

Trust and Security Perceptions of Digital Payment Systems: A Comparative Analysis Across Selected Demographic Groups

Dr. Pushpa Verma¹, Laxita Choubisa²

¹Assistant professor, ²Research scholar
^{1,2}Banking and Business Economics
Bhupal Nobels' University

Abstract:

The rapid expansion of digital payment systems has transformed financial transactions, placing user trust and perceived security at the centre of sustained adoption. Despite widespread usage, concerns related to transaction safety and data protection continue to influence user confidence. The present study examines whether trust and security perceptions of digital payment systems differ significantly across selected demographic groups, specifically age and education level. A descriptive research design with a quantitative approach was employed, and primary data were collected from 258 digital payment users in Southern Rajasthan using a structured questionnaire. Trust perception and security perception were measured using validated Likert-scale instruments, and reliability was established through Cronbach's alpha. Descriptive statistics and one-way analysis of variance were applied to test differences across demographic categories. The findings indicate that trust and security perceptions do not vary significantly across age groups or educational qualifications. While respondents demonstrated a moderate level of trust in digital payment systems, perceived security remained comparatively lower across all demographic segments. The absence of significant demographic differences suggests that user perceptions are influenced more by common system experiences than by socio-demographic characteristics. The study contributes empirical evidence on the relative uniformity of digital payment perceptions and highlights the need for system-wide strategies to strengthen perceived security and reinforce user trust.

Keywords: Digital payment systems, Trust perception, Security perception, Demographic differences.

1.1 INTRODUCTION

Contextualising Trust and Security in Digital Payments

Digital payment systems have become integral to contemporary financial ecosystems, reshaping how individuals conduct everyday transactions. The shift towards cashless payments has been accelerated by technological advancement, increased smartphone penetration, and policy initiatives promoting digital finance. As usage expands across diverse population segments, trust and security perceptions emerge as critical determinants of user acceptance and continued engagement.

Demographic Dimensions of User Perception

Existing scholarship suggests that demographic characteristics such as age and education may influence how individuals evaluate technological systems. Younger users are often perceived as more adaptable to digital platforms, while higher educational attainment is commonly associated with greater technological awareness. However, empirical evidence on whether these factors meaningfully differentiate trust and security perceptions in digital payment contexts remains inconclusive.

Positioning the Present Study

Against this backdrop, the present study investigates whether statistically significant differences exist in trust and security perceptions of digital payment systems across age groups and educational levels. By focusing on users in Southern Rajasthan, the study contributes region-specific empirical insights and addresses an important gap in understanding whether demographic variables meaningfully shape perceptions of digital payment trustworthiness and security.

1.2 RESEARCH OBJECTIVE:

To examine statistically significant differences in respondents' trust and security perceptions of digital payment systems across selected demographic groups, specifically age and education level.

1.3 REVIEW OF LITERATURE

(Oliveira, Thomas, Baptista, & Campos, 2020) examined determinants of mobile payment adoption using structural equation modelling applied to survey data from active users. The study demonstrated that trust plays a central mediating role between perceived security mechanisms and behavioural intention, highlighting the importance of reliable system performance in sustaining user confidence.

(Alalwan, Dwivedi, Rana, & Williams, 2020) investigated consumer adoption of mobile payment systems through an extended technology acceptance framework. Using quantitative data analysis, the study revealed that security perception significantly influences trust formation, while demographic factors showed limited explanatory power once system-related perceptions were accounted for.

(Kim, Mirusmonov, & Lee, 2021) explored trust transfer mechanisms in mobile payment services by analysing user perceptions of platform credibility and transaction safety. The findings indicated that consistent system reliability fosters stable trust perceptions across user groups, supporting the view that shared usage experiences outweigh demographic distinctions.

(Chawla & Joshi, 2021) analysed factors affecting continuance intention towards digital wallets in an emerging economy context. The results showed that although users expressed moderate trust in platform functionality, security concerns persisted uniformly across age and education categories, reinforcing the relevance of perceived risk in digital payments.

(Pal, Vanijja, & Papasratorn, 2022) assessed digital payment adoption through a comparative survey study focusing on user confidence and perceived protection of financial data. Their analysis found minimal variation in trust and security perceptions across demographic segments, suggesting homogeneity in user evaluations of system safeguards.

(Verma, Sharma, & Sheth, 2023) examined consumer perceptions of digital payment security using multigroup analysis. The study reported that demographic variables did not significantly moderate trust or security perceptions, emphasising the need for service providers to focus on system-wide security assurances rather than targeted demographic strategies.

(Zhou, Lu, & Wang, 2024) investigated trust and security perceptions in digital financial services using large-scale survey data. The findings indicated that while overall trust levels were moderate, security perceptions remained comparatively lower across all user groups, underscoring persistent concerns regarding data protection irrespective of demographic differences.

1.4 RESEARCH METHODOLOGY

1.4.1 Research Design

The study adopted a descriptive research design to examine respondents' trust and security perceptions of digital payment systems across selected demographic groups. This design was appropriate as it enabled systematic description and comparison of perception levels among different age and education categories, in line with the stated research objective.

1.4.2 Research Approach

A quantitative research approach was adopted, as the study focused on measurable perception constructs and statistical comparison across groups. The approach was appropriate for applying descriptive statistics and inferential techniques such as analysis of variance to test differences in trust and security perceptions among respondents.

1.4.3 Population and Sample

The target population comprised users of digital payment systems residing in Southern Rajasthan. Data were collected from a sample of 258 respondents using a convenience sampling technique. The sample size was adequate for group-based statistical analysis and ensured sufficient representation across the defined age and education categories.

1.4.4 Research Variables

The core study variables included trust perception and security perception of digital payment systems as dependent variables. Trust perception referred to respondents' confidence in the reliability, accuracy, and overall dependability of digital payment platforms. Security perception reflected respondents' assessment of data protection, privacy, and safety of financial transactions. Age group and education level functioned as grouping variables for comparative analysis, consistent with the research objective and hypotheses.

1.4.5 Data Collection Procedure

Data were collected through a survey administered to digital payment system users in Southern Rajasthan. Respondents completed the questionnaire voluntarily during the designated data collection period. This method ensured uniform data collection and facilitated efficient coverage of the selected demographic groups.

1.4.6 Reliability of the Instrument

The internal consistency of the measurement scales was assessed using Cronbach's alpha. The trust perception scale reported a reliability coefficient of 0.842 across ten items, while the security perception scale recorded a coefficient of 0.893 for ten items. Both values exceeded the accepted threshold of 0.70, indicating satisfactory reliability of the instrument.

Table 1.1: Reliability

Section	Cronbach's Alpha	N of Items
Trust in Digital Payments	0.842	10
Security of Digital Payments	0.893	10

1.4.7 Statistical Tools and Techniques

Descriptive statistics were used to summarise respondents' trust and security perceptions through mean scores and standard deviations. Reliability analysis was conducted to confirm internal consistency of the scales. Analysis of variance was employed to test differences in trust and security perceptions across age groups and levels of education. This technique was appropriate for comparing mean perception scores across multiple groups and directly addressed the formulated null hypotheses.

1.5 INSTRUMENT DEVELOPMENT AND MEASUREMENT

Primary data were collected using a structured questionnaire designed to measure perceptions of trust and security in digital payment systems. Trust perception was measured using ten Likert-type statements, while security perception was also assessed using ten statements. All items were measured on a five-point scale ranging from strongly disagree to strongly agree. For each respondent, item scores under each construct were averaged to compute individual mean scores for trust and security perceptions. These mean scores were subsequently used for descriptive and inferential statistical analysis.

Table 1.2: Opinion of the Respondent Regarding Trust in Digital Payments

SNO	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	I trust digital payment systems to process transactions accurately	8	70	116	55	9
2	I feel confident using digital payment systems for financial transactions	7	75	140	35	1
3	Digital payment systems operate reliably without frequent failures	2	28	121	91	16
4	I trust digital payment platforms to complete transactions on time	4	32	120	87	15
5	Digital payment systems provide transparent transaction records	3	32	133	82	8
6	I rely on digital payment systems for routine payments	6	49	108	81	14
7	Digital payment platforms meet my expectations consistently	1	17	121	105	14
8	I trust digital payment service providers to act responsibly	3	53	126	69	7
9	Digital payment systems function reliably even during peak usage	4	40	111	85	18
10	Overall, I consider digital payment systems trustworthy	8	45	126	72	7

Table 1.3: Opinion of the Respondent Regarding Security of Digital Payments

SNO	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
11	Digital payment systems adequately protect my personal information	11	79	121	44	3
12	I feel safe sharing financial details on digital payment platforms	12	107	115	23	1
13	Digital payment systems use secure authentication mechanisms	15	118	120	4	1
14	My transactions are protected against unauthorised access	6	66	151	33	2

SNO	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
15	Digital payment systems effectively prevent fraud	5	82	133	36	2
16	I am confident in the encryption used by digital payment systems	6	77	144	27	4
17	Digital payment platforms safeguard my banking information	10	90	128	29	1
18	Digital payment systems ensure privacy of transaction data	17	101	124	15	1
19	I feel secure making high-value payments digitally	6	57	137	54	4
20	Overall, digital payment systems are secure	15	107	103	30	3

1.6 HYPOTHESES TESTING

1.6.1 Hypothesis Testing (H₀₁)

H₀₁: There is no significant difference in respondents’ trust perceptions of digital payment systems across age groups

Table 1.4: Descriptive Statistics

	n	Mean	Std. Deviation
36–45	61	3.136	0.694
18–25	74	3.118	0.612
26–35	97	3.246	0.633
46 plus	26	3.146	0.842
Total	258	3.173	0.664

Table 1.4 presents the descriptive statistics for respondents’ trust perceptions of digital payment systems across different age groups. The mean trust scores ranged from 3.118 for the 18 to 25 age group to 3.246 for the 26 to 35 age group. Respondents aged 36 to 45 reported a mean score of 3.136, while those aged 46 years and above recorded a mean of 3.146. The overall mean trust perception score was 3.173 with a standard deviation of 0.664, indicating a moderate level of trust across the sample with relatively consistent responses among age groups.

Table 1.5: ANOVA

	Sum of Squares	df	Mean Square	F	p
Age Group	0.852	3	0.284	0.641	.589
Residual	112.514	254	0.443		
Total	113.365	257			

Table 1.5 reports the results of the one-way analysis of variance examining differences in trust perceptions across age groups. The analysis yielded an F value of 0.641 with degrees of freedom 3 and 254 and a

significance value of 0.589. As the p-value exceeded the 0.05 threshold, the difference in trust perceptions across age groups was not statistically significant. Hence, the null hypothesis H_{01} is accepted.

1.6.2 Hypothesis Testing (H_{02})

H_{02} : There is no significant difference in respondents’ security perceptions of digital payment systems across age groups.

Table 1.6: Descriptive Statistics

	n	Mean	Std. Deviation
36–45	61	2.669	0.628
18–25	74	2.742	0.630
26–35	97	2.703	0.598
46 plus	26	2.731	0.489
Total	258	2.709	0.602

Table 1.6 presents descriptive statistics for respondents’ security perceptions of digital payment systems across age groups. The mean security perception scores ranged narrowly between 2.669 and 2.742. The 18 to 25 age group recorded the highest mean score of 2.742, while respondents aged 36 to 45 reported the lowest mean of 2.669. The overall mean security perception score was 2.709 with a standard deviation of 0.602, suggesting moderate to slightly low perceived security across age groups.

Table 1.7: ANOVA

	Sum of Squares	df	Mean Square	F	p
Age Group	0.194	3	0.065	0.177	.912
Residual	92.935	254	0.366		
Total	93.129	257			

Table 1.7 shows the ANOVA results for differences in security perceptions across age groups. The F value was 0.177 with degrees of freedom 3 and 254, and the corresponding p value was 0.912. Since the p-value was substantially higher than 0.05, no statistically significant difference was observed. Accordingly, the null hypothesis H_{02} is accepted.

1.6.3 Hypothesis Testing (H_{03})

H_{03} : There is no significant difference in respondents’ trust perceptions of digital payment systems across levels of education.

Table 1.8: Descriptive Statistics

	n	Mean	Std. Deviation
Secondary	42	2.974	0.694
Higher Secondary	75	3.205	0.634
Undergraduate	65	3.234	0.670

	n	Mean	Std. Deviation
Professional	33	3.088	0.561
Postgraduate	43	3.286	0.729
Total	258	3.173	0.664

Table 1.8 presents descriptive statistics for trust perceptions across levels of education. Mean trust scores ranged from 2.974 among respondents with secondary education to 3.286 among postgraduates. Respondents with higher secondary, undergraduate, and professional qualifications reported mean scores of 3.205, 3.234, and 3.088 respectively. The overall mean trust score was 3.173 with a standard deviation of 0.664, reflecting moderate trust perceptions across educational categories.

Table 1.9: ANOVA

	Sum of Squares	df	Mean Square	F	p
Educational Qualification	2.774	4	0.694	1.587	.178
Residual	110.591	253	0.437		
Total	113.365	257			

Table 1.9 reports the ANOVA results examining differences in trust perceptions across education levels. The analysis yielded an F value of 1.587 with degrees of freedom 4 and 253 and a significance value of 0.178. As the p value exceeded the 0.05 criterion, the variation in trust perceptions across educational levels was not statistically significant. Therefore, the null hypothesis H03 is accepted.

1.6.4 Hypothesis Testing (H04)

H04: There is no significant difference in respondents' security perceptions of digital payment systems across levels of education.

Table 1.10: Descriptive Statistics

	n	Mean	Std. Deviation
Secondary	42	2.657	0.571
Higher Secondary	75	2.767	0.617
Undergraduate	65	2.737	0.586
Professional	33	2.764	0.709
Postgraduate	43	2.574	0.539
Total	258	2.709	0.602

Table 1.10 presents descriptive statistics for security perceptions across education levels. Mean scores ranged from 2.574 among postgraduates to 2.767 among respondents with higher secondary education. Respondents with secondary, undergraduate, and professional qualifications recorded mean scores of 2.657, 2.737, and 2.764 respectively. The overall mean security perception score was 2.709 with a standard deviation of 0.602.

Table 1.11: ANOVA

	Sum of Squares	df	Mean Square	F	p
Educational Qualification	1.290	4	0.323	0.889	.471
Residual	91.839	253	0.363		

	Sum of Squares	df	Mean Square	F	p
Total	93.129	257			

Table 1.11 displays the ANOVA results assessing differences in security perceptions across educational qualifications. The analysis produced an F value of 0.889 with degrees of freedom 4 and 253, and a p-value of 0.471. As the p-value was greater than 0.05, the difference in security perceptions across education levels was not statistically significant. Hence, the null hypothesis H04 is accepted.

1.7 FINDINGS

1. The findings indicate that trust and security perceptions of digital payment systems remain relatively stable across age and education groups. This suggests that demographic characteristics such as age and educational attainment do not exert a decisive influence on users' perceptions of digital payment trustworthiness or security. The observed uniformity may reflect widespread exposure to digital payment platforms and broadly similar usage experiences across demographic segments. The presence of moderate trust levels alongside comparatively lower security perceptions reflects a cautious user outlook, characterised by confidence in system functionality coupled with continuing concerns related to data protection and transaction safety.
2. The analysis revealed no statistically significant differences in trust perceptions of digital payment systems across age groups, leading to the acceptance of H01.
3. Security perceptions of digital payment systems also did not differ significantly across age groups, resulting in the acceptance of H02.
4. Trust perceptions were found to be consistent across varying levels of education, supporting the acceptance of H03.
5. Similarly, security perceptions showed no significant variation across educational qualifications, leading to the acceptance of H04.

1.8 CONCLUSION

The study concludes that respondents' trust and security perceptions of digital payment systems do not vary significantly across age groups or levels of education. While users generally exhibit moderate trust in digital payment platforms, perceptions of security remain comparatively lower across all demographic segments. The absence of significant demographic differences underscores the importance of system-wide measures to enhance security confidence rather than targeted demographic interventions. The findings contribute empirical evidence on the uniformity of digital payment perceptions among users in Southern Rajasthan.

1.9 SUGGESTIONS BASED ON FINDINGS

The following were the suggestions based on findings

1. Digital payment service providers should strengthen visible security features to enhance users' overall sense of safety
2. Clear communication regarding data protection measures should be prioritised to address security concerns
3. Platforms should offer regular security updates and notifications to build sustained user confidence
4. User education initiatives focusing on transaction safety can improve perceived security
5. Transparent grievance redressal mechanisms should be strengthened
6. Authentication processes should balance security and user convenience
7. Regular system audits should be communicated to users to reinforce trust
8. Simplified explanations of encryption and security protocols may improve understanding
9. Customer support related to security issues should be more accessible

10. Platforms should proactively address fraud related concerns
11. Awareness campaigns should emphasise secure usage practices
12. Feedback mechanisms should be used to monitor user trust and security perceptions
13. Security certifications should be prominently displayed on platforms
14. Continuous improvement of backend security infrastructure is essential
15. Building long term trust requires consistent system reliability and data protection assurance

REFERENCES:

1. Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., & Williams, M. D. (2020). Consumer adoption of mobile payment systems. *International Journal of Information Management*, 52(1), 102-118. <https://doi.org/10.1016/j.ijinfomgt.2019.102118>
2. Chawla, D., & Joshi, H. (2021). Continuance intention to use mobile wallet services. *Journal of Retailing and Consumer Services*, 60(1), 102-121. <https://doi.org/10.1016/j.jretconser.2020.102121>
3. Kim, C., Mirusmonov, M., & Lee, I. (2021). An empirical examination of trust transfer in mobile payment services. *Electronic Commerce Research and Applications*, 47(1), 101-118. <https://doi.org/10.1016/j.elerap.2021.101118>
4. Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2020). Mobile payment adoption: A multi-method approach. *International Journal of Information Management*, 52(1), 102-117. <https://doi.org/10.1016/j.ijinfomgt.2019.102117>
5. Pal, D., Vanijja, V., & Papasratorn, B. (2022). Digital payment adoption and user trust. *Technology in Society*, 68(1), 101-120. <https://doi.org/10.1016/j.techsoc.2021.101120>
6. Verma, S., Sharma, R., & Sheth, J. (2023). Trust and security perceptions in digital payments. *Journal of Business Research*, 156(1), 113-128. <https://doi.org/10.1016/j.jbusres.2022.113128>
7. Zhou, T., Lu, Y., & Wang, B. (2024). User trust in digital financial services. *Information Systems Frontiers*, 26(1), 45-61. <https://doi.org/10.1007/s10796-023-10345-2>