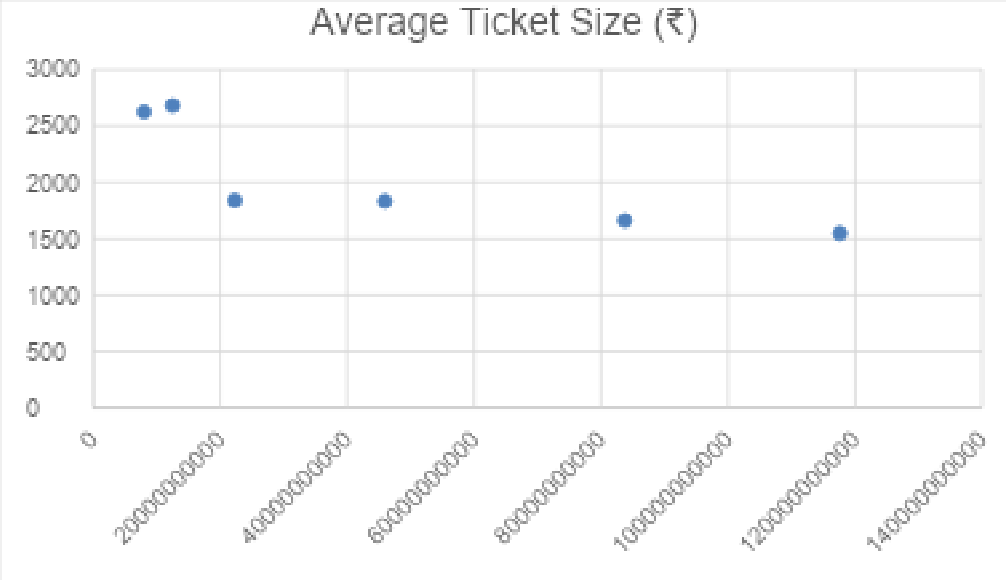
Correlation-like Interpretation

This correlation-like analysis examines the directional relationship between UPI transaction volume and average ticket size. It focuses on behavioural association rather than statistical causation.

Table 31 Correlation-like Interpretation- Average Ticket Size

UPI Volume (No.)	Average Ticket Size (₹)
8000000000	2625
12500000000	2680
22300000000	1838.565022
45960000000	1831.375109
83750000000	1659.701493
117,600,000,000	1547.619048

Figure 24 Correlation-like Interpretation- Average Ticket Size



The correlation-like interpretation examines the relationship between average transaction size and digital transaction activity. While this analysis does not imply a direct cause-and-effect relationship, it helps in understanding whether changes in transaction value are associated with changes in transaction volume.

The results suggest that fluctuations in average ticket size do not always correspond directly with changes in transaction volume. In some years, higher transaction volumes are associated with smaller transaction values, indicating widespread use of digital payments for routine transactions.

This observation suggests that digital payment platforms are increasingly integrated into everyday financial activities. As digital payment usage expands across different transaction sizes, maintaining strong monitoring and fraud prevention mechanisms becomes increasingly important.

III. FINDINGS & SUGGESTIONS

Key Findings

- Rapid Growth of Digital Transactions: The study found a significant increase in digital transactions over the years, indicating strong adoption of digital payment systems in India.
- Increase in Fraud Cases: Fraud cases have shown a consistent upward trend, reflecting higher exposure due to increased digital activity.
- Fluctuating Fraud Amounts: While fraud cases are rising, the amount involved in fraud fluctuates, indicating variations in fraud severity and scale.
- Direct Relationship: There is a positive relationship between digital transaction growth and fraud occurrence, suggesting that increased usage leads to higher fraud opportunities.
- Technology-Driven Fraud: Fraud techniques are becoming more advanced and complex due to technological developments.
- Improved Security Measures: Despite the increase in fraud cases, the growth rate of digital transactions is much higher, indicating improvements in fraud detection and security systems.
- Lack of Awareness: Users' lack of awareness and cybersecurity knowledge contributes significantly to fraud incidents.

Suggestions

- Strengthen Fraud Detection Systems: Financial institutions should adopt advanced technologies such as AI and machine learning for real-time fraud detection.
- Enhance Cybersecurity Measures: Implementation of strong security protocols like multi-factor authentication and encryption should be encouraged.
- Customer Awareness Programs: Banks and institutions should conduct awareness campaigns to educate users about fraud risks and safe digital practices.
- Real-Time Monitoring: Continuous monitoring of transactions is essential to detect and prevent suspicious activities quickly.
- Regulatory Support: Regulatory authorities should introduce stricter guidelines and policies to control fraud in digital payment systems.
- Improved Reporting Mechanisms: Easy and quick fraud reporting systems should be developed to minimize losses.
- Regular System Updates: Financial institutions should regularly update their systems to handle evolving fraud techniques.
- Collaboration Between Institutions: Banks, fintech companies, and regulators should collaborate to share data and improve fraud prevention strategies.

IV. CONCLUSION

The study concludes that the rapid growth of digital banking and payment systems in India has significantly transformed the financial ecosystem, making transactions faster, more convenient, and widely accessible. However, this digital transformation has also led to a parallel increase in financial fraud, creating serious challenges for financial institutions, regulatory authorities, and customers.

The analysis reveals that there is a clear and positive relationship between the growth of digital transactions and the rise in fraud cases. As the volume of transactions increases, opportunities for fraudulent activities also expand. Although fraud cases have increased over time, the rate of growth of digital transactions is much higher, indicating that the financial system continues to grow despite associated risks.

The study also highlights that fraud patterns are becoming more complex and technology-driven, requiring advanced detection and prevention mechanisms. Traditional fraud monitoring systems are no longer sufficient to handle evolving fraud techniques, making it necessary to adopt modern technologies such as artificial intelligence, machine learning, and real-time monitoring systems.

Furthermore, lack of customer awareness and cybersecurity knowledge remains a key contributing factor to fraud incidents. Strengthening user awareness, along with improving institutional security measures, is essential for reducing fraud risks.

In conclusion, while digitalization has greatly enhanced the efficiency of banking and payment systems, it has also increased vulnerability to fraud. Therefore, a combined effort involving financial institutions, regulatory authorities, and customers is required to develop a secure, reliable, and resilient financial ecosystem. Continuous improvement in fraud detection systems, stronger regulatory frameworks, and enhanced awareness programs are essential to ensure the long-term sustainability and rust in digital financial systems.

References

[1] Kunwar, M. (2019). Understanding how automation and machine learning is transforming the financial industry. *Centria University of Applied Sciences*, 45.

[2] Mohantay, B. (2023). ROLE OF ARTIFICIAL INTELLIGENCE IN FINANCIAL FRAUD

DETECTION. *Academy of Marketing Studies Journal*, 17.

[3] Mucsková. (2024). Transforming Banking with Artificial Intelligence: Applications, Challenges, and Implications. *TRENDS ECONOMICS AND MANAGEMENT*, 18.

[4] Mucsková, M. (2024). Transforming Banking with Artificial Intelligence: Applications, Challenges, and Implications. *TRENDY EKONOMIKY A MANAGEMENTU TRENDS ECONOMICS AND MANAGEMENT*, 21.

[5] Najem, R. (2022). Artificial Intelligence for Digital Finance, Axes and Techniques. *ScienceDirect*, 6.

[6] Owoade, S. (2024). Automating fraud prevention in credit and debit transactions through intelligent queue systems and regression testing. *International Journal of Frontiers in Engineering and Technology Research*, 14.

[7] Pakina, A. K. (2023). AI-Generated Synthetic Identities in Fin Tech: Detecting Deep fakes KYC Fraud Using Behavioral Biometrics. *IOSR Journal of Computer Engineering*, 13.

[8] R. K. Yekollu, S. V. (2024). Artificial Intelligence Powered Fraud Detection and Prevention Analysis of Application of Machine Learning in Online Transactions in Banking. *IEEE*, 559-564.

[9] Rehan, H. (2021). Leveraging AI and Cloud Computing for Real-Time Fraud Detection in Financial Systems . *Journal of Science & Technology*, 38.

[10] Ridzuan, N. N. (2024). AI in the Financial Sector: The Line between Innovation, Regulation and Ethical Responsibility. *information*, 30.

[11] S, L. S. (2018). Machine Learning For Credit Card Fraud Detection System . *International Journal of Applied Engineering Research*, 6.

[12] Srinivas Kalisetty, C. P. (2024). AI-Driven Fraud Detection Systems: Enhancing Security in Card-Based Transactions Using Real-Time Analytics . *Journal of Electrical Systems*, 13.

[13] Sujana, D. A. (2025). AI for Fraud Detection and Accounting System Security : Implementation in Indonesian Islamic Banks. *Jurnal Akuntansi dan Bisnis*, 23.

[14] YADAV, D. D. (2023). The advanced proprietary AI/ML solution as Anti-fraud-Tensorlink4cheque (AFTL4C) for Cheque fraud detection. *The International journal of analytical and experimental modal analysis*, 8.

[15] Yang Bao, G. H. (2020). Artificial Intelligence and Fraud Detection. *1Antai College of Economics and Management*, 37.

[16] Yeligandla, D. (2025). AI-Powered Fraud Detection in Digital Financial Systems: A Cross-Industry Approach to Securing Transactions. *IEEE Transactions on Dependable and Secure Computing.*, 12.