Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 1 (2025)

AN OVERVIEW OF DIGITAL PAYMENT FRAUDS: CAUSES, CONSEQUENCES, AND COUNTERMEASURES

Amit Kumar Singh
Research Scholar,
Department of Commerce, Mahatma Gandhi Kashi Vidyapith, Varanasi
Prof. Krishna Kumar Agarwal
Professor, Faculty of Commerce and Management Studies,
Mahatma Gandhi Kashi Vidyapith

ABSTRACT
Digital payment is a double edge sword, the widespread adoption of digital payments has enhanced financial transactions, but it has also led to a rise in digital payment frauds, posing challenges to individuals and financial institutions. This study aims to identify and analyze the underlying causes of digital payment frauds, compare perceptions between victims and non-victims, evaluate countermeasures, and examine the government's role in fraud prevention. A primary study was conducted in Varanasi district, collecting primary data from 280 respondents (118 victims and 132 non-victims) through a structured questionnaire, while secondary data was sourced from RBI reports and financial publications and the data was analyzed using appropriate statistical tools such as Mann-Whitney U test, Wilcoxon rank-sum test, and Friedman test. The findings indicate that financial illiteracy, low awareness, cybersecurity vulnerabilities, and technological complexity are key fraud drivers. Victims emphasize financial illiteracy and technology complexity, while non-victims highlight cybersecurity flaws and slow investigations. Awareness and education emerged as the most effective countermeasures, followed by strict regulations and security intelligence, while emerging technologies like sound wave authentication and network tokenization were perceived as less effective. The study suggests AI-driven fraud detection, biometric authentication, cybersecurity frameworks, and fraud intelligence sharing as essential strategies for improving digital payment security, requiring a multi-stakeholder approach involving consumers, financial institutions, and regulators.

Keywords: Digital Payment System, Digital Payment Frauds, Multifactor Authentication, Cyber Security and Varanasi.

INTRODUCTION
In the present scenario every country wants to become digitally advanced in all aspects for its overall development. On the way of becoming digitally advance, India made the longest stride and leads the global digital payments landscape, accounting for nearly **48.5%** of worldwide real-time transactions followed by Brazil and China (Report on currency and finance, 2024). This rapid expansion of digital payment systems has revolutionized the way individuals and businesses handle transactions. Online banking, mobile payment applications, and electronic wallets provide customers with incomparable accessibility and simplicity of use. However, this advancement in financial technology comes with an alarming growth in digital payment fraud due to free flow of sensitive personal Information on open database, posing significant threats to both consumers and financial institutions (Kannan, 2018). In recent years, the volume and sophistication of digital payment fraud has increased, threatening existing security measures and opening up fresh ways for exploitation. These serious issues must be invalidated within time to give a new height to digital payments system.

Digital Payment fraud is an act of stealing someone's payment information to complete an unauthorized transaction (Digital fraud and banking: supervision and financial stability implications, 2023). Here fraudsters deprive the victim either of money or sensitive information

related to their bank accounts. Nowadays conducting these types of fraudulent activity has become easy because of the rampant adoption of digital payment modes. In an attempt to take the best use of technology today people are ending up being victims of technology. As any UPI application links debit card, credit card, and bank account with phone number and wallets for ease of doing the transaction, at the same time it is also easy for a fraudster to access account details with a mere phone number and attempt to do the fraudulent activity by sending fake links, asking OTP on fake calling or hacking mobile phone. To safeguard public against such fraud, the first step is to understand the various types of digital payment frauds that emerge in India.

1. **Phishing** – It is a form of fraud in which an attacker masquerades as a reputable entity or person via email or other communication channels, said Alexander S. Gillis 2020. In this fraud, the attacker sends malicious links or attachments that are designed to steal your money, your identity, your data, etc. if the user will navigate the site (Zainab, Hewage , Nawaf, & Khan, 2021).

On 24th August 2022, a 45-year-old woman Poonam Dhat lost 4 lakh rupees in a phishing attack in Ahmedabad after receiving a text on her mobile that ask to click on the hyperlink to update her suspended account and after opening and providing the necessary details she got and OTP and after entering it she got a text message for the amount debited from their account.

2. **Vishing –** Vishing is also known as voice phishing. Here fraudster uses voice calls that appear to be coming from a trusted source but are not trustworthy to get the target's personal information (Toapanta, Rivadeneira, Tipantuña, & Guam, 2024). It may be a person or pre-recorded audio on the other end that tells you that you have an issue with your bank account or last transaction and then asked your login credentials to resolve the problem. If you give them your login credentials then they can easily do fraudulent activity with your account

In July 2018 a 59-year-old retired BEST official in Goregaon Mumbai brought a credit card limit of Rs. 5 lakhs. After a month he got a phone call from a person that narrated him as a government official and verify the user's name and address to gain trust and later asked for credit card information for verification purposes. After getting the information an OTP was generated and the user ended up giving away the OTP and lost 0.40 lakhs in 3 attempts on the first day and the next morning again made 3 transactions of Rs. 49999, 10000, and 10000 to a vishing attack.

2. Smishing – It is a form of phishing that assesses mobile phones. In smishing, the fraudster sends short message service (SMS) or multimedia messaging services (MMS) text instead of emails that have malicious links or attachments (Chichwadia & Mpekoa, 2024). Typically, it has 2 ways

a) By asking the target to click on the link to steal phone data in two ways either by directing the user to a fake website which is similar to the alleged official page in to fill the details or by downloading malware to spy on the target device silently

b) By asking the user to reply to a message as it seems to come from a certain official company ask the target to reply to the message with personal information.

In March 2022 Delhi Police arrested 23 people for running a fake version of SBI YONO which seems to be original. The fraudster was accused of sending SMS to SBI users in bulk with a link that directs them to a fake page once the account holder fills their credentials on these pages the accused got access to the original account and was able to make transactions.

3. **Money Mule –** It is also called smurfer. A money mule is a person who receives and transfers money on the behalf of fraudsters for commission. Fraudsters recruit these mules that assist them in money laundering scams but they are not aware that they are helping in criminal activities (DeSantis, Dougherty, & McDowell, 2011). It can be done either by courier services or electronically.

According to a Hindustan Times report on January 2022, three Indian students Nandi Niladri, Akash Deep Singh, and Giri Debjit were arrested in a money mule syndicate and sentenced to prison for 18 months, one year, and seven months respectively in Singapore.

In the past few years, we rely more on digital modes of payment for making our transactions due to this the rate of adoption of digital payments has significantly risen. The two most important goal of digital payment is user friendly and secure than other modes. But in present context seamless and secure payment is one of the most important challenges of digital payment as the number of digital payment frauds are increasing rapidly year by year with rise of digital payment.

Financial Year	Overall Frauds in Value (in Cr.)	Fraud Digital Transaction in Value (in Cr.)	No. of Overall Frauds Reported	No. of Digital Fraud Reported
2020	185391	129	8702	2677
2021	132389	119	7338	2545
2022	59819	155	9097	3596
2023	30252	277	13530	6696
2024*	21367	1457	18461	29082

Table 01: Statistics of Total Frauds and Digital Frauds

* Up to December 2024
Source-
The above table shows the statistics of financial frauds in India in past five financial years (2020–2024). It shows a significant decline in the overall value of frauds which reduces from ₹1,85,391 crore in 2020 to ₹21,367 crore in 2024. Whereas, digital payment frauds shown a significant rise from ₹129 crore in 2020 to ₹1,457 crore in 2024. Additionally, while the total number of all banking frauds initially fluctuate then shown a substantial rise in 2024, reaching 18,461 cases from 8,702 in 2020. Notably, digital fraud incidents have risen immensely, from 2,677 cases in 2020 to 29,082 cases in 2024, highlighting the threats of digital financial transactions. This shift reflects a transformation in fraudulent activities, with a decline in large-scale financial frauds but a significant rise in digital fraud, prompting the need for stronger cybersecurity and regulatory actions.

This paper seeks to provide a comprehensive understanding of the evolving nature of digital payment fraud and assess the underlying causes, analyse the root causes of difference in perception of victims and non-victims. It also focuses on exploring the measures to reduced digital payment fraud and analyse the role of government to mitigate these frauds. For this, first hand study has been conducted on victims and non-victims of digital payment frauds to provide the meaningful insight to identify the root causes and appropriate measures to reduce digital payment frauds and overall transformation of digital payments.

REVIEW OF LITERATURE

Sanjeev. T. A. et.al (2023), in their research paper entitled “A Study on Awareness of E-Banking Frauds with Reference to Bank Customers in Kerela”. The purpose of the study is to increase banking customers' awareness of electronic banking scams and gauge their level of knowledge in

Kerala using questionnaires. This study used a descriptive research technique. The Purposive Sampling approach was employed to get samples from Keralan bank clients. The study used a Likert scale to gauge the bank customers' views. They found that convenience, accessibility, authentication, connectivity security, and technology are the main variables impacting the use of internet banking. It is advised that further study be done to examine the market and economic systems that enable financial fraud as well as the part that financial intermediaries play in it.

Ray. K. P. (2023), in his research paper entitled "A study on cyber financial frauds in the district of Jamtara, Jharkhand" researcher investigated cyber financial theft in Jamtara with an emphasis on offenders' instruments, socioeconomic situations, and problems in cybercrime investigation and also try to highlight difficulties to discovering digital financial crime in Jharkhand because of ambiguous jurisdiction, a lack of technical staff, and inadequate training of police officers. Researcher had used a survey approach to examine cyber financial fraud in Jamtara, Jharkhand, including both secondary and primary data. Primary data was acquired through observation and conversations with police officers, while secondary data was gathered from numerous sources, such as newspapers, e-sources, and government websites. This paper emphasized the difficulties that law enforcement agencies have while investigating cyber financial crimes owing to the ever-changing nature of digital threats and the lack of a secure money flow infrastructure. Improved jurisdictional frameworks and technical training for police personnel were highlighted as critical to increasing the efficiency of countering cyber financial crime in the area.

Ruangmei. T. & Gethe. R. (2023), in their research paper titled "A Study on Modes of Digital Payment System, Analysis of Frauds Occurring through Digital Payment System". The goal of the researcher is to examine potential flaws in digital transactions and comprehend how digital payment systems have evolved. It also focuses on the perception, trust, and experience of consumers with online fraud as well as other aspects that impact their behavior while making digital payments. The study used quantitative exploratory research methodologies, selecting 60 respondents by simple random selection. In addition to visual aids like charts and tables for improved data display, statistical methods like mean and percentage were used for data analysis. They concluded that financial transactions have been transformed by digital payment systems, which provide security, speed, and ease of use. They suggested that for a secure digital payment environment, users must report any suspicious behavior, adhere to security best practices, and remain up to date on the most recent fraud trends.

Tiwari. R. & Sharma. V. (2021), in their research article entitled "Digital Banking: A Study of Fraudulent Practices in Indian Banks". In this paper the researcher has examined how digitalization has affected banking operations, emphasizing how improvements in technology have led to an increase in financial fraud. The study employed secondary data sources from several sources such as RBI bulletins, annual reports, and articles from online publications and used correlation and the student t-test were used to ascertain the effect of digitalization on banking frauds in India. They concluded that customers may now enjoy essential benefits including seamless money transfers, error-free transactions, and ease of use while making purchases online thanks to digital banking. Along with these benefits digitization of banking significantly contributes to an increase in cyber and financial fraud in the Indian banking industry.

Ansar. A. S. (2021), in their research paper entitled "A Critical Analysis of Fraud Cases on Internet". The study highlights the impact of online fraud on financial loss and advocates for new rules and regulations to fight cybercrime. Researchers also emphasized the necessity of website security in protecting personal and organizational data. To gain a better understanding of online fraud victims' reporting experiences, in-depth interviews were performed with a group of 80 people who filed complaints. The study examined several forms of detecting fraud strategies in order to

solve the rising number of illicit transactions and fraud detection concerns. Several data mining tools, including rule-based mining, decision trees, neural networks, and hidden Markov models, were utilized to detect online fraud. The conclusion of the study emphasized the significance of website security in protecting persons and corporate data, as well as combating online fraud. Researchers proposed the establishment of new rules and regulations to combat cybercrime and limit financial losses caused by fake websites.

Chatterjee. A. (2021), in their research article titled "Analysis of Financial Fraud in Electronic Payment System in India and China". With an emphasis on the financial losses caused on by fraudsters' illegal actions, the research examines fraud incidents in China and India with the intention of enhancing consumer awareness, education, and policy-making for fraud prevention. The study makes use of quotative data collected through questionnaire to analyse consumer behavior in online transactions, pointing out areas where fraud detection needs to be improved and advocating a change in focus to investigate fraud from the standpoint of the financial institution. They have recorded 1200 responses from India and China and used SPSS for analysis. They concluded that China's consumers are less pleased and receive poorer-quality services, which suggests that fraud detection has to be improved. They suggested that financial fraud may be decreased by educating customers on how to spot possible deception areas and restrict the amount of personal information they disclose online.

Eneeji. et.al (2019), in their research article entitled "A Study of Electronic Banking Fraud, Fraud Detection and Control". This study analyses electronic banking fraud, including detection, control, and associated issues and also highlight the emerging technologies, such as geocoding and artificial neural networks, are evaluated for fraud detection in electronic banking. Researcher tries to review the emerging technologies such as geocoding and artificial neural networks for detecting fraud in electronic banking. Using biometric authentication to verify and authenticate persons in electronic financial transactions. They concluded that electronic banking has tremendously enhanced financial services throughout the world, but it has also facilitated severe crimes committed by fraudsters, causing economic harm. Emerging technologies, such as geocoding and artificial neural networks, play an important role in fraud detection and control in electronic banking.

Kannan. M. (2018), in their research paper entitled "The Face of Digital Frauds in Digital Banking Scenario- A Literature based Study" focuses on the development and causes of digital frauds in digital banking services, the research examines the simultaneous movements of digital banking services and associated digital frauds through the body of literature. The study reviewed pertinent literature on various types of digital fraud in various digital banking services offered by various bank types. In order to comprehend the nature and consequences of fraud in the financial sector, a formal examination of this issue was carried out. They found that a direct correlation to digital banking, digital frauds are most prevalent and significant in the banking industry. This emphasizes the need for improved consumer knowledge to reduce frauds. The study highlights the fact that digital frauds are still inevitable in the age of rapid technological advancement, even in the face of strict regulations and safeguards.

OBJECTIVES

1. To identify and analyse the underlying causes contributing to digital payment frauds.
2. To compare the digital payment fraud perception between the victims and non-victims.
3. To identify and analyse the suitable measures that can resolve digital payment issues.
4. To study the role of government for digital payment frauds.

HYPOTHESIS

$H0_1$: There is no significant difference in the perception of digital payment fraud causes between the victims and non-victims.
HA_1: There is a significant difference in the perception of digital payment fraud causes between the victims and non-victims.
$H0_2$: There is no significant difference in how respondents rank different measures for preventing digital payment fraud.
HA_2: There is a significant difference in how respondents rank different measures for preventing digital payment fraud.

RESEARCH METHODOLOGY

This research is empirical and analytical in nature. Both primary and secondary data has been used to fulfil the stated objective. Primary data has been collected from Varanasi district during the period of December 2024 to January 2025. For the collection of data, a structured questionnaire was formed and distributed using random sampling method, and a total of 280 responses were collected. Secondary data was arranged from several websites such as RBI annual report, RBI circulars and NPCI. The collected data was analysed using simple average, Mann-witney u test and Friedman test using SPSS.

DATA ANALYSIS AND INTERPRETATION

DEMOGRAPHIC PROFILE

The study collected 280 responses from individuals of Varanasi district, representing a diverse demographic profile. The gender distribution was nearly balanced, with 52.8% male and 47.2% female respondents. In terms of age, the majority of respondents (49.2%) were aged 26 to 35 years, followed by 15 to 25 years (32%), while 11.2% were in the 36 to 45 years category, and 7.6% were above 45 years. Regarding educational qualifications, most respondents have a postgraduate degree (61.6%), followed by graduates (21.2%), while 9.6% had other qualifications, and smaller proportions had intermediate (4.4%) or matric (3.2%) education. The occupational distribution shows that students formed the largest group (44%), followed by employed professionals (33.2%), unemployed individuals (12.4%), and self-employed participants (10.4%). Additionally, 70% of respondents resided in urban areas, while 30% belonged to rural areas. This demographic composition provides a well-rounded and representative sample for analysing digital payment frauds, its causes and the measures to cater digital payment frauds.

ANALYTICAL FRAMEWORK

For the analysis and interpretation, the collected responses have been divided into two sections. The first section which is based on the first and second objectives of the study, that is, to identify and analyse the underlying causes contributing to digital payment frauds, and to compare the digital payment fraud perception between the victims and non-victims. Out of 280 respondents, 118 respondents had faced digital payment fraud, considered as victims, and 132 respondents had not faced digital payment fraud, while 30 responses were inconsistent and thus eliminated for the further analysis. For the analysis purpose six major causes were identified, i.e. Financial Illiteracy, Low Awareness, Cyber Security Issues, Technology Complexity, Operational Changes, and Slow Investigation, and perception of both the victims and non-victims were collected through questions based on Likert Scale. Further, the data was analysed using Mann-Whitney U test and Wilcoxon rank-sum test. While the second section is based on the third objective of the study, stating to identify and analyse the suitable measures that can resolve digital payment issues. For the fulfilment of above objective ten measures were identified, and data related to this were collected using questions based on Likert scale, and analysed using Friedman rank test.

Reliability Test

The reliability of the questions has been measured using Cronbach's Alpha, on the 17 questions for various dependent variables categorised into two sections causes and measures of digital payment fraud. The result shows that the data has high internal consistency with the coefficient valued 0.930 for 17 items. It suggests that the scale effectively measures the intended construct with minimal measurement error.

$H0_1$: There is no significant difference in the perception of digital payment fraud causes between the victims and non-victims.

Normality Test

The Tests of Normality has been conducted for all dependent variable i.e. Financial Illiteracy, Low Awareness, Cyber Security Issues, Technology Complexity, Operational Changes, and Slow Investigation by using the Kolmogorov-Smirnov and Shapiro-Wilk tests. Their result indicate that the data is not normal distributed, the p-values (Sig.) are 0.000, which is below the significance limit of 0.05. This leads to the rejection of the assumption of normality. The Shapiro-Wilk test values range from 0.769 to 0.899 which also confirming deviation from normality. Due to the non-normality of data, Mann-Whitney U test and Wilcoxon rank-sum test is being used to compare the two independent groups, i.e. victims and non-victims.

Mann-Whitney U test and Wilcoxon rank-sum test				
Causes	**Faced Digital_ Payment Fraud**	**N**	**Mean Rank**	**Sum of Ranks**
(Financial Illiteracy)	YES	118	143.39	16919.50
	NO	132	109.51	14455.50
	Total	250		
(Low Awareness)	YES	118	137.50	16225.50
	NO	132	114.77	15149.50
	Total	250		
(Cyber Security Issues)	YES	118	112.87	13319.00
	NO	132	136.79	18056.00
	Total	250		
(Technology Complexity)	YES	118	141.14	16654.50
	NO	132	111.52	14720.50
	Total	250		
(Operational Changes)	YES	118	137.94	16277.00
	NO	132	114.38	15098.00
	Total	250		
(Slow Investigation)	YES	118	110.52	13041.50
	NO	132	138.89	18333.50
	Total	250		

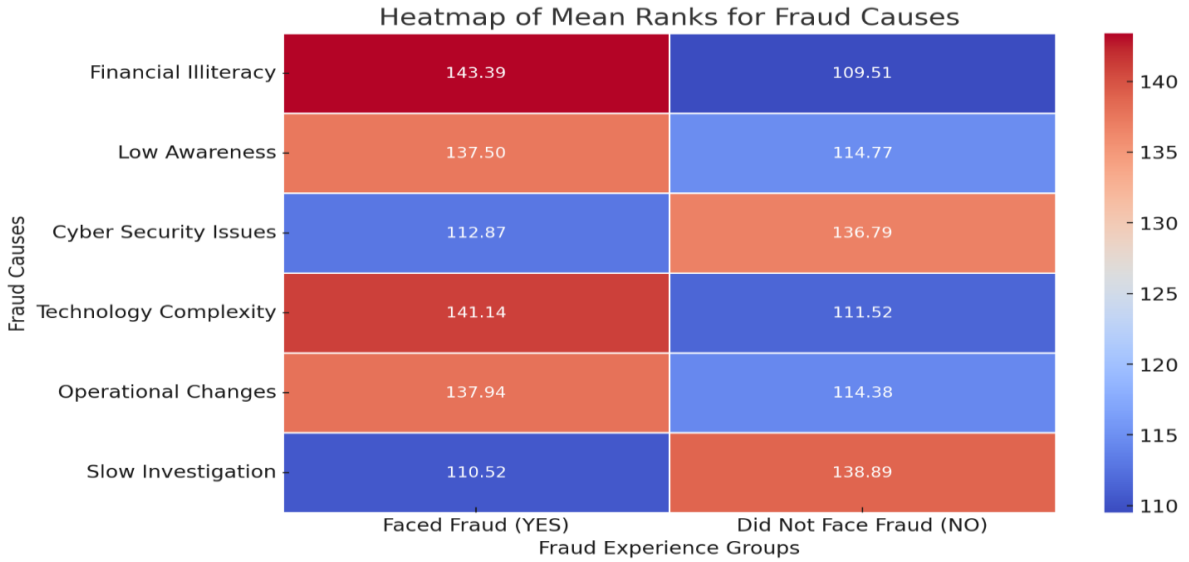
Table 02: Mean Rank of Causes of Digital Payment Fraud

The above table examines the relationship between digital payment fraud experiences and potential contributing causes using mean rank comparisons. Financial illiteracy (Mean Rank = 143.39) and technology complexity (Mean Rank = 141.14) are associated with higher fraud experiences, suggesting a significant role in vulnerability. Conversely, cybersecurity issues (Mean Rank = 112.87) and slow investigation processes (Mean Rank = 110.52) are more prevalent among those who have not faced fraud, indicating that other factors may have greater influence. Low awareness (Mean Rank = 137.50) and operational changes (Mean Rank = 137.94) also appear to be associated with increased fraud risks.

Test Statistics[a]						
Causes	**Financial Illiteracy**	**Low Awareness**	**Cyber Security Issues**	**(Technology Complexity)**	**Operational Changes**	**Slow Investigation**
Mann-Whitney U	5677.500	6371.500	6298.000	5942.500	6320.000	6020.500
Wilcoxon W	14455.500	15149.500	13319.000	14720.500	15098.000	13041.500
Z	-3.896	-2.644	-2.725	-3.389	-2.662	-3.212
Asymp. Sig. (2-tailed)	.000	.008	.006	.001	.008	.001
a. Grouping Variable: Faced_Digital_Payment_Fraud						

Table 03: Mann-Whitney U test and Wilcoxon rank-sum test

The above table shows that there are significant differences in the perception of digital payment fraud causes between those who have experienced it and those who have not. Financial illiteracy ($U = 5677.500$, $Z = -3.896$, $p < .001$) and technology complexity ($U = 5942.500$, $Z = -3.389$, $p = .001$) exhibit the strongest differences, indicating their major role in fraud vulnerability. Other factors, including low awareness ($p = .008$), cybersecurity issues ($p = .006$), operational changes ($p = .008$), and slow investigation ($p = .001$), also show statistically significant disparities. The negative Z-values suggest that those who faced fraud attribute higher importance to these causes compared to those who did not.



Graph 01: Heatmap of Mean Ranks

The above heatmap visualizes the mean rank differences for perceived fraud causes between individuals who faced digital payment fraud and those who did not. Financial illiteracy (143.39) and technology complexity (141.14) have higher mean ranks among fraud victims, indicating their significant role in fraud vulnerability. Conversely, cybersecurity issues (136.79) and slow investigation (138.89) are ranked higher by those who did not face fraud, suggesting they perceive these as less critical risks. The colour gradient highlights these contrasts, with red indicating higher ranks and blue representing lower ranks.

$H0_2$: There is no significant difference in how respondents rank different measures for preventing digital payment fraud.

Normality Test

The normality test has been conducted on all dependent variable. The results of the Kolmogorov-Smirnov and Shapiro-Wilk tests indicate that all measured variables significantly deviate from a normal distribution ($p < 0.001$). The Shapiro-Wilk statistics range from 0.720 (measures Awareness) to 0.901 (measures Sound wave technology), suggesting varying degrees of non-normality across the dataset. The strongest deviation from normality is observed in awareness-related measures, whereas biometric and advanced authentication technologies exhibit relatively higher normality statistics. This leads to the rejection of the assumption of normality. Due to the non-normality of data, Friedman Test is being used to identify difference between multiple related groups.

MESURES	MEAN RANK
[Education]	6.42
[Awareness]	6.72
[Security and Intelligence]	6.10
[Strict rules and regulation against fraudsters]	6.33
[Biometric Authentication]	5.47
[Two factors Authentication]	5.43
[GPS]	5.23
[Facial Recognition]	4.66
[Network Tokenization]	4.37
[Sound wave technology]	4.27

Table 04: Mean Rank of Measures of Digital Payment Fraud

The above table indicate that **Awareness (6.72)** and **Education (6.42)** are perceived as the most effective measures for preventing digital payment fraud, suggesting that users believe knowledge and information play a crucial role in fraud prevention. **Strict rules and regulations (6.33)** and **Security and Intelligence (6.10)** also rank highly, emphasizing the importance of enforcement and monitoring in reducing fraud risks. **Biometric Authentication (5.47)** and **Two-Factor Authentication (5.43)** are moderately ranked, indicating that while security technologies are valued, they may not be seen as standalone solutions. Lower-ranked measures, such as **Sound Wave Technology (4.27)** and **Network Tokenization (4.37),** suggest that these emerging technologies are either less familiar or perceived as less effective in comparison to traditional security methods. Overall, the results highlight that educational initiatives, regulatory frameworks, and intelligence-based security approaches are considered the most critical in combating digital payment fraud.

Test Statistics[a]	
N	250
Chi-Square	337.799
df	9
Asymp. Sig.	.000

a. Friedman Test

Table 05: Friedman Test

The Friedman Test results indicate a **statistically significant difference (p = 0.000)** in how respondents rank various fraud prevention measures, with a **Chi-Square value of 337.799** and **9 degrees of freedom**. This confirms that not all measures are perceived equally effective. The rankings suggest that **Education and Awareness** are viewed as the most effective strategies, emphasizing the importance of knowledge in preventing digital payment fraud. Meanwhile, **Security measures like biometric authentication and two-factor authentication** received

moderate rankings, indicating that while technological solutions are valued, they may not be seen as standalone solutions. Lower-ranked measures, such as **Sound Wave Technology and Network Tokenization**, suggest that these emerging technologies may be either less familiar or perceived as less effective.

Objective 4: To study the role of government for digital payment frauds.

The growing threat of digital payment fraud is a major risk to financial stability, consumer trust, and the whole economic system. As online transaction become more prevalent and complicated, governments throughout the world acknowledge the vital need to address vulnerabilities and safeguard financial systems. Government agencies play an important role in accomplishing legal frameworks, coordinating law enforcement activities, and launching public awareness programs that effectively discourage digital payment fraud.

Key government measures and initiatives in combating digital payment fraud in India

1. **Implementation of Strong Customer Authentication (SCA)-** In India, the Reserve Bank of India (RBI) needs Strong Customer Authentication (SCA) to safeguard digital transactions. Most payments need two-factor authentication (2FA), which combines a password/PIN with a dynamic factor such as an OTP. Biometric verification, frequently using Aadhaar-based identity, improves SCA, especially for high-value transactions. These techniques limit fraud by requiring strong identification verification before processing payments.

2. **Data Protection and Privacy Regulations-** India's Data Protection and Privacy Regulations try to protect personal data in digital transactions, particularly through the Digital Personal Data Protection Act (2023). The act compels financial institutions and payment providers to reduce data collecting, protect data storage, and manage data responsibly in order to avoid unlawful access and use. Compliance with these standards is enforced by strong fines for violations, promoting the secure management of user data. These safeguards aim to protect customers' privacy and limit the possibility of fraud in digital payment systems.

3. **Mandatory Encryption and Tokenization-** In order to protect against fraud and data breaches, India requires that all digital payment data be encrypted and tokenized. The Reserve Bank of India (RBI) requires that sensitive payment information be encrypted during transactions and storage to ensure safe transmission between networks. Furthermore, card tokenization replaces sensitive card information with unique, randomly generated tokens, lowering the risk of card fraud by prohibiting unauthorized access to card data. These methods improve data security by securing users' financial information in digital payments.

4. **Enhanced Transaction Monitoring and Reporting Systems-** India's legal framework requires enhanced transaction monitoring and reporting systems to identify and prevent digital payment fraud. Financial institutions are expected to utilize real-time monitoring techniques to detect suspicious transactions and odd activity patterns. Reporting suspected fraud to government authorities, such as the Financial Intelligence Unit-India (FIU-IND), facilitates a prompt action and allows for the tracking of fraud trends. These approaches improve digital payment security by allowing for the proactive identification and prevention of fraudulent activity.

5. **Consumer Protection and Liability Limitations-** The Reserve Bank of India (RBI) issued India's Consumer Protection and Liability Limitations rules to shield customers from damages caused by unlawful digital transactions. According to these guidelines, consumers have reduced responsibility if fraud is discovered quickly, and liability is sometimes dismissed totally in circumstances when the bank is at fault. Specific time constraints for reporting

unlawful transactions promote prompt responses, allowing customers to get refunds more effectively. These safeguards increase trust in digital payments by protecting consumers from potential financial losses due to fraud.

6. Regular Audits and Compliance Checks- In India, the Reserve Bank of India (RBI) mandates regular audits and compliance checks to ensure all financial institutions maintain strong cybersecurity and fraud prevention standards. These audits examine compliance with the RBI's Cybersecurity Framework, which includes secure data measures, safe transaction methods, and timely upgrades. Noncompliance can result in penalties, which encourages institutions to maintain high security levels. The RBI confirms that banks and payment providers respond to new risks by conducting frequent evaluations, therefore improving the security of digital transactions.

7. Cross-Border Regulations and Collaboration- India's cross-border regulations and collaboration are aimed at combating digital payment fraud across several nations. The government collaborates extensively with international organizations like as INTERPOL and banking authorities to exchange information and coordinate efforts to combat transnational fraud networks. This coordination facilitates the tracking of cross-border fraudsters and assures quick response. Strengthening global collaboration helps reduce threats and improve the security of international digital payments.

8. Public Awareness and Education Campaigns- India's Public Awareness and Education Campaigns seek to educate customers about secure digital payment procedures and fraud prevention. Initiatives such as the RBI Kehta Hai initiative create awareness about phishing, vishing, and secure online transactions. Other initiatives include Digital India, National Cyber Security Awareness Month (NCSAM), Cyber Dosti Campaign, Bharat Interface for Money (BHIM) Campaign, Awareness by Financial Literacy Week (FLW) and Cyber Crime Reporting Helplines. Banks and financial organizations are also urged to offer cybersecurity instruction to their consumers. These advertisements teach people how to spot and avoid fraud, dramatically lowering the chance of financial loss.

9. Promotion of Technology-Driven Fraud Prevention- India emphasizes technology-driven fraud prevention by employing modern techniques such as artificial intelligence (AI), machine learning, and blockchain to identify and prevent fraud in digital payments. Financial institutions are encouraged to deploy AI-powered fraud detection systems capable of identifying anomalous trends and flagging questionable transactions in real time. To keep up with growing threats, the government also finances cybersecurity research and innovation. These technical improvements improve the security of electronic payments and assist to avoid fraudulent activity.

Governments play an important role in combatting digital payment fraud by establishing regulatory frameworks, enforcing laws, and educating consumers. Regulations such as PCI DSS and PSD2 assure high security standards, while international coordination and specialist cybercrime units combat cross-border fraud. Public awareness programs enable customers to protect their personal information, while technology-driven initiatives improve fraud detection. Governments must stay adaptable and invest in modern technology to ensure a safe and resilient digital payment system.

Results and Findings

The study shows a substantial rise in digital payment frauds in India. The value of frauds increased from ₹129 crore in 2020 to ₹1457 crore in 2024, while the volume nearly doubled from 2667

incidents in 2020 to 29082 cases in 2024. Card Present (CP) Fraud, which uses physical cards, and Card Not Present (CNP) Fraud, which exploits card details without the need of an actual card, are two major forms of fraud. Furthermore, phishing, vishing, smishing, and money mule scams are common, with fraudsters adopting misleading ways to gain critical information. According to the survey, financial illiteracy, low awareness, cybersecurity issues, technical complexity, and slow investigation processes are all important factors to fraud. Victims of fraud consider financial illiteracy and technological complexity to be key causes, while non-victims stress cybersecurity concerns and slow investigations. In the context of countermeasures, awareness and education are rated as the most effective, followed by strict regulations and security intelligence, while technological advances such as sound wave technology and network tokenization are deemed less successful. Government measures such as Strong Customer Authentication (SCA), data protection rules, and public awareness campaigns have helped to prevent fraud. However, the report advises that more efforts are required, such as increasing consumer education, implementing advanced cybersecurity measures, upgrading regulatory frameworks, and investing in technical advancements such as blockchain and AI-based fraud detection systems. Overall, a coordinated strategy encompassing governments, financial institutions, and consumers is required to reduce the risk of digital payment fraud and maintain a safe digital payment environment.

Suggestions:

1. **AI and Machine Learning for Real-Time Fraud Detection:**

Advanced AI Algorithms: Implement AI and machine learning algorithms that can analyze transaction patterns in real-time to detect anomalies and flag suspicious activities. These systems can learn from historical fraud data to improve accuracy over time.

Behavioral Biometrics: Use behavioral biometrics, such as typing patterns, mouse movements, and device usage, to authenticate users and detect fraudulent activities. This adds an additional layer of security beyond traditional biometrics.

2. **Advanced Tokenization and Encryption**:

Dynamic Tokenization: Use dynamic tokenization, where tokens are generated uniquely for each transaction and expire after use. This reduces the risk of token reuse and enhances security.

End-to-End Encryption: Implement end-to-end encryption for all digital payment transactions to ensure that data is encrypted from the point of origin to the destination, preventing interception and tampering.

3. **Multi-Factor Authentication (MFA) with Advanced Methods**:

Context-Aware MFA: Implement context-aware multi-factor authentication that considers the context of the transaction, such as location, device, and time, to determine the level of authentication required.

Biometric MFA: Enhance MFA by incorporating multiple biometric factors, such as fingerprint, facial recognition, and voice recognition, to provide a higher level of security.

4. **Zero Trust Architecture**:

Zero Trust Model: Adopt a zero-trust architecture where no user or device is trusted by default, even if they are within the network. Continuous verification and strict access controls are enforced to minimize the risk of unauthorized access.

Micro-Segmentation: Use micro-segmentation to divide the network into smaller, isolated segments, reducing the attack surface and limiting the spread of potential breaches.

5. **Fraud Intelligence Sharing Platforms**:

Collaborative Networks: Establish collaborative networks where financial institutions, payment processors, and regulatory bodies can share fraud intelligence in real-time. This helps in identifying and mitigating emerging fraud trends quickly.

Global Fraud Databases: Create global fraud databases that aggregate fraud data from various sources, enabling predictive analytics and proactive fraud prevention.

6. **Cybersecurity Mesh**:

Distributed Security Architecture: Implement a cybersecurity mesh architecture that provides a distributed and flexible approach to security. This allows for the integration of various security tools and services to create a cohesive defense system.

Adaptive Security Policies: Use adaptive security policies that dynamically adjust based on the current threat landscape and the specific context of each transaction.

7. Incident **Response and Recovery**:

Automated Incident Response: Develop automated incident response systems that can quickly detect, contain, and mitigate fraud incidents. These systems can reduce response times and minimize the impact of fraud.

Fraud Recovery Mechanisms: Establish robust fraud recovery mechanisms to assist victims in recovering lost funds and restoring their accounts. This includes clear protocols for reporting fraud and expedited investigation processes.

8. Enhanced **Consumer Education and Engagement:**

Interactive Training Programs: Develop interactive training programs and simulations to educate consumers about digital payment fraud and safe practices. These programs can be gamified to increase engagement and retention.

Real-Time Alerts and Notifications: Implement real-time alerts and notifications to inform consumers about suspicious activities and provide guidance on how to respond.

Conclusion

The overall amount of fraud cases in India increased from ₹129 crore in 2020 to ₹1457 crore in 2024 as a result of the spike in digital payments. The growing threat was demonstrated by the more than ten times increase in fraud cases from 2677 in 2020 to 29082 in 2024. Financial illiteracy, low awareness, cybersecurity flaws, technological complexity, and slow investigations are some of the main factors. While non-victims highlight security vulnerabilities and slow responses, victims point the finger at financial complexity and illiteracy. The best countermeasures are awareness and education, which are followed by strict regulations and security intelligence. While they are helpful, two-factor authentication and biometric authentication are not stand-alone solutions. Though neglected, emerging technologies like network tokenization and sound wave technology show promise. Government programs like encryption laws, awareness campaigns, and Strong Customer Authentication (SCA) play an important role. However, further efforts are needed to strengthen consumer education and cybersecurity safeguards. Blockchain, AI, and machine learning provide real-time fraud prevention and detection capabilities. It is crucial to have a multifaceted approach that involves customers, regulators, and financial institutions. Security can be improved by promoting international collaboration and fortifying regulatory structures. Campaigns for public awareness must keep informing people about safe online conduct. Stakeholders need to

remain proactive and adaptable in response to emerging fraud tactics. A balance between innovation, regulation, and education is necessary to guarantee the stability of digital payments.

References

- A STUDY ON MODES OF DIGITAL PAYMENT SYSTEM, ANALYSIS OF FRAUDS OCCURING THROUGH DIGITAL PAYMENT SYSTEMS. (2023). *International Research Journal of Modernization in Engineering Technology and Science*. https://doi.org/10.56726/irjmets42773
- Anas, S., Banarasi, A. B., Yadav, J., Kumar, S., Bhimrao, D. B., Srivastava, S. P., Anas Ansar, S., Kumar Dwivedi, S., Pandey, A., Ishrat, M., Khan, W., Pandey, D., Khan, R. A., & Khan, M. W. (2021). A Critical Analysis of Fraud Cases on the Internet. In *Article in Turkish Journal of Computer and Mathematics Education* (Vol. 12, Issue 1). https://www.researchgate.net/publication/352157135
- Akintoye, K. A., & Araoye, O. I. (2011). Combating e-fraud on electronic payment system. *International Journal of Computer Applications*, *25*(8), 48-53.
- Chatterjee, A. (2021). Analysis of financial frauds in electronic payment systems in India and China. In *Turkish Online Journal of Qualitative Inquiry (TOJQI)* (Vol. 12, Issue 7).
- Chichwadia, A. E., & Mpekoa, N. (2024). Detecting Smishing and Vishing Attacks using Machine Learning. *International Journal of Intelligent Computing Research (IJICR)*.
- DeSantis, M., Dougherty, C., & McDowell, M. (2011). Understanding and Protecting Yourself against money mule. *United State Computer Emergency Readiness Team*.
- Eneeji, S., Udie, M., Eyong, W., & Chimdike, K. (2019). A Study of Electronic Banking Fraud, Fraud Detection and Control. In *International Journal of Innovative Science and Research Technology* (Vol. 4, Issue 3). www.ijisrt.com708
- Evidence from Deposit Money Banks in Nigeria. In *African Journal of Economic Review* (Vol. 12, Issue 4).
- Fernandes, L. (2013). Fraud in electronic payment transactions: Threats and countermeasures. *Asia Pacific Journal of Marketing & Management Review ISSN*, *2319*, 2836.
- Folami, R. A., Yinusa, G. O., & Toriola, A. K. (2024). Digital Payment Fraud and Bank Fragility:
- Kannan, D. (2021). E-Frauds and Its Causes in Digital Transactions-A Myth or Reality. *Indian JL & Legal Rsch.*, *2*, 1.
- Kannan, m. (2018). The Face of Digital Frauds in Digital Banking Scenaria- A literature based study. *International Journal of Science and Research (IJSR)*.
- Kannan, M. (2018). The Face of Digital Frauds in Digital Banking Scenario-A Literature Based Study. *International Journal of Science and Research*. https://doi.org/10.21275/ART20197419
- Pranav Kumar, R. (2022). A study on cyber financial frauds in the district of Jamtara, Jharkhand. *Journal of Forensic Science and Research*, *6*(1), 042–044. https://doi.org/10.29328/journal.jfsr.1001034
- Rajput, R., & Thakral, B. (2024). Challenges in Digital Payments and Financial Cyber Frauds in Rural India. In *The Future of Computing: Ubiquitous Applications and Technologies* (pp. 56-69). Bentham Science Publishers.
- Sajeev, A. T., Nair, A. R., & Prasanth, A. P. A STUDY ON AWARENESS OF E-BANKING FRAUDS WITH REFERENCE TO BANK CUSTOMERS IN KERALA.
- Sharma, P., Gallani, V., & Maheria, S. (2024). DIGITAL PAYMENTS AND FRAUD CONNECTION: INSIGHTS FROM THE INDIAN ECONOMY.

- Shree, S., Pratap, B., Saroy, R., & Dhal, S. (2021). Digital payments and consumer experience in India: a survey based empirical study. *Journal of Banking and Financial Technology*, *5*, 1-20.
- Toapanta, F., Rivadeneira, B., Tipantuña, C., & Guam, D. (2024). AI-Driven Vishing Attacks: A Practical Approach . *Engineering Proceedings*.
- Zainab, A., Hewage , C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers*.
- (2023, April 04). *Digital fraud and banking: supervision and financial stability implications.* Supervision, Basel Committee on Banking. Retrieved from Razorpay: https://razorpay.com/blog/online-payment-fraud-and-risk-mitigation/
- (2024). *Report on currency and finance.* Researve Bank of India.
- https://www.pwc.in/industries/financial-services/fintech/dp/combating-fraud-in-the-era-of-digital-payments.html retrieved on Jan 05 2025
- https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=916 retrieved on Jan 08 2025 https://timesofindia.indiatimes.com/city/ahmedabad/4l-stolen-from-45-year-old-in-phishing-attack/articleshow/93742172.cms retrieved on Jan 03 2025
- https://indianexpress.com/article/cities/mumbai/vishing-case-retired-best-official-loses-lakh-claims-police-5359514/ retrieved on Jan 03 2025
- https://www.indiatoday.in/cities/delhi/story/delhi-police-busts-pan-india-racket-of-online-kyc-frauds-arrests-23-1931698-2022-03-31 retrieved on Jan 03 2025
- https://www.hindustantimes.com/india-news/singapore-jails-3-indian-students-in-transnational-money-mule-syndicate-case-101641461223297.html retrieved on Jan 03 2025