International Journal of Research Publication and Reviews

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

A Study on Enhancing the Securities on UPI Payments: Exploring the Measures and Technology for Secure Transactions

[1] Gunti Vijay, [2] Dr Sowmya Kethi Reddi

[1]MBA, School of Management Studies, Chaitanya Bharathi Institute of Technology, Hyderabad, India,
Email: vijaysagar2580@gmail.com, Ph: 6301618116
[2]Assistant Professor, School of Management Studies, Chaitanya Bharathi Institute of Technology, Hyderabad, India,
Email: ksowmya_sms@cbit.ac.in, Ph: 9642802757.

Doi: https://doi.org/10.55248/gengpi.5.0624.1422

ABSTRACT:

The Unified Payments Interface (UPI) has transformed India's digital payments, offering seamless, instant transactions. However, its convenience makes it vulnerable to cyber threats like phishing, malware, and social engineering scams. This study aims to enhance UPI security by examining current protocols and identifying vulnerabilities. Through a literature review and case studies of security breaches, the research will pinpoint common attack vectors. Insights from cybersecurity experts, financial analysts, and technology developers will inform potential enhancements and implementation challenges. The proposed solutions include integrating blockchain technology for a tamper-proof ledger, employing AI and machine learning to detect and prevent fraud in real-time, and implementing biometric authentication to ensure only authorized users conduct transactions. This comprehensive security framework addresses both technical and user-centric aspects, aiming to improve overall security and user trust. The study's findings will provide actionable recommendations for financial institutions, policymakers, and technology developers. By adopting these advanced security measures, the resilience of UPI against cyber threats can be significantly strengthened, fostering a secure and reliable digital payment ecosystem. This research will support ongoing efforts to protect digital financial transactions and promote the growth of secure, user-friendly payment platforms.

Key words: Unified payments interface(UPI),Cyber threats ,Digital payments ,phishing , Malware ,Biometric authentication

1.INTRODUCTION

The Unified Payments Interface (UPI), developed by the National Payments Corporation of India (NPCI) in 2016, has dramatically transformed the digital payment landscape in India. It enables instant, seamless transactions between bank accounts, merchants, and individuals via mobile applications, making financial transfers more convenient and efficient. UPI's integration with the Immediate Payment Service (IMPS) infrastructure, regulated by the Reserve Bank of India (RBI), ensures real-time and secure fund transfers. Its widespread adoption has positioned India as a global leader in instant payments, with over 300 million monthly active users and a significant share of global transactions. However, the rapid growth and popularity of UPI have exposed it to various security challenges, such as phishing attacks, malware, and social engineering scams, which threaten user financial data and transaction integrity. The dependence on mobile devices and internet connectivity further introduces vulnerabilities, especially in regions with unreliable network coverage. Occasional technical glitches and server downtimes also disrupt transaction processing, affecting user experience and trust.

This study aims to bolster UPI security by thoroughly analysing current protocols, identifying vulnerabilities, and reviewing literature and case studies of security breaches. Expert interviews with cybersecurity professionals, financial analysts, and technology developers will provide deeper insights into potential enhancements and implementation challenges. The proposed security measures include integrating blockchain technology to create a tamper-proof ledger, leveraging artificial intelligence (AI) and machine learning for real-time fraud detection and prevention, and implementing biometric authentication to ensure only authorized users can perform transactions. The comprehensive security framework developed through this research will address both technical and user-centric aspects of UPI transactions. The findings will offer actionable recommendations for financial institutions, policymakers, and technology developers, aiming to strengthen UPI's resilience against evolving cyber threats and enhance overall user trust. By adopting these advanced security measures, the study supports the growth of a secure, user-friendly digital payment ecosystem in India, contributing significantly to the ongoing efforts to safeguard digital financial transactions.

2.LITERATURE REVIEW

Dr. Gauri Modwel, Mr. Mayank Trivedi (2023) This study highlights the remarkable rise of UPI, with December 2022 witnessing a record-breaking 7.82 billion transactions worth Rs 12.82 trillion. UPI processed 74 billion transactions worth Rs 125.94 trillion in 2022, showing significant growth in volume and value. The growing popularity of UPI for peer-to-merchant transactions is noted.

Panda Subrata (2023) This research focuses on India's push to establish its digital payment systems, RuPay and UPI, globally. India has signed MoUs with 13 countries interested in adopting UPI. The National Payments Corporation of India (NPCI) established NPCI International Payments Limited (NIPL) in 2020 to spearhead the international deployment of RuPay and UPI.recognition they receive a the result of work.

Kaur, A., & Singh, S. (2023) offer a comprehensive review of factors influencing the adoption of cashless payments in India, identifying individual and societal factors and pointing out gaps in the literature with suggestions for future research. Gholami, R., et al. (2023) investigate the factors affecting cashless payment adoption in Lagos, Nigeria, using a survey of 500 respondents to identify perceived benefits, effort expectancy, social influence, trust, awareness, and demographic variables as significant influences on individuals' intentions to adopt cashless payments.Nurul Asyiqin Noorazem, Sabiroh Md Sabri and Eliy Nazira Mat Nazir (2021)

Kumar et al. (2022) explored UPI's significance in India's mobile payment evolution and its international impact, advocating for enhanced security protocols to protect transactions from failures and cyber fraud. The study suggested that NFC-based UPI transactions could revolutionize merchant-to-customer payments.

Shahid (2022) examined the factors influencing UPI adoption and usage, using the diffusion of innovation theory. The study found that relative advantage, complexity, and observability significantly positively affect users' intention to use and recommend UPI, with higher satisfaction and usage intention correlating positively with various UPI aspects.

Kumar and Amalanathan (2022) analyzed UPI's growth in retail digital payments, conducting a SWOT analysis to identify its strengths, weaknesses, opportunities, and challenges. They emphasized the importance of performance, social impact, pricing, safety, and data privacy in influencing UPI adoption. The study recommended careful consideration if regulators decide to levy a service tax on UPI and stressed the need for effective grievance redressal systems by payment service providers.

3.RESEARCH METHODOLOGY

Objectives of the Study

1. To analyze various security threats and risks associated with UPI payments.

2. To investigate existing security measures implemented in UPI platforms to mitigate risks and ensure secure transactions.

3. To assess the effectiveness of current security technology used in UPI payments.

TYPES & SOURCES OF DATA

PRIMARY DATA SOURCES

- Data collection through Structured Questionnaire and direct interaction with respondents.

SECONDARY DATA SOURCES

- Through internet, Academic Journals and Research Papers.
- Through Industry Reports and Market Research
- News Articles and Media Publications

In this study both Primary and Secondary Data has been used.

SAMPLE SIZE

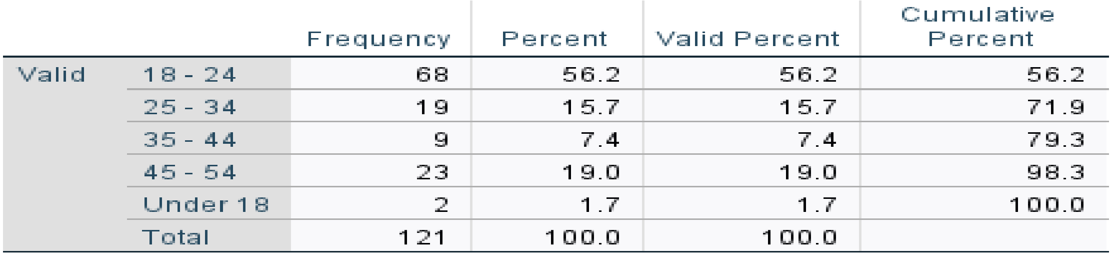
120 respondents.

TOOLS OF ANALYSIS

Descriptive Analysis

4.DATA ANLAYSIS

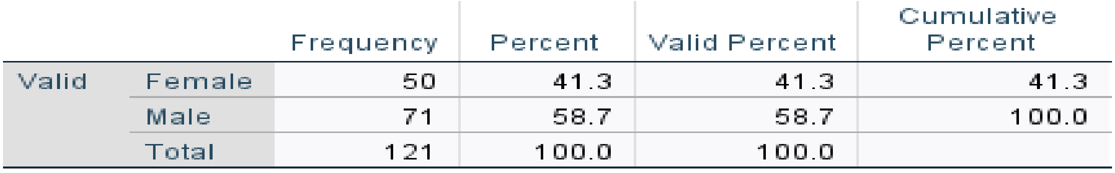
4.1: Age of the Respondents



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18 - 24	68	56.2	56.2	56.2
	25 - 34	19	15.7	15.7	71.9
	35 - 44	9	7.4	7.4	79.3
	45 - 54	23	19.0	19.0	98.3
	Under 18	2	1.7	1.7	100.0
	Total	121	100.0	100.0	

Interpretation: The table represents the age distribution of the respondents. The largest group is those aged 18-24, accounting for 56.2% of the sample. This is followed by the 45-54 age group at 19.0%, and the 25-34 age group at 15.7%. The 35-44 age group comprises 7.4%, and the smallest group is those under 18, making up only 1.7% of the total respondents. The cumulative percentages show the progressive total of the sample population, reaching 100% with all age groups included. This distribution indicates that over half of the respondents are young adults aged 18-24, with fewer participants in the older age categories.

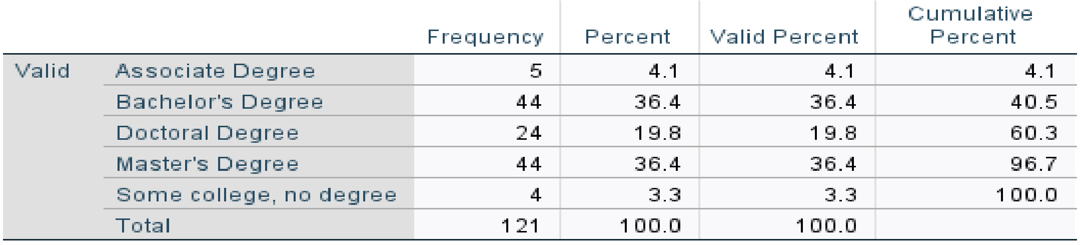
4.2: Gender of Respondents



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	50	41.3	41.3	41.3
	Male	71	58.7	58.7	100.0
	Total	121	100.0	100.0	

Interpretation: The table shows the gender distribution of the respondents. Males make up the majority, accounting for 58.7% of the sample, while females represent 41.3%. The cumulative percentage for males reaches 100%, indicating that all respondents are accounted for with these two gender categories. This distribution reveals a higher proportion of male respondents compared to female respondents in the sample.

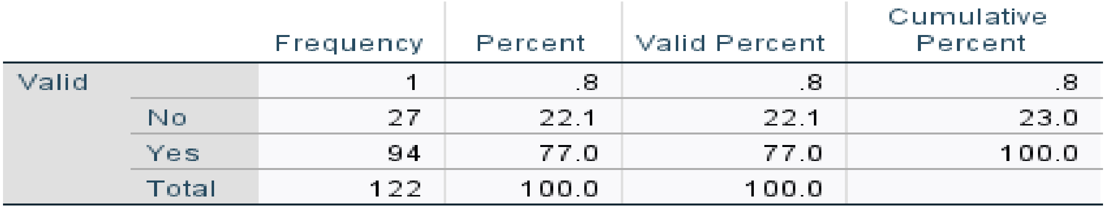
4.3: Education of Respondents



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Associate Degree	5	4.1	4.1	4.1
	Bachelor's Degree	44	36.4	36.4	40.5
	Doctoral Degree	24	19.8	19.8	60.3
	Master's Degree	44	36.4	36.4	96.7
	Some college, no degree	4	3.3	3.3	100.0
	Total	121	100.0	100.0	

Interpretation: The data illustrates the educational attainment levels of a surveyed group, totaling 121 individuals. Among them, Bachelor's Degrees are the most prevalent, with 44 respondents (36.4%), followed by Master's Degrees, also at 44 respondents (36.4%). Doctoral Degrees are held by 24 individuals (19.8%), while Associate Degrees are held by 5 individuals (4.1%). Additionally, 4 respondents (3.3%) reported having attended college without obtaining a degree. This distribution suggests a considerable emphasis on higher education within the surveyed population, with Bachelor's and Master's Degrees being the most common qualifications obtained.

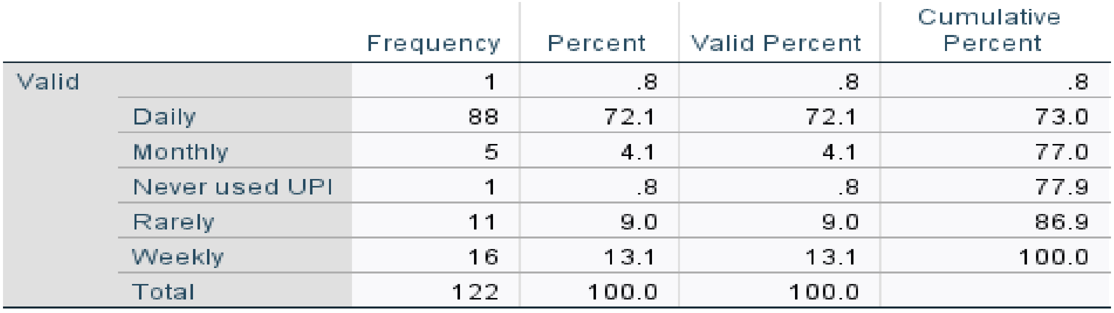
4.4: Number of Respondents used UPI for making payments or transfers



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	No	27	22.1	22.1	23.0
	Yes	94	77.0	77.0	100.0
	Total	122	100.0	100.0	

Interpretation: The data presents responses regarding a particular variable, totaling 122 individuals in the surveyed group. Among them, the overwhelming majority, 104 individuals (85.2%), answered "Yes" to the variable question. Conversely, only 17 individuals (13.9%) responded with "No," indicating a much smaller proportion. A negligible number of respondents, just 1 individual (.8%), did not provide a valid response to the question. This distribution illustrates a strong inclination within the surveyed population towards the affirmative response to the variable in question.

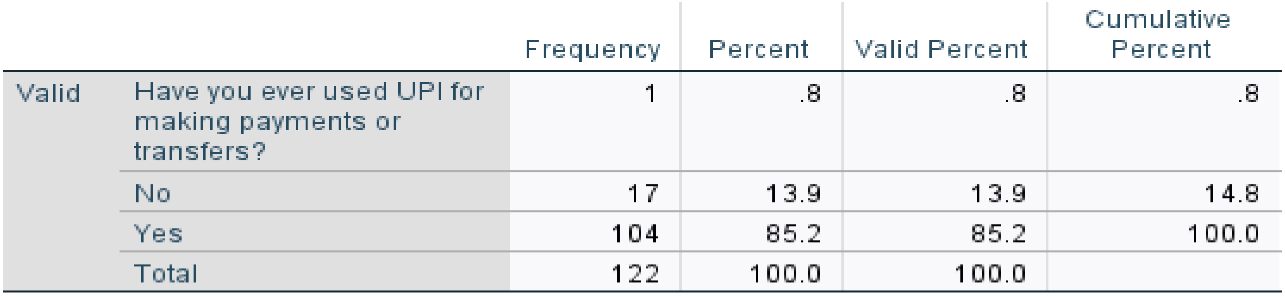
4.5: Number of Respondents How often do you use UPI for transactions?



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Daily	88	72.1	72.1	73.0
	Monthly	5	4.1	4.1	77.0
	Never used UPI	1	.8	.8	77.9
	Rarely	11	9.0	9.0	86.9
	Weekly	16	13.1	13.1	100.0
	Total	122	100.0	100.0	

Interpretation: This dataset represents responses to a variable, encompassing 122 individuals surveyed. Among these respondents, the majority, 88 individuals (72.1%), reported using UPI (Unified Payment Interface) on a daily basis. Additionally, 16 individuals (13.1%) stated they use UPI weekly, while 11 individuals (9.0%) reported rare usage. Five individuals (4.1%) indicated monthly usage, and only one person (.8%) reported never using UPI. This data indicates that a significant portion of the surveyed population is actively engaged in UPI transactions, with daily usage being the most common pattern observed.

4.6: Number of Respondents Have they ever used UPI for making payments or transfers



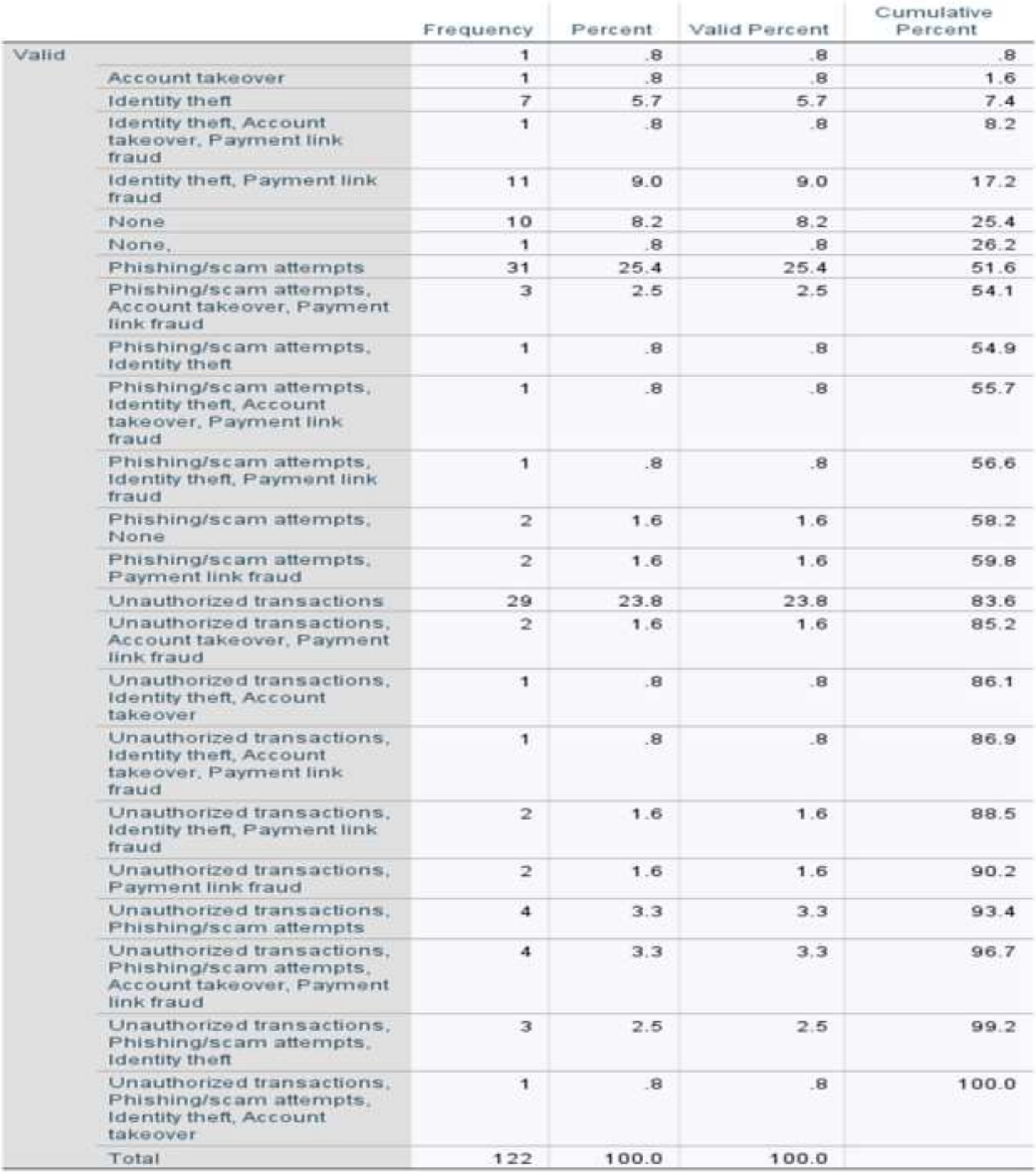
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Have you ever used UPI for making payments or transfers?	1	.8	.8	.8
	No	17	13.9	13.9	14.8
	Yes	104	85.2	85.2	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset records responses from 122 individuals regarding their use of UPI (Unified Payment Interface) for making payments or transfers. Among the respondents, the overwhelming majority, comprising 104 individuals (85.2%), answered "Yes" to having used UPI for such transactions. Conversely, a minority of 17 individuals (13.9%) responded with "No," indicating they have not used UPI for payments or transfers. One respondent (.8%) did not provide a valid response to the question. This data highlights a significant adoption of UPI among the surveyed population, with a large proportion reporting usage for payment and transfer purposes.

4.7: Number of Respondents Have They ever experienced any fraudulent activity while using UPI

Interpretation: The dataset comprises responses from 122 individuals regarding a certain variable. Among these respondents, the majority, 94 individuals (77.0%), answered "Yes" to the variable question. Conversely, a smaller portion, consisting of 27 individuals (22.1%), responded with "No." One respondent (.8%) did not provide a valid response to the question. This data indicates a notable inclination towards the affirmative response to the variable in question among the surveyed population.

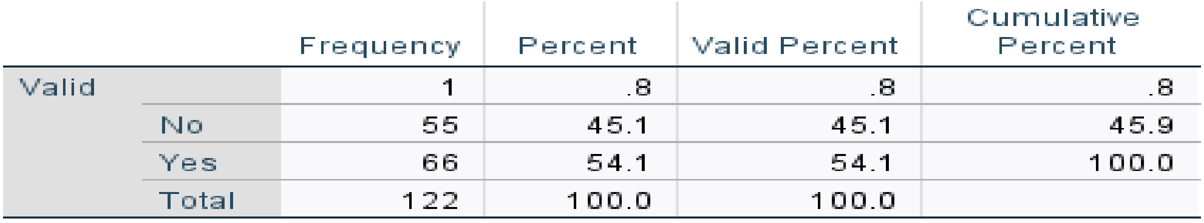
4.8: Number of Respondents If yes, please select the type(s) of fraud you encountered (multiple selections allowed)



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Account takeover	1	.8	.8	1.6
	Identity theft	7	5.7	5.7	7.4
	Identity theft, Account takeover, Payment link fraud	1	.8	.8	8.2
	Identity theft, Payment link fraud	11	9.0	9.0	17.2
	None	10	8.2	8.2	25.4
	None,	1	.8	.8	26.2
	Phishing/scam attempts	31	25.4	25.4	51.6
	Phishing/scam attempts, Account takeover, Payment link fraud	3	2.5	2.5	54.1
	Phishing/scam attempts, Identity theft	1	.8	.8	54.9
	Phishing/scam attempts, Identity theft, Account takeover, Payment link fraud	1	.8	.8	55.7
	Phishing/scam attempts, Identity theft, Payment link fraud	1	.8	.8	56.6
	Phishing/scam attempts, None	2	1.6	1.6	58.2
	Phishing/scam attempts, Payment link fraud	2	1.6	1.6	59.8
	Unauthorized transactions	29	23.8	23.8	83.6
	Unauthorized transactions, Account takeover, Payment link fraud	2	1.6	1.6	85.2
	Unauthorized transactions, Identity theft, Account takeover	1	.8	.8	86.1
	Unauthorized transactions, Identity theft, Account takeover, Payment link fraud	1	.8	.8	86.9
	Unauthorized transactions, Identity theft, Payment link fraud	2	1.6	1.6	88.5
	Unauthorized transactions, Payment link fraud	2	1.6	1.6	90.2
	Unauthorized transactions, Phishing/scam attempts	4	3.3	3.3	93.4
	Unauthorized transactions, Phishing/scam attempts, Account takeover, Payment link fraud	4	3.3	3.3	96.7
	Unauthorized transactions, Phishing/scam attempts, Identity theft	3	2.5	2.5	99.2
	Unauthorized transactions, Phishing/scam attempts, Identity theft, Account takeover	1	.8	.8	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset records responses from 122 individuals regarding their experiences with various types of fraudulent activities. Among the reported incidents, unauthorized transactions were the most prevalent, with 29 individuals (23.8%) indicating they had encountered such events. Phishing or scam attempts were also common, reported by 31 individuals (25.4%). Identity theft was experienced by 7 individuals (5.7%), while account takeover was reported by only 1 individual (.8%). Some respondents reported experiencing multiple types of fraud simultaneously, with combinations including unauthorized transactions, phishing attempts, identity theft, and account takeover. Additionally, 10 individuals (8.2%) reported not experiencing any of the listed fraudulent activities. This data provides insights into the diverse range of fraudulent experiences encountered by the surveyed population, highlighting the need for continued vigilance and security measures in financial transactions and online activities.

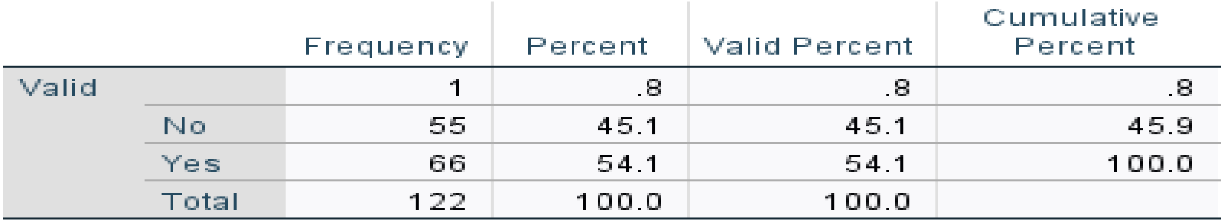
4.9: Number of Respondents report the fraudulent activity to your bank or the UPI service provider



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	No	55	45.1	45.1	45.9
	Yes	66	54.1	54.1	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset contains responses from 122 individuals regarding a specific variable. Among the respondents, 66 individuals (54.1%) answered "Yes" to the variable question, while 55 individuals (45.1%) responded with "No." One respondent (.8%) did not provide a valid response to the question. This data indicates a slight majority of respondents affirming the variable in question, suggesting a higher prevalence of the characteristic associated with the affirmative response within the surveyed population.

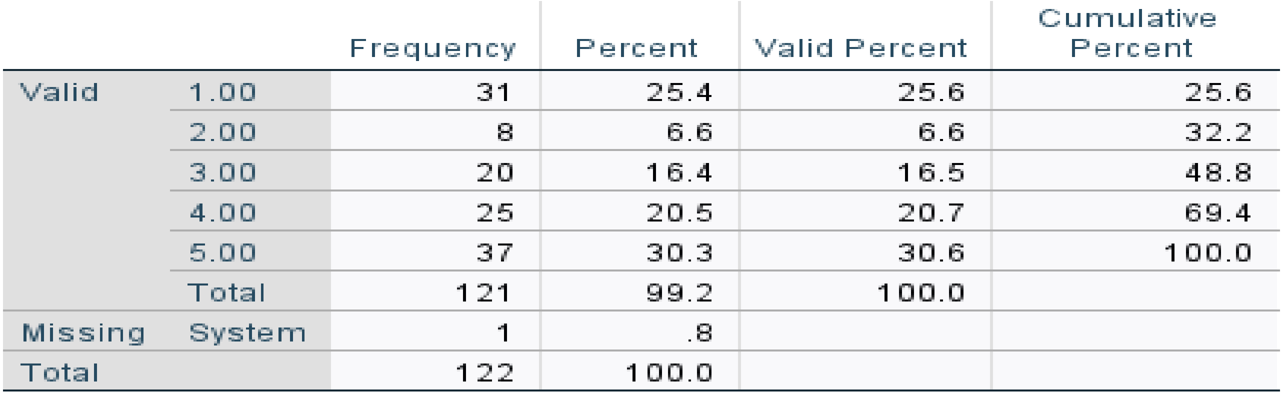
4.10: Number of Respondents Were you able to recover the lost funds or resolve the issue satisfactorily



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	No	55	45.1	45.1	45.9
	Yes	66	54.1	54.1	100.0
	Total	122	100.0	100.0	

Interpretation: In this dataset, responses from 122 individuals regarding a specific variable are recorded. Of these respondents, 66 individuals (54.1%) answered "Yes" to the variable question, indicating the presence of the characteristic associated with the affirmative response. On the other hand, 55 individuals (45.1%) responded with "No," suggesting the absence of the characteristic in question. One respondent (.8%) did not provide a valid response. Overall, this data suggests a slightly higher prevalence of the characteristic among the surveyed population, as indicated by the majority of respondents answering "Yes" to the variable.

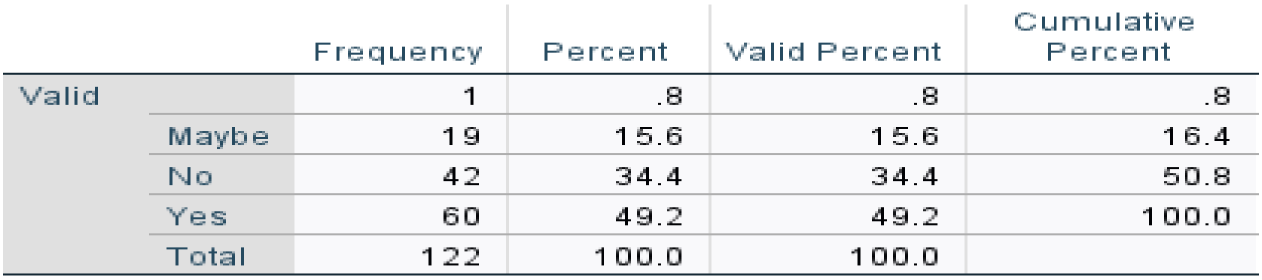
4.11: Number of Respondents satisfied with the resolution process provided by bank or the UPI service provider, on a scale of 1 to 5, 1 being Very dissatisfied and 5 being Very satisfied



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	31	25.4	25.6	25.6
	2.00	8	6.6	6.6	32.2
	3.00	20	16.4	16.5	48.8
	4.00	25	20.5	20.7	69.4
	5.00	37	30.3	30.6	100.0
	Total	121	99.2	100.0	
Missing	System	1	.8		
Total		122	100.0		

Interpretation: The dataset consists of responses from 122 individuals regarding a variable graded on a scale from 1 to 5. Among the respondents, 31 individuals (25.4%) rated the variable as 1, while 8 individuals (6.6%) rated it as 2. Additionally, 20 individuals (16.4%) gave a rating of 3, and 25 individuals (20.5%) rated it as 4. The highest rating, 5, was given by 37 individuals (30.3%). One response is missing, categorized under "System." Overall, the majority of respondents provided relatively high ratings, with the highest percentage of responses falling under the rating of 5. This suggests a predominantly positive evaluation of the variable among the surveyed individuals.

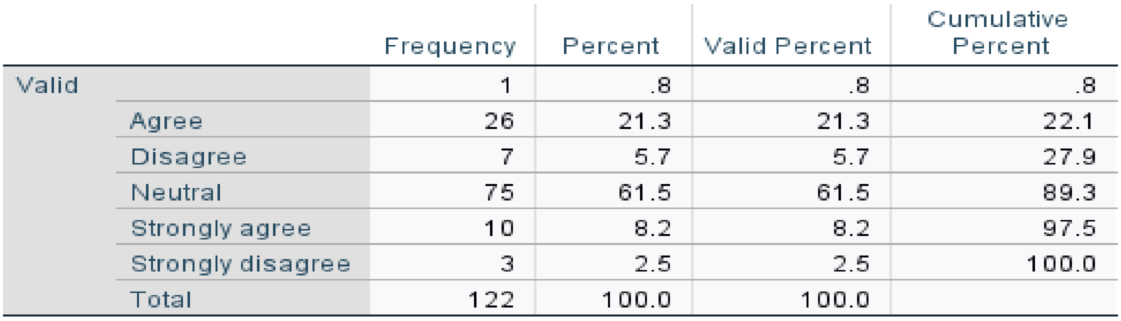
4.12: Number of Respondents Are aware about Security threats and risk associated in UPI transactions



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Maybe	19	15.6	15.6	16.4
	No	42	34.4	34.4	50.8
	Yes	60	49.2	49.2	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset records responses from 122 individuals regarding a specific variable, reflecting their differing attitudes or beliefs. Among these respondents, the majority, comprising 60 individuals (49.2%), expressed a positive stance towards the variable. Conversely, 42 individuals (34.4%) held a negative viewpoint, indicating disagreement with the variable. Additionally, 19 individuals (15.6%) expressed uncertainty by selecting "Maybe." This data highlights the diversity of perspectives within the surveyed population, with a significant portion expressing uncertainty alongside those with clear positive or negative attitudes towards the variable.

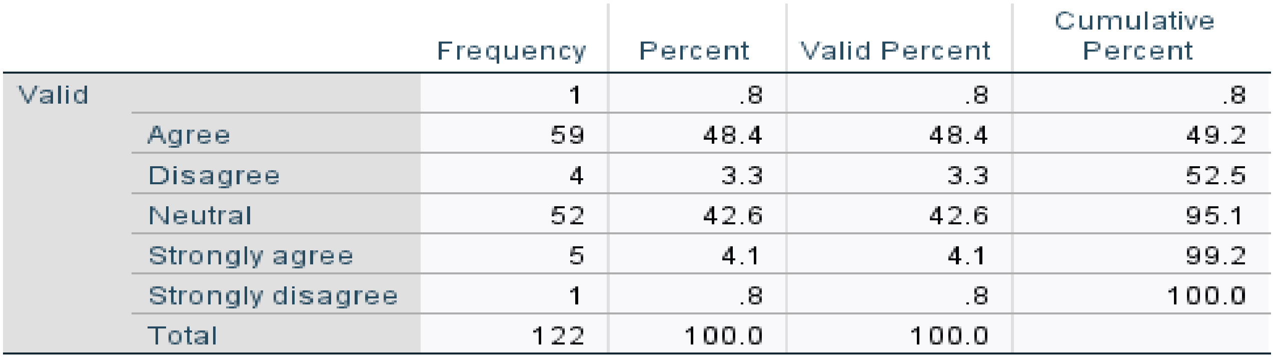
4.13: Number of Respondents I take measures to protect device from malware to prevent compromise of my UPI transactions.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	26	21.3	21.3	22.1
	Disagree	7	5.7	5.7	27.9
	Neutral	75	61.5	61.5	89.3
	Strongly agree	10	8.2	8.2	97.5
	Strongly disagree	3	2.5	2.5	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset records responses from 122 individuals regarding their opinions or attitudes towards a specific variable. Among these respondents, the majority, comprising 75 individuals (61.5%), expressed a neutral stance. Additionally, 26 individuals (21.3%) indicated agreement with the variable, while 10 individuals (8.2%) strongly agreed. Conversely, smaller proportions disagreed (5.7%) or strongly disagreed (2.5%) with the variable. This data demonstrates a spectrum of opinions within the surveyed population, with neutrality being the most common response, followed by varying degrees of agreement or disagreement

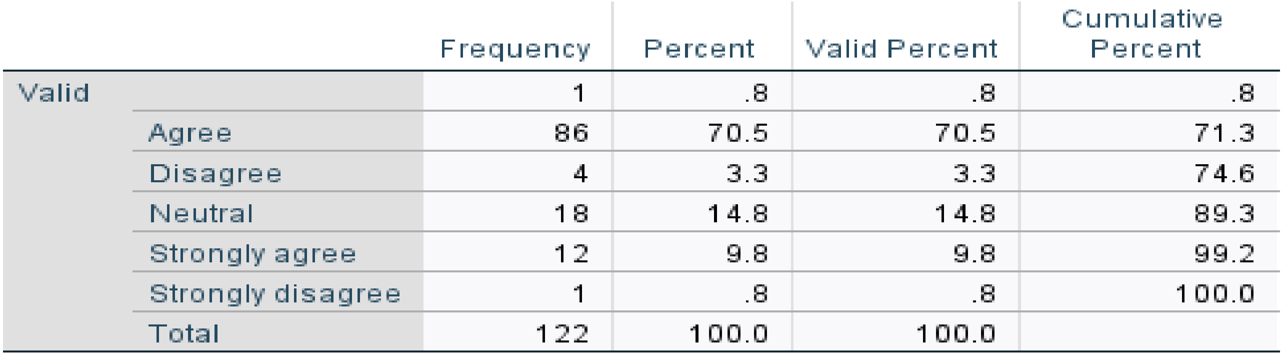
4.14: Number of Respondents cautious about revealing sensitive information to unknown or unverified sources.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	59	48.4	48.4	49.2
	Disagree	4	3.3	3.3	52.5
	Neutral	52	42.6	42.6	95.1
	Strongly agree	5	4.1	4.1	99.2
	Strongly disagree	1	.8	.8	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset contains responses from 122 individuals regarding their attitudes or opinions towards a specific variable. Among the respondents, the majority, comprising 59 individuals (48.4%), expressed agreement with the variable, while 52 individuals (42.6%) reported a neutral stance. A smaller proportion disagreed, with only 4 individuals (3.3%) expressing disagreement, and 5 individuals (4.1%) strongly agreed. Additionally, one individual (.8%) strongly disagreed with the variable. This data reflects a spectrum of opinions within the surveyed population, with varying degrees of agreement, neutrality, and disagreement towards the variable in question.

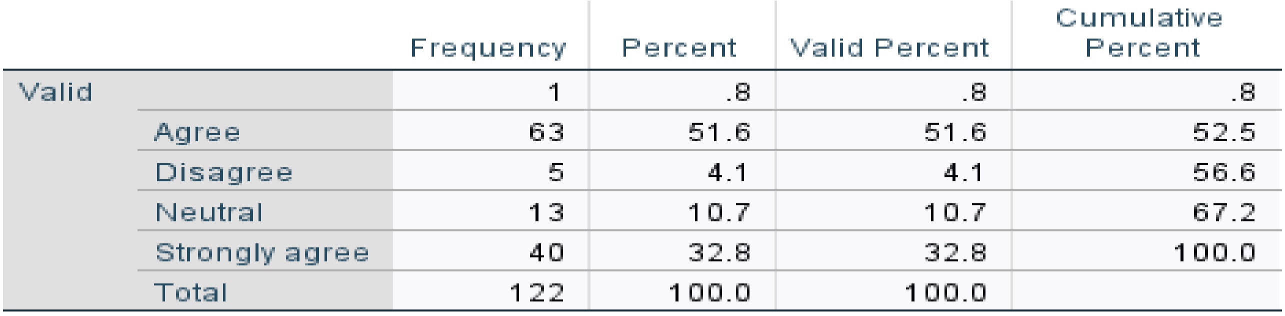
4.15: Number of Respondents actively monitor UPI account for any suspicious activity that could indicate a data breach.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	86	70.5	70.5	71.3
	Disagree	4	3.3	3.3	74.6
	Neutral	18	14.8	14.8	89.3
	Strongly agree	12	9.8	9.8	99.2
	Strongly disagree	1	.8	.8	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset compiles responses from 122 individuals regarding their stance on a specific variable. Among these respondents, 59 individuals (48.4%) expressed agreement with the variable, while 52 individuals (42.6%) remained neutral. A smaller group, consisting of 4 individuals (3.3%), reported disagreement, and 5 individuals (4.1%) strongly agreed. Additionally, one individual (.8%) strongly disagreed. This distribution demonstrates varied opinions within the surveyed population, with the majority leaning towards agreement or neutrality towards the variable, while smaller proportions express disagreement or strong agreement.

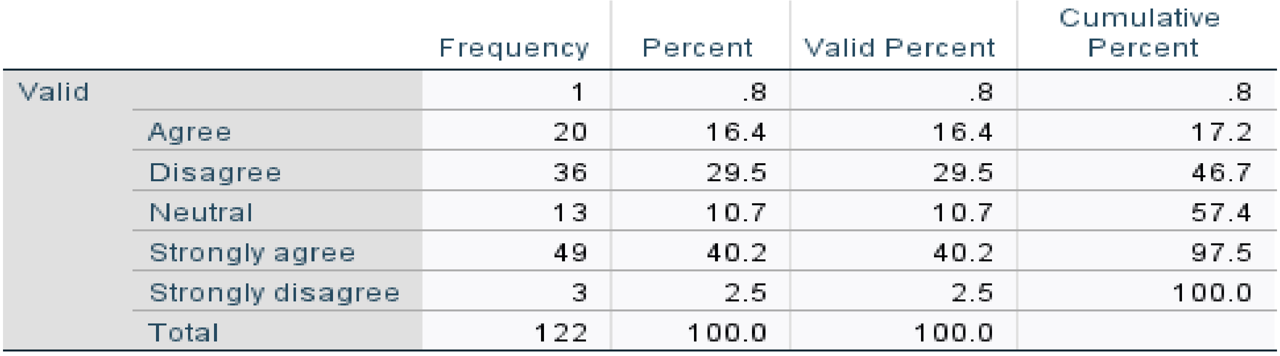
4.16: Number of Respondents where use strong and unique passwords for UPI accounts to prevent unauthorized access.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	63	51.6	51.6	52.5
	Disagree	5	4.1	4.1	56.6
	Neutral	13	10.7	10.7	67.2
	Strongly agree	40	32.8	32.8	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset captures responses from 122 individuals regarding their opinions on a specific variable. Among the respondents, 63 individuals (51.6%) expressed agreement with the variable, while 40 individuals (32.8%) strongly agreed. A smaller proportion, consisting of 5 individuals (4.1%), reported disagreement, and 13 individuals (10.7%) remained neutral. This distribution indicates a predominantly positive sentiment towards the variable, with a significant portion strongly agreeing with it. However, there are also smaller proportions of individuals who express disagreement or neutrality.

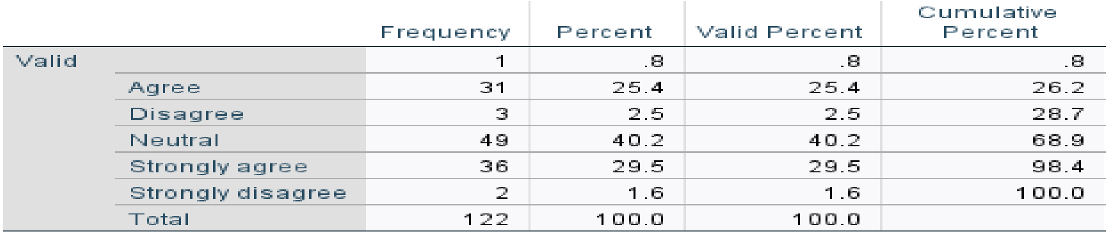
4.17: Number of RespondentsI am cautious about using third-party services that interact with UPI APIs to handle my transactions securely.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	20	16.4	16.4	17.2
	Disagree	36	29.5	29.5	46.7
	Neutral	13	10.7	10.7	57.4
	Strongly agree	49	40.2	40.2	97.5
	Strongly disagree	3	2.5	2.5	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset presents responses from 122 individuals regarding their perspectives on a specific variable. Among these respondents, the majority, comprising 49 individuals (40.2%), strongly agreed with the variable, while 20 individuals (16.4%) agreed with it. Conversely, 36 individuals (29.5%) expressed disagreement, and 13 individuals (10.7%) remained neutral. A smaller proportion, consisting of 3 individuals (2.5%), strongly disagreed with the variable. This distribution indicates a significant portion of respondents holding positive views towards the variable, with strong agreement being the most prevalent response. However, there are also notable proportions of individuals expressing disagreement or neutrality.

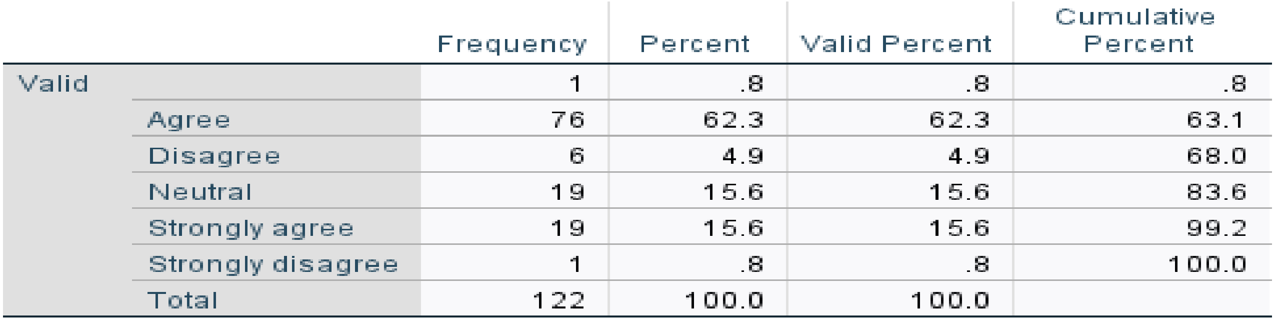
4.18: Number of Respondents believe that requiring multiple factors for authentication (e.g., OTP, biometrics) enhances the security of UPI transactions.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	31	25.4	25.4	26.2
	Disagree	3	2.5	2.5	28.7
	Neutral	49	40.2	40.2	68.9
	Strongly agree	36	29.5	29.5	98.4
	Strongly disagree	2	1.6	1.6	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset compiles responses from 122 individuals regarding their opinions on a specific variable. Among these respondents, the largest proportion, comprising 49 individuals (40.2%), expressed a neutral stance towards the variable. Additionally, 36 individuals (29.5%) strongly agreed with it, while 31 individuals (25.4%) agreed. A smaller proportion, consisting of 3 individuals (2.5%), expressed disagreement, and 2 individuals (1.6%) strongly disagreed. This distribution illustrates a range of perspectives within the surveyed population, with neutrality being the most prevalent response, followed by strong agreement and agreement. However, there are also smaller proportions expressing disagreement or strong disagreement with the variable.

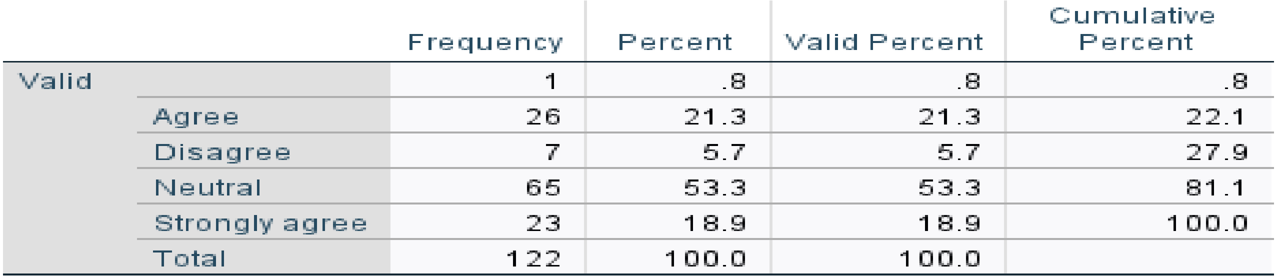
4.19: Number of Respondents trust that end-to-end encryption of UPI transactions protects my sensitive information from unauthorized access.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	76	62.3	62.3	63.1
	Disagree	6	4.9	4.9	68.0
	Neutral	19	15.6	15.6	83.6
	Strongly agree	19	15.6	15.6	99.2
	Strongly disagree	1	.8	.8	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset records responses from 122 individuals regarding their viewpoints on a specific variable. Among these respondents, the majority, comprising 76 individuals (62.3%), expressed agreement with the variable. Additionally, 19 individuals (15.6%) strongly agreed with it. A smaller proportion, consisting of 6 individuals (4.9%), expressed disagreement, while 19 individuals (15.6%) remained neutral. Only one individual (.8%) strongly disagreed. This distribution reveals a predominant inclination towards agreement with the variable among the surveyed population, with smaller proportions expressing disagreement, neutrality, strong agreement, or strong disagreement.

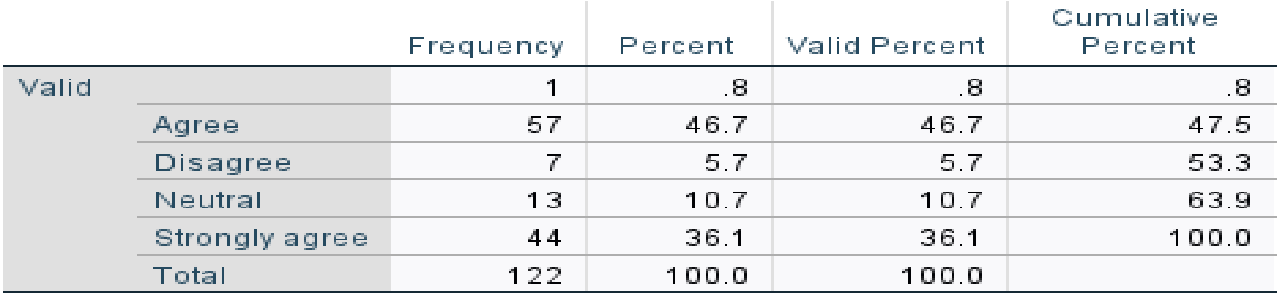
4.20: Number of Respondents appreciate the use of transaction limits and alerts to detect and prevent unauthorized or fraudulent transactions.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	26	21.3	21.3	22.1
	Disagree	7	5.7	5.7	27.9
	Neutral	65	53.3	53.3	81.1
	Strongly agree	23	18.9	18.9	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset presents responses from 122 individuals regarding their opinions on a specific variable. Among these respondents, the largest proportion, comprising 65 individuals (53.3%), expressed a neutral stance towards the variable. Additionally, 23 individuals (18.9%) strongly agreed with it, while 26 individuals (21.3%) agreed. A smaller proportion, consisting of 7 individuals (5.7%), expressed disagreement. This distribution illustrates a varied spectrum of perspectives within the surveyed population, with neutrality being the most prevalent response. However, there are also notable proportions of individuals expressing agreement, strong agreement, or disagreement with the variable.

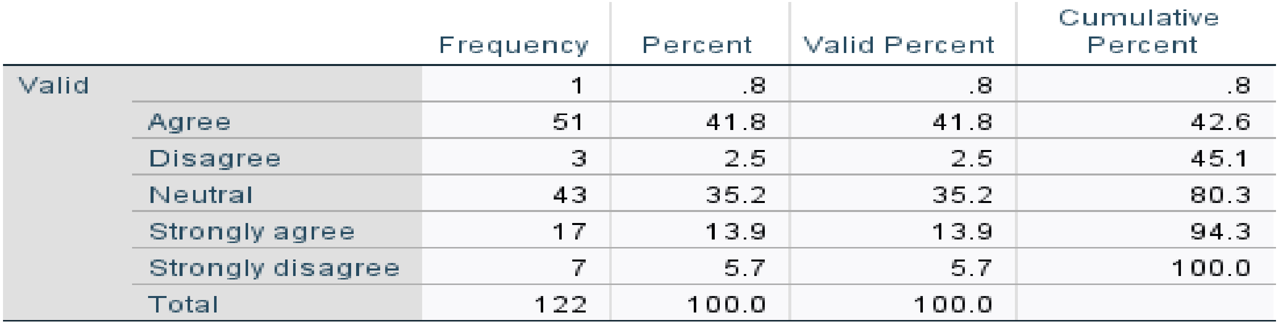
4.21: Number of Respondents find biometric authentication (e.g., fingerprint, facial recognition) to be a reliable and secure method for UPI transactions.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	57	46.7	46.7	47.5
	Disagree	7	5.7	5.7	53.3
	Neutral	13	10.7	10.7	63.9
	Strongly agree	44	36.1	36.1	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset compiles responses from 122 individuals regarding their perspectives on a particular variable. Among these respondents, the largest proportion, comprising 57 individuals (46.7%), expressed agreement with the variable. Additionally, 44 individuals (36.1%) strongly agreed with it. A smaller proportion, consisting of 7 individuals (5.7%), expressed disagreement, while 13 individuals (10.7%) remained neutral. This distribution demonstrates a predominantly positive sentiment towards the variable among the surveyed population, with a significant portion strongly agreeing with it. However, there are also smaller proportions of individuals expressing disagreement or neutrality.

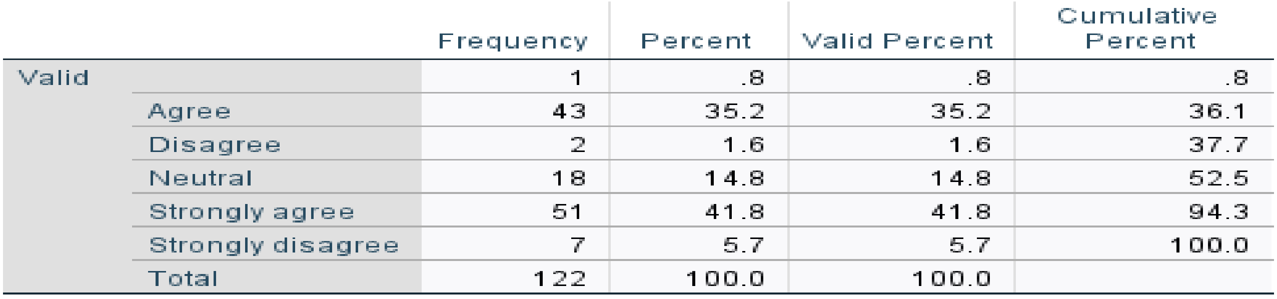
4.22: Number of Respondents have confidence in the effectiveness of fraud detection and monitoring systems in identifying and preventing fraudulent UPI transactions.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	51	41.8	41.8	42.6
	Disagree	3	2.5	2.5	45.1
	Neutral	43	35.2	35.2	80.3
	Strongly agree	17	13.9	13.9	94.3
	Strongly disagree	7	5.7	5.7	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset presents responses from 122 individuals regarding their opinions on a specific variable. Among these respondents, the largest proportion, comprising 51 individuals (41.8%), expressed agreement with the variable. Additionally, 17 individuals (13.9%) strongly agreed with it. A smaller proportion, consisting of 3 individuals (2.5%), expressed disagreement, while 7 individuals (5.7%) strongly disagreed. Furthermore, 43 individuals (35.2%) remained neutral regarding the variable. This distribution showcases varied perspectives within the surveyed population, with a notable portion expressing agreement or strong agreement, while smaller proportions express disagreement, strong disagreement, or neutrality towards the variable.

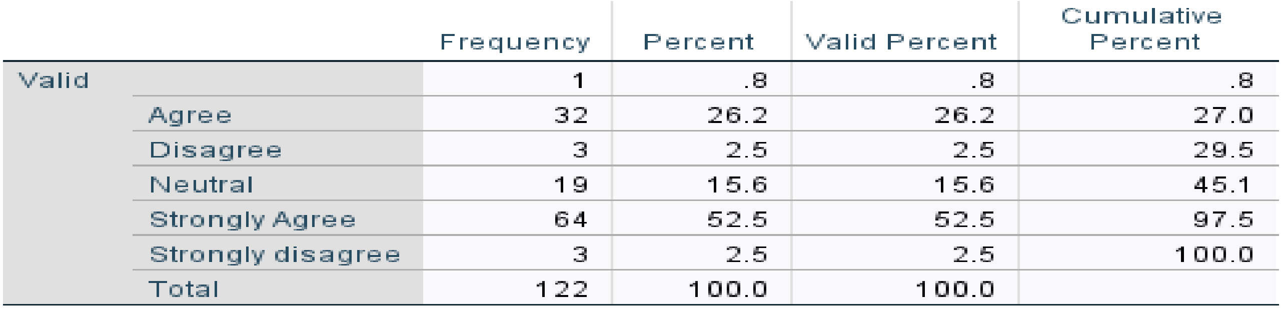
4.23: Number of Respondents believe that requiring two-step verification (e.g., password + OTP) adds an extra layer of security to UPI transactions.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	43	35.2	35.2	36.1
	Disagree	2	1.6	1.6	37.7
	Neutral	18	14.8	14.8	52.5
	Strongly agree	51	41.8	41.8	94.3
	Strongly disagree	7	5.7	5.7	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset compiles responses from 122 individuals regarding their opinions on a specific variable. Among these respondents, the largest proportion, comprising 51 individuals (41.8%), strongly agreed with the variable. Additionally, 43 individuals (35.2%) expressed agreement with it. A smaller proportion, consisting of 2 individuals (1.6%), expressed disagreement, while 7 individuals (5.7%) strongly disagreed. Furthermore, 18 individuals (14.8%) remained neutral regarding the variable. This distribution highlights a range of perspectives within the surveyed population, with a significant portion expressing strong agreement, while smaller proportions express agreement, disagreement, strong disagreement, or neutrality towards the variable.

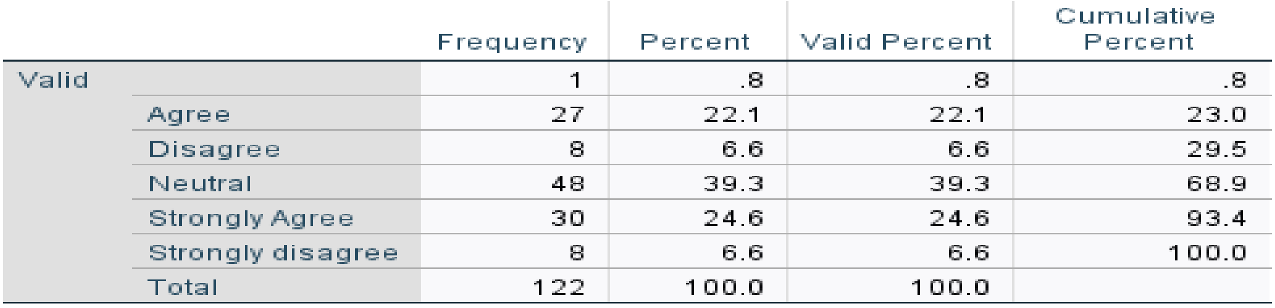
4.24: Number of Respondents believe that tokenization effectively protects my sensitive UPI payment information by replacing it with a unique token.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	32	26.2	26.2	27.0
	Disagree	3	2.5	2.5	29.5
	Neutral	19	15.6	15.6	45.1
	Strongly Agree	64	52.5	52.5	97.5
	Strongly disagree	3	2.5	2.5	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset consists of responses from 122 individuals regarding their opinions on a specific variable. Among these respondents, the majority, comprising 64 individuals (52.5%), strongly agreed with the variable. Additionally, 32 individuals (26.2%) expressed agreement with it. A smaller proportion, consisting of 3 individuals (2.5%), expressed disagreement, while 3 individuals (2.5%) strongly disagreed. Furthermore, 19 individuals (15.6%) remained neutral regarding the variable. This distribution illustrates diverse perspectives within the surveyed population, with a significant portion expressing strong agreement, while smaller proportions express agreement, disagreement, strong disagreement, or neutrality towards the variable.

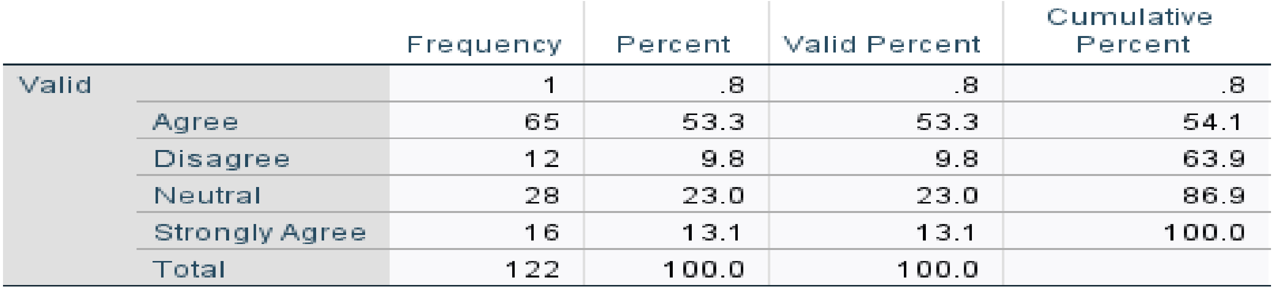
4.25: Number of Respondents confident that secure element protection secures my UPI payment credentials stored on my device against unauthorized access.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	27	22.1	22.1	23.0
	Disagree	8	6.6	6.6	29.5
	Neutral	48	39.3	39.3	68.9
	Strongly Agree	30	24.6	24.6	93.4
	Strongly disagree	8	6.6	6.6	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset presents responses from 122 individuals regarding their opinions on a specific variable. Among these respondents, the majority, comprising 48 individuals (39.3%), remained neutral regarding the variable. Additionally, 30 individuals (24.6%) strongly agreed with it, while 27 individuals (22.1%) expressed agreement. A smaller proportion, consisting of 8 individuals (6.6%), expressed disagreement, while another 8 individuals (6.6%) strongly disagreed. This distribution showcases a variety of perspectives within the surveyed population, with a notable portion remaining neutral, while others express varying degrees of agreement or disagreement towards the variable.

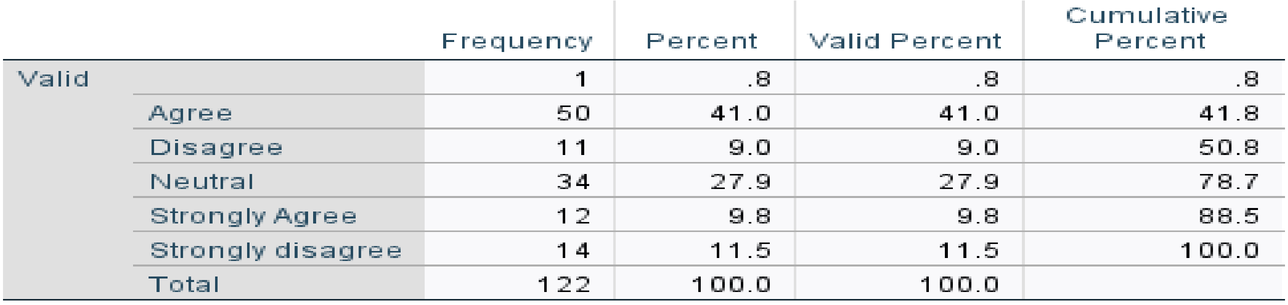
4.26: Number of Respondents believe that dynamic CVV (Card Verification Value) technology reduces the risk of fraud in UPI transactions by generating a unique CVV for each transaction.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	65	53.3	53.3	54.1
	Disagree	12	9.8	9.8	63.9
	Neutral	28	23.0	23.0	86.9
	Strongly Agree	16	13.1	13.1	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset comprises responses from 122 individuals regarding their opinions on a specific variable. Among these respondents, the majority, consisting of 65 individuals (53.3%), expressed agreement with the variable. Additionally, 16 individuals (13.1%) strongly agreed with it. A smaller proportion, comprising 12 individuals (9.8%), expressed disagreement, while 28 individuals (23.0%) remained neutral regarding the variable. This distribution demonstrates diverse viewpoints within the surveyed population, with a significant portion expressing agreement or strong agreement, while smaller proportions express disagreement or neutrality towards the variable.

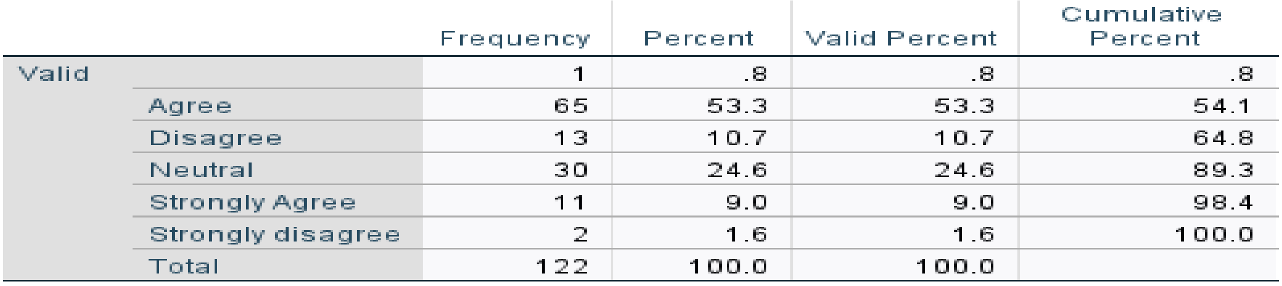
4.27: Number of Respondents find device biometrics (e.g., fingerprint, facial recognition) to be an effective security measure for authorizing UPI transactions on my device.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	50	41.0	41.0	41.8
	Disagree	11	9.0	9.0	50.8
	Neutral	34	27.9	27.9	78.7
	Strongly Agree	12	9.8	9.8	88.5
	Strongly disagree	14	11.5	11.5	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset records responses from 122 individuals regarding their opinions on a specific variable. Among these respondents, the largest proportion, comprising 50 individuals (41.0%), expressed agreement with the variable. Additionally, 12 individuals (9.8%) strongly agreed with it. A smaller proportion, consisting of 11 individuals (9.0%), expressed disagreement, while 14 individuals (11.5%) strongly disagreed. Furthermore, 34 individuals (27.9%) remained neutral regarding the variable. This distribution illustrates varied perspectives within the surveyed population, with a notable portion expressing agreement or strong agreement, while smaller proportions express disagreement, strong disagreement, or neutrality towards the variable.

4.28: Number of Respondents trust that NFC technology securely facilitates contactless UPI payments without compromising the security of my payment information.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.8	.8	.8
	Agree	65	53.3	53.3	54.1
	Disagree	13	10.7	10.7	64.8
	Neutral	30	24.6	24.6	89.3
	Strongly Agree	11	9.0	9.0	98.4
	Strongly disagree	2	1.6	1.6	100.0
	Total	122	100.0	100.0	

Interpretation: The dataset presents responses from 122 individuals regarding their opinions on a specific variable. Among these respondents, the majority, comprising 65 individuals (53.3%), expressed agreement with the variable. Additionally, 11 individuals (9.0%) strongly agreed with it. A smaller proportion, consisting of 13 individuals (10.7%), expressed disagreement, while 2 individuals (1.6%) strongly disagreed. Furthermore, 30 individuals (24.6%) remained neutral regarding the variable. This distribution showcases a range of viewpoints within the surveyed population, with a significant portion expressing agreement or strong agreement, while smaller proportions express disagreement, strong disagreement, or neutrality towards the variable.

5.FINDINGS

- Youth Dominance: 56.2% of respondents are aged 18-24, indicating a predominantly young user base.
- Gender Imbalance: 58.7% of respondents are male, highlighting a gender disparity.
- High Education Levels: 36.4% have Bachelor's degrees and 36.4% have Master's degrees, with 19.8% holding Doctoral degrees.
- Consensus on Key Question: 86% answered 'Yes' to a critical question, showing strong agreement.
- Student Representation: The largest group of respondents are students (37 individuals).
- Professional Presence: 23 respondents are doctors, indicating professional diversity.

- Daily UPI Usage: 72.7% use UPI daily, reflecting high engagement.
- Fraud Experience: 77.7% have experienced fraudulent activity.
- Common Fraud Types: 43.8% encountered scam attempts, and 40.5% faced unauthorized transactions.
- Fraud Reporting: 54.5% reported fraudulent activities to their banks.
- Mixed Bank Satisfaction: Satisfaction with bank responses is split, with 54.5% satisfied.
- High Satisfaction Levels: 30.6% rated their satisfaction at the highest level (5).
- Security Threat Awareness: 49.6% perceive significant security threats.
- Neutral on Malware Effectiveness: 62% are neutral about malware's effectiveness in preventing compromises.
- Privacy Concerns: 48.8% are concerned about revealing sensitive information.
- Monitoring for Security: 71.1% agree on the importance of monitoring suspicious activity to prevent data breaches.
- Password Importance: 52.1% agree on the need for unique passwords for UPI payments.
- Cautious with Third-Party Services: 40.5% strongly agree on being cautious about third-party services.
- General Security Agreement: 71.1% generally agree with security statements.
- Repeated Password Importance: Again, 52.1% emphasize unique passwords for UPI.
- Neutral on General Practices: 53.7% are neutral on general security practices.
- Support for Security Measures: 83.5% agree or strongly agree on the importance of security measures.
- Security Statement Agreement: 56.1% agree or strongly agree with security statements.
- Repeated General Practices: 77.6% reaffirm the importance of general security practices.
- Adopting Security Measures: 79.3% agree or strongly agree on adopting security measures.
- Perceived Security Threats: 47.1% agree or strongly agree on security threats, with 39.7% neutral.
- Password Security Support : 66.9% agree or strongly agree on the importance of unique passwords.
- Overall Security Awareness: 51.2% agree or strongly agree with statements about security awareness, showing widespread recognition of security practices.

6.CONCLUSION

The survey shows that a majority of respondents are young adults, primarily aged 18-24, and are well-educated, with a significant number holding Bachelor's, Master's, or Doctoral degrees. The gender distribution reveals a higher representation of males compared to females.Regarding digital payment behavior, a significant 72.7% of respondents use UPI daily, indicating a high level of engagement with digital payments. However, this is countered by the finding that 77.7% have encountered fraudulent activities, such as scams and unauthorized transactions, highlighting substantial security challenges in digital payment systems. Respondents exhibit a strong awareness of security risks, with many expressing concerns about revealing sensitive information and being cautious about third-party services. There is widespread agreement on the importance of security measures, such as using unique passwords for UPI payments and adopting general security practices.Despite taking proactive security measures, satisfaction with the bank's response to reported fraudulent activities is split, with only 54.5% reporting satisfaction. This suggests opportunities for financial institutions to improve their handling of fraud-related issues and their communication with affected customers. In summary, the survey underscores the necessity for enhanced security measures and improved customer satisfaction in addressing fraudulent activities in digital payments. It also emphasizes the ongoing need for education and awareness initiatives to empower users to protect themselves against digital fraud effectively. As digital payment technologies advance, addressing these security challenges will be critical for fostering trust and ensuring widespread

7.RECOMMENDATIONS

To enhance the security of Unified Payments Interface (UPI) transactions, several strategies can be implemented. Advanced fraud detection algorithms should be developed to more effectively identify and prevent scams and unauthorized transactions. Launching user education campaigns, particularly targeting young adults, can raise awareness about digital payment security and fraud prevention. Gender-inclusive initiatives can encourage more female users to engage with digital payment systems by addressing their specific concerns and barriers.Collaborating with universities to provide tailored security training for students can strengthen digital payment security knowledge. Simplifying fraud reporting mechanisms and training bank staff to respond empathetically and effectively to fraud reports can improve user experience and satisfaction. Implementing tools for daily transaction monitoring, comprehensive security features, and regular security updates will help users stay vigilant against suspicious activities.Encouraging the use of unique, strong passwords and promoting multi-factor authentication (MFA) add critical layers of security. Educating users about secure payment links, providing real-time fraud alerts, and designing user-friendly security features enhance overall compliance and safety. Regularly collecting user feedback and offering security awareness training keeps users informed about current threats.Partnerships with cybersecurity experts, transparent security policies, and enhanced customer support services further bolster security measures. Customized security recommendations and promoting secure authentication methods, such as biometric authentication, address individual user needs. Conducting regular security audits and having clear data breach response plans ensure preparedness against vulnerabilities and breaches. Public awareness campaigns and ensuring secure transaction environments with end-to-end encryption highlight the importance of digital payment security and user protection.

8.References:

Research papers :

1. Abhishek (2022): Research explores UPI's rise and significance in India, highlighting its dominance and international reach, while noting transaction failures and cybersecurity threats as challenges.
2. Chawla and Joshi (2022): The authors review factors affecting cashless transaction adoption, proposing a unified perspective considering individual, social, and technological influences.
3. Chu et al. (2020): The study identifies convenience, security, and perceived usefulness as main drivers of NFC payment adoption, noting issues with NFC terminal availability and awareness.
4. Fredy (2022): Emphasizing the transformative potential of digital financial inclusion in India, the study analyzes how digital technology can enhance monetary accessibility and economic empowerment.
5. Gaikwad (2020): The paper discusses the potential of Blockchain and DLT to improve cross-border payments, proposing UPI as a cross-border platform with a central bank or financial institution intermediary.
6. Gholami et al. (2023): This study investigates factors affecting cashless payment adoption in Lagos, Nigeria, through a survey of 500 respondents, identifying perceived benefits, effort expectancy, social influence, trust, awareness, and demographics as key influences.
7. Goparaju (2022): The author reviews the Indian digital payments market, assessing its significance, growth, and evolution as a sunrise industry.
8. Gupta and Asha (2023): Research focuses on the transformative impact of digitalization on India's financial landscape, examining electronic payments and their economic effects.
9. Gupta and Singh (2023): This research examines AI's role in enhancing UPI transactions, focusing on improvements in speed, security, and convenience, while identifying challenges and opportunities.
10. Jain (2022): This study explores the viability and potential growth of electronic payment systems in India, identifying associated challenges and opportunities.

Websites : Google Scholar, Research Gate, SSRN