

Cybersecurity Awareness and Privacy Protection Perceptions in UPI Payments: An Empirical Study of user Trust in Bangalore

Amrita Potdar¹, Dr. Sumera Aluru²

Abstract-- The Unified Payments Interface (UPI) has been rapidly growing in India and has transformed the digital financial transactions landscape, processing more than 700 million transactions a day (NPCI, 2024). Although UPI has greatly facilitated financial inclusion and cashless transactions, its tremendous growth has also resulted in an increased risk in cybersecurity and privacy. This paper examines how cybersecurity awareness and perceived privacy protection affect user trust in UPI payments, particularly among 330 users in Bangalore, India. A descriptive and analytical research design was adopted, based on which primary data were gathered with the help of a structured questionnaire with 5-point Likert scale questions. The statistical methods such as Pearson correlation, multiple regression, and Structural Equation Modeling (SEM) were used to conduct the analysis. The measurement scales were found to be reliable with Cronbach alpha values more than 0.83 of all constructs. Findings show that user trust is significantly positively predicted by both cybersecurity awareness ($= 0.469, p < 0.001$) and perceived privacy protection ($= 0.451, p < 0.001$), and these two variables jointly explain 44.2% of its variability ($R^2 = 0.442$). These results are further supported by SEM, where the path coefficients are 0.529 and 0.550 respectively. The paper finds that promoting cybersecurity awareness and reinforcing the sense of security in users regarding the safety of their data are key measures to instill trust in UPI ecosystems.

Keywords-- UPI payments, cybersecurity awareness, perceived privacy protection, user trust, digital payments, Structural Equation Modeling, fintech security

I. INTRODUCTION

The high growth of digital technology has been a major change in the financial industry and electronic payment systems have been extensively adopted. In India, one of the most popular and effective real-time payment platforms is the Unified Payments Interface (UPI), which was launched by the National Payments Corporation of India (NPCI) in 2016. UPI allows users to send money immediately between bank accounts via mobile applications with ease, speed, and convenience. Its ease of use, low transaction cost and interoperability has made it have a huge following among individuals, businesses and government programs.

Nevertheless, the growing use of UPI payments has posed serious issues in the aspects of cybersecurity and data privacy, as well.

With the increase in the number of digital transactions, hackers are taking advantage of the vulnerabilities in systems by engaging in phishing, social engineering, malware, SIM swap fraud, and unauthorized transactions. Such threats do not only lead to financial losses but also a lack of confidence of users in digital payment systems.

Along with security risks, privacy protection perceptions have emerged as a very serious issue in UPI transactions. The system manages confidential personal and financial data like bank details, phone numbers, and the history of transactions. The perception of the users regarding their data being processed safely, being inaccessible to others, and being processed in a clear and transparent manner directly affects the attitude of the users towards trusting it and using UPI further. Although the Reserve Bank of India (RBI) regulates and fintech companies provide technological protection against cyber fraud and privacy violations, cases of cyber fraud and privacy breaches are on the increase.

The study will thus fill this empirical gap by investigating how much cybersecurity awareness and perceived privacy protection affect user trust in UPI payments by using 330 users in Bangalore.

II. NEED OF THE STUDY

The blistering development of UPI has brought a wave of transformation to digital payments in India as transactions have become quicker, simpler, and more convenient. At the moment, UPI manages more than 70 crore (700+ million) transactions daily, which indicates its gigantic penetration in the country (NPCI, 2024). UPI supports over 80 percent of the digital payments in India and is one of the biggest real-time payment systems in the world. Such high transaction volume can result in huge financial and data risks even after a small vulnerability.

The growing number of phishing, fraud, unauthorized transactions, and data abuse are alarming the issue of user security and privacy. Safe digital practices are unfamiliar to many users and thus they are more susceptible to cyber threats. This vulnerability is further compounded by the discrepancy between formal security recommendations and the real user practices.



Thus, the research is critical to investigate cybersecurity awareness, how users perceive privacy protection, and how both of these can influence user trust, thus contributing to increasing the confidence level, enhancing security, and providing the safe development of UPI-based digital payments.

III. REVIEW OF LITERATURE

Hossain (2019) made a comparison between risk and trust in the adoption of mobile payment in terms of EFA, CFA, and SEM, and established that perceived risk has a negative influence and trust has a positive influence of user satisfaction. Wadkar et al. (2025) compared obstacles to UPI fraud and cybersecurity and concluded that the frequency of frauds grows due to the lack of awareness of users. Sharma et al. (2024) highlighted that demographics affect the level of cybersecurity awareness, and that the lack of awareness results in the increased exposure to risks. Similarly, Khandal (2022) also found out that the level of adoption of UPI is high, whereas the degree of safe usage awareness is low, which influences the security practice. Aljaradat and Shukla (2025) revealed that trust, usability, and perceived usefulness are the driving forces of UPI acceptance, and that cybersecurity is a critical factor in influencing the perception of users. Bhatt (2025) also observed that one of the leading causes of privacy and human rights concerns is cyber threats, which should be more regulated. According to Mungara et al. (2025), users are likely to fall into scams because of the absence of appropriate security guidelines. According to Acharya (2017), privacy risks are a result of a weak data protection law, and better legal frameworks should be implemented. Thakkar et al. (2025) came to the conclusion that convenience is more important to users than security; security details also impact trust and behavior. Edburg et al. (2024) demonstrated that the perception of security has a direct impact on UPI usage and that more vigilance is needed with the increasing number of cases of fraud. Altogether, the past studies have explored the trust, risk, and privacy individually, yet there is a lack of empirical research that explores both cybersecurity awareness and perceived privacy protection as predictors of user trust in the context of Indian UPI, which is the focus of the present research.

IV. RESEARCH GAP

Despite a number of studies having been conducted on the topic of digital payment systems, most studies are on general mobile or online payments as opposed to UPI. The few studies that have been conducted on cybersecurity awareness and online perceived privacy protection regarding the UPI context do not conduct a simultaneous study of both.

Also, most of the studies focus on technical elements of security, but do not take into account the aspects that are user centric like the awareness, perception and trust.

Regarding the Indian context, particularly in big cities such as Bangalore, there exists a gap in the literature that explores the combined effect of cybersecurity awareness and perception of privacy protection on user trust and user behavior. The lack of Structural Equation Modeling in the previous India-based UPI research also restricts the extent of causal interpretation. Therefore, this paper attempts to bridge these shortcomings with a user-friendly, comprehensive analysis.

V. RESEARCH DESIGN

5.1 Problem Statement.

The fast expansion of UPI payments has brought about ease in online transactions, but at the same time, it has contributed to the emerging cybersecurity threats and privacy concerns. A high number of daily transactions have led to a greater number of phishing, fraud and misuse of data, which has undermined user confidence. The level of security that is currently in place tends to be inadequate in the user level because of the absence of awareness and knowledge on safe practices. This research focuses on the role of and perceived privacy protection on user confidence in UPI payments and how to enhance security confidence in digital payment systems.

5.2 Objectives of the Study

- To determine the key cybersecurity concerns of UPI payments.
- To survey the perceived privacy protection of the users in UPI transactions.
- To determine the degree of cybersecurity awareness amongst UPI users.
- To test how awareness of cybersecurity and perceived privacy protection affect user trust in UPI payments.

5.3 Hypotheses

H0: There is no significant difference in the user trust in UPI payments between the groups with cybersecurity awareness and privacy protection.

H0: There is a strong association between cybersecurity awareness and privacy protection and user trust in UPI payments.

5.4 Research Methodology

This study adopts a Descriptive and Analytical research design.

It is descriptive because it is concerned with the level of cybersecurity awareness and perceived protection of privacy among the UPI users. It is analytical in the sense that it investigates the connection between cybersecurity awareness, perceived protection of privacy and user trust of UPI payments.

5.5 Sources of Data

Primary Data: Direct data were gathered using a structured questionnaire, involving 330 UPI users in Bangalore to obtain first-hand data on the experiences of the users, their awareness, and their perception of cybersecurity and privacy when using UPI payments.

Secondary Data: The secondary data were obtained using research journals, RBI reports, NPCI publications, government websites, and scholarly articles, which offer theoretical background and information on cybersecurity concerns, trends in fraud, and privacy of digital payments.

5.6 Sampling Plan

Sampling Unit: UPI users in Bangalore (individuals).

Sample Size: 330 respondents.

Sampling Method: Convenience Sampling was employed, and the respondents were chosen according to the availability and readiness to take part.

5.7 Data collection tools.

A structured questionnaire with 5-point Likert scale items (1 = Strongly Disagree to 5 = Strongly Agree) was used to gather data based on the perceptions of cybersecurity awareness, perceived protection of privacy and user confidence in UPI payments.

5.8 Plan of Analysis

The information gathered was systematically arranged, categorized and tabulated.

The level of awareness and perception was evaluated by the use of descriptive statistics, such as percentage analysis and mean score analysis. Internal consistency and reliability were validated by Cronbachs Alpha. Pearson correlation was used to test bivariate correlations between user trust, perceived privacy protection and cybersecurity awareness. Multiple regression was used to establish the predictive power of the two independent variables on user trust. The hypothesized relationships between the latent constructs were tested using Structural Equation Modeling (SEM) and the whole research model was validated. All the calculations were done in MS Excel, JMP software and python.

5.9 Conceptual Framework and Variable Definitions.

The conceptual model assumes that the independent variables (Cybersecurity Awareness and Perceived Privacy Protection) intersect to influence User Trust in UPI payments (the dependent variable).

Cybersecurity awareness can be described as the amount of knowledge users have about safe UPI, including keeping their PIN confidential, detecting fraud, and unfamiliar links.

Perceived privacy protection is the perception that users have about the level of security provided by UPI systems in managing their personal and financial information such as a belief that the information is not accessible to unauthorized parties, is used correctly and is handled effectively.

User trust is the level of confidence that users have in the security and reliability of UPI payment systems, higher trust will motivate users to continue using the system.

VI. ANALYSIS AND FINDINGS

6.1 Reliability Analysis

Internal consistency and reliability were measured by Cronbachs alpha. The values of all constructs are above the suggested level of 0.70, which proves good to very good reliability.

Table 1: Reliability Test Results (Cronbach's Alpha)

Variable	Cronbach's Alpha	Interpretation
Cybersecurity Awareness	0.833	Good
User Trust	0.873	Good
Perceived Privacy Protection	0.831	Good

6.2 Descriptive Analysis

Age Distribution

Table 2: Age Group Distribution

Age Group	Frequency (n)	Percentage (%)
Below 20	45	13.6
21–30	111	33.7
31–40	49	14.8
41–50	77	23.3
Above 50	48	14.5
Total	330	100.0

Most of the respondents (33.7) are in the age bracket of 21-30 years, which means that young adults constitute the highest proportion of the sample and the UPI usage is higher among the younger population.

Gender Distribution

Table 3: Gender Distribution

Gender	Frequency (n)	Percentage (%)
Male	153	46.4
Female	177	53.6
Total	330	100.0

The sample size is 53.6 percent females and 46.4 percent males, which represents a rather equal gender distribution.

Education Level

Table 4: Education Level

Education Level	Frequency (n)	Percentage (%)
High School	44	13.3
Undergraduate	69	20.9
Postgraduate	130	39.4
Others	87	26.4
Total	330	100.0

Another important fact is that a large percentage of the respondents (39.4) are postgraduates and this implies a well-educated group, which could also contribute to increased adoption and awareness of UPI.

Occupation

Table 5: Occupation

Occupation	Frequency (n)	Percentage (%)
Student	51	15.5
Employee	142	43.0
Self-employed	88	26.7
Retired	49	14.8
Total	330	100.0

The majority of respondents (43.0%), self-employed people (26.7%), which implies that working professionals are the most frequent users of UPI.

UPI Applications Used by Respondents (Multiple Response — % of 330 respondents)

Table 6: UPI Applications Used (Multiple Response — percentages sum to >100% as respondents may use multiple apps)

UPI Application	Frequency (n)	% of Respondents
Google Pay	159	48.2
PhonePe	252	76.4
BHIM	96	29.1
Paytm	49	14.8

The most popular application is PhonePe (76.4% and Google Pay (48.2%). A large number of respondents have various UPI applications, which indicates flexible usage.

UPI Usage Frequency

Table 7: UPI Usage Frequency

Usage Frequency	Frequency (n)	Percentage (%)
Daily	158	47.9
Weekly	133	40.3
Monthly	39	11.8
Total	330	100.0

The high adoption and frequent use of UPI are confirmed by the fact that almost half of the respondents (47.9%) use it on a daily basis and 40.3% use it weekly.

To examine the levels of cybersecurity awareness, perceived privacy protection, and user trust, descriptive statistics were calculated. The mean scores of all three constructs on a 5-point scale are very near to 3.00, which implies a moderate level in all dimensions.

Table 8: Descriptive Statistics of Key Variables

Variable	Mean	Std. Deviation	Minimum	Maximum	Interpretation
Cybersecurity Awareness	2.95	0.49	1.6	4.4	Moderate
User Trust	3.06	0.58	1.4	4.6	Moderate
Perceived Privacy Protection	3.00	0.52	1.6	4.6	Moderate

The results indicate that, users demonstrate equal attitudes to cybersecurity, privacy protection and trust in UPI platforms. The mentioned moderate level of awareness is an indication of a vast potential of specific educational interventions.

6.3 Correlation Analysis

Bivariate correlation between the three important constructs was done using Pearson correlation analysis. Statistically significant moderate positive correlations are found between all variables.

Table 9: Pearson Correlation Matrix

Variable	Cybersecurity Awareness	User Trust	Perceived Privacy Protection
Cybersecurity Awareness	1.000	0.556	0.406
User Trust	0.556	1.000	0.558
Perceived Privacy Protection	0.406	0.558	1.000

There is a moderate positive relationship between user trust and cybersecurity awareness ($r = 0.556$) which shows that users possessing a higher level of cybersecurity awareness are more likely to demonstrate higher levels of trust in UPI. In the same manner, the perceived protection of privacy exhibits a similarly positive correlation with user trust ($r = 0.558$) with a logical consistency since users who think that their data is being treated securely inherently trust the platform more.

There was also a moderate relationship between perceived privacy protection and cybersecurity awareness ($r = 0.406$).

6.4 Multiple Regression Analysis

The effect of cybersecurity awareness and perceived privacy protection on user trust was measured using multiple regression analysis. The general regression equation was found to be statistically significant ($p < 0.001$).

Table 10: Multiple Regression Analysis Results

Variable	Coefficient (β)	Std. Error	t-value	p-value	Result
Constant	0.323	0.172	1.881	0.061	Not Significant
Cybersecurity Awareness	0.469	0.054	8.740	<0.001	Significant
Perceived Privacy Protection	0.451	0.051	8.806	<0.001	Significant

$R^2 = 0.442$ | *F-statistic significant at $p < 0.001$*

The awareness of cybersecurity became a very strong positive predictor of user trust ($\beta = 0.469$, $p = 0.001$). User trust is also positively and significantly predicted by perceived privacy protection ($\beta = 0.451$, $p < 0.001$). The value of R^2 equals 0.442 that means the model explains the variation of user trust about 44.2 percent of the overall variance- a moderate to high explanatory power which is

also agreeable in the study of behavior. According to these conclusions, H_0 is rejected and H_a is accepted.

6.5 Structural Equation Modeling (SEM) Analysis.

SEM was used to test structural paths simultaneously and to test the measurement model.

Table 11: SEM Structural Path Coefficients

Path	Coefficient (β)	Std. Error	z-value	p-value	Result
Cybersecurity Awareness → User Trust	0.529	0.081	6.555	<0.001	Significant
Perceived Privacy Protection → User Trust	0.550	0.084	6.513	<0.001	Significant

Note: The SEM coefficients are a bit larger than regression coefficients since SEM models the latent variable and considers measurement error, which tends to overstate the path estimates compared to OLS regression. The two techniques always validate the meaning and orientation of relationships.

Note on factor loadings (Table 12): Unstandardized factor loadings of the SEM measurement model are given below. Unstandardized loadings are not constrained by 01 and indicate the scale relationships between indicators and latent constructs, which are not standardized.

Table 12: Measurement Model Factor Loadings (Unstandardized)

Construct	Items	Unstandardized Loading	Result
Cybersecurity Awareness	A1–A5	0.97–1.07	Strong
Perceived Privacy Protection	P1–P5	1.03–1.20	Strong
User Trust	T1–T5	0.95–1.08	Strong

The regression findings are supported and reinforced by the SEM findings. Perceived protection of privacy ($\beta = 0.550$) is slightly more powerful than cybersecurity awareness ($\beta = 0.529$) and both are very significant ($p < 0.001$). Convergent validity and construct reliability are supported by strong factor loadings in all constructs.

VII. DISCUSSION

The demographic data show that most of the respondents (33.7) are aged between 21 and 30, which emphasizes that young adults are the main consumers of UPI payments. There is a relatively equal gender balance (53.6% female, 46.4% male). The number of postgraduates (39.4%), is quite big, which shows that education has a significant influence on digital payment adoption. Occupation wise, 43% are employees with 26.7% self-employed.

In terms of application usage, PhonePe (76.4%), and Google Pay (48.2) dominate the UPI ecosystem. It is also observed that users frequently use several UPI applications, which can be characterized as adaptive and flexible usage behaviour. The frequency of UPI is also quite high, with 47.9% of the respondents using it on a daily basis.

Descriptive statistics show that cybersecurity awareness (Mean = 2.95), perceived privacy protection (Mean = 3.00), and user trust (Mean = 3.06) are moderate. The reliability analysis allows asserting that there is a high level of internal consistency among all constructs (Cronbach 0.83 and higher). Correlation analysis demonstrates moderately positive correlation between the two independent variables and user trust ($r \approx 0.556$ -0.558). The multiple regression proves that 44.2% of the difference in the user trust is explained by cybersecurity awareness ($\beta = 0.469$) and perceived privacy protection ($\beta = 0.451$).

These results are also confirmed by SEM, where perceived privacy protection ($= 0.550$) demonstrates slightly higher path to user trust compared to cybersecurity awareness ($= 0.529$). The correlation between the perceived protection of privacy and trust is also logically consistent: it is only natural that a user who believes that his or her data is processed safely trusts the platform. According to these findings the null hypothesis is dismissed and the alternative hypothesis is accepted.

VIII. CONCLUSION

This paper examined how cybersecurity awareness, perceived privacy protection and user trust in UPI payments relate in Bangalore, India. The results present strong empirical data that the two variables are important positive predictors of user trust. The more informed users of the dangers of cybersecurity and those who think their information is secured are likely to trust UPI platforms more. The fact that the positive effects of perceived privacy protection on trust are theoretically consistent is natural: when users are sure that their personal and financial data are processed in a safe and open way, their trust into the platform is strengthened automatically.

The fact that the means of all constructs are moderate indicates that UPI users have not attained high security literacy or privacy confidence yet, even though UPI is widely used. Digital literacy courses, clear data control regulations, and fraud alerts in real-time can help fill this gap.

RBI and policymakers ought to enforce more stringent data protection policies, which were inspired by frameworks like GDPR. NPCI and fintech firms need to invest in convenient security measures, active fraud detection, and publicly available information on data usage. Schools and civil society groups can significantly contribute to filling the cybersecurity awareness gap, especially in first-time and low-literacy users of digital payment.

To conclude, the issue of trust in UPI depends on both the knowledge of cybersecurity of the users and their beliefs regarding the effectiveness of data protection. The training of informed, privacy-confident users is thus just as important as improving the technical base of digital payment systems.

IX. FUTURE STUDY

It can be extended to a bigger sample size and diversified by incorporating more rural regions in the study in the future to enhance the generalizability. Other aspects that could impact on UPI adoption and trust are also open to scrutiny by the researchers like technological literacy, ease of use, and government policies.

Longitudinal research can be used to comprehend the nature of cybersecurity awareness and perceived privacy protection changes overtime. A further comparison with other digital payment options and the application of qualitative methods, e.g., interviews, could help gain more information on user behavior and trust. Moreover, more sophisticated methods of Structural Equation Modeling, including multi-group analysis, can be utilized in order to investigate the demographic variations.

REFERENCES

- [1] Acquisti, A., Brandimarte, L., & Loewenstein, G. (2016). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514.
- [2] Acharya, S. (2017). Privacy risks in digital financial services: A policy perspective. *Journal of Financial Regulation*, 3(1), 45–67.
- [3] Aljaradat, M., & Shukla, V. K. (2025). Analyzing trust and cybersecurity in digital payment systems: A structural approach. *International Journal of Information Security*, 24(2), 112–128.
- [4] Bhatt, P. (2025). Cybersecurity and privacy in digital systems: Implications for human rights. *Digital Policy, Regulation and Governance*, 27(1), 23–38.
- [5] Edburg, R., et al. (2024). UPI usage and fraud mitigation: A multivariate analysis. *Journal of Digital Commerce*, 18(4), 201–219.
- [6] Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59(4), 451–474.
- [7] Hossain, M. A. (2019). Examining risk and trust factors in mobile payment adoption. *Journal of Financial Services Marketing*, 24(3), 88–102.
- [8] Khandal, V. (2022). Customer awareness of UPI and mobile banking: An empirical study. *Indian Journal of Finance*, 16(5), 33–47.
- [9] Kim, C., et al. (2019). Trust and security as drivers of continuance intention in mobile payments. *Computers in Human Behavior*, 94, 210–220.
- [10] Liébana-Cabanillas, F., et al. (2018). Trust and risk in mobile payments: A meta-analysis. *Journal of Business Research*, 91, 245–255.
- [11] Mungara, A., et al. (2025). Security and privacy concerns of UPI users: A mixed-method inquiry. *Telematics and Informatics*, 78, 101925.
- [12] National Payments Corporation of India. (2024). UPI ecosystem statistics. Retrieved from <https://www.npci.org.in>
- [13] Reserve Bank of India. (2023). Annual report on digital payments and cybersecurity. RBI Publications.
- [14] Sharma, M., et al. (2024). Cybersecurity awareness in digital India: A demographic analysis. *Journal of Cybersecurity Education, Research and Practice*, 12(1), 1–18.
- [15] Thakkar, P., et al. (2025). Security versus convenience in UPI adoption: Behavioral insights from Indian users. *Electronic Commerce Research and Applications*, 59, 101268.
- [16] Wadkar, A., et al. (2025). Cybersecurity challenges in UPI: Fraud patterns and awareness gaps. *Information & Computer Security*, 33(1), 55–72.
- [17] Zhou, T. (2011). An empirical examination of initial trust in mobile payment. *Wireless Personal Communications*, 77(2), 1519–1531.