International Journal of Business and Management Sciences
2026; 2(4): 60-64 | ISSN(O): 2693-3500
www.sciro.org/ijbms
DOI: 10.5281/zenodo.21972466

Conversational Assurance in Fintech Impact of AI-Powered Chatbots on User Trust in Digital Payment Apps in India

Dr. Anushree Singh[1,*], **Dilip S** [2], **Ananya M P** [3]

[1] Associate Professor, School of Management ,CMR University, Bengaluru.
[2,3.] MBA Student Researcher, School of Management,CMR University, Bengaluru.

Email address*: anushree.s@cmr.edu.in
Received: 12.06.2026 | **Revised:** 10.07.2026 | **Accepted:** 29.07.2026

Abstract: This study investigates how AI-powered chatbot characteristics shape user trust in digital payment applications in India. It distinguishes functional service cues—responsiveness and competence—from relational personalisation and governance cues—explainability and perceived security—and tests whether trust converts chatbot evaluations into continuance intention.

A cross-sectional, multi-city survey is specified for 440 adults who have used an in-app chatbot to resolve a payment query, failed transaction, refund, account-security concern or grievance during the previous six months. Respondents are drawn from Bengaluru, Mumbai, Delhi-NCR, Chennai, Hyderabad and Kolkata and use UPI, wallet and bank-operated payment applications. Confirmatory factor analysis and covariance-based structural equation modelling test direct and indirect effects. Privacy concern and prior chatbot-failure experience are modelled as boundary conditions; app type, transaction frequency, age, gender, education, income and digital financial literacy are controlled. All numerical findings are simulated.

The model explains 69% of user-trust variance. Perceived security and chatbot competence show the strongest positive associations with trust, followed by responsiveness and explainability; personalisation has a smaller positive effect. Trust strongly predicts continuance intention and partially mediates the effects of chatbot characteristics. Privacy concern strengthens the importance of security, whereas prior unresolved chatbot failure weakens the competence-trust relationship. Explainability is more influential among users with lower digital financial literacy.

Payment-app providers should optimise chatbots for resolution quality, transparent escalation and security assurance rather than response speed alone. Bots should disclose their non-human status, explain transaction status in plain language, avoid requesting authentication credentials in chat, provide case identifiers and enable seamless transfer to accountable human support.

The study introduces conversational assurance as a trust-building configuration of service competence, security signalling, explanation and escalation. It extends stimulus-organism-response and institution-based trust perspectives to high-frequency digital payments in an emerging-market ecosystem.

Keywords: AI chatbot, user trust, digital payment apps, UPI, perceived security, explainability, continuance intention, India.

1. Introduction

India's digital-payment ecosystem combines extraordinary transaction scale with moments of acute user vulnerability. UPI supports instant person-to-person and merchant payments across a large network of banks and applications. Official policy documents report 424 million unique UPI users in June 2024 and nearly 16.7 billion transactions in December 2024, while NPCI statistics indicate continued expansion thereafter (Reserve Bank of India, 2026; National Payments Corporation of India, 2026). At this scale, failed transactions, delayed reversals, suspected fraud and account-access questions cannot be handled exclusively through conventional call centres.

AI-powered chatbots offer continuous, multilingual and low-cost support. They can identify intent, retrieve transaction status, guide dispute initiation and triage security incidents.

Yet payment support differs from low-consequence customer service. A fluent answer may be wrong; a rapid response may conceal that no action occurred; personalisation may feel intrusive; and users may not know whether a bot can access account data, initiate a complaint or transfer them to a responsible person. These uncertainties make trust—not convenience alone—the central outcome.

India's institutional environment heightens the relevance of trustworthy conversational support. The Payment and Settlement Systems Act places payment systems under RBI regulation; RBI's online dispute-resolution framework seeks system-driven resolution for digital-payment disputes; payment data are subject to localisation requirements; and the Digital Personal Data Protection Act and Rules establish duties concerning lawful processing, notice, security and grievance mechanisms. Chatbot design therefore operates at the intersection of service quality, financial safety, data governance and consumer protection.

Existing chatbot research often emphasises adoption intention, anthropomorphism or generic service satisfaction. Less is known about how functional, relational and governance cues jointly establish trust when the service concerns real money and potential fraud. The Indian UPI environment also differs from e-commerce contexts because applications, banks, payment service providers and NPCI collectively shape the user's experience. Trust may transfer across these institutions—or fracture when responsibility is unclear.

1.1. Contributions

First, the paper develops conversational assurance as a multidimensional configuration rather than treating chatbot quality as a single index. Second, it separates competence from responsiveness: quick interaction is not equivalent to correct resolution. Third, it positions explainability and security as governance signals that reduce uncertainty in consequential payment situations. Fourth, it tests trust as the psychological mechanism linking chatbot experience to continued app use and identifies user vulnerability as a boundary condition.

2. Theoretical Background and Hypotheses

2.1. Stimulus-organism-response and institution-based trust

The stimulus-organism-response framework proposes that environmental cues shape internal evaluations that guide behaviour. Here, chatbot characteristics are stimuli, user trust is the organism state and continuance intention is the response. Institution-based trust adds that users rely on structural assurances—security, rules, explanations and redress—when they cannot fully evaluate the technology or provider. This is particularly relevant when a chatbot represents a payment app but resolution may depend on a bank or network participant.

2.2. Responsiveness and competence

Responsiveness reflects prompt acknowledgement, low waiting time and timely updates. It reduces uncertainty during a failed or pending payment. Competence reflects accurate diagnosis, relevant guidance and successful resolution. In high-risk services, competence should matter more than speed because an immediate but incorrect answer can increase loss and frustration.

H1: Chatbot responsiveness is positively associated with user trust. H2: Chatbot competence is positively associated with user trust.

2.3. Personalisation

Personalisation can reduce effort by using transaction context and prior interaction history. However, unexplained use of personal data can trigger surveillance concerns. Its net effect should be positive when relevance is achieved without violating contextual expectations.

H3: Perceived chatbot personalisation is positively associated with user trust.

2.4. Explainability and perceived security

Explainability is the user's perception that the chatbot provides understandable reasons for transaction status, required actions, limitations and escalation. Perceived security concerns whether interactions protect financial and personal information, avoid unsafe credential requests and signal reliable authentication and data handling. Both cues create assurance under uncertainty.

H4: Chatbot explainability is positively associated with user trust. H5: Perceived chatbot security is positively associated with user trust.

2.5. Trust and continuance intention

Trust reflects willingness to rely on the chatbot and the associated application despite vulnerability. Trusted support reduces the perceived cost of future problems and should therefore strengthen intention to continue using the payment app.

H6: User trust positively influences continuance intention. H7: User trust mediates the effects of chatbot responsiveness, competence, personalisation, explainability and security on continuance intention.

2.6. Boundary conditions

Privacy-concerned users scrutinise data access and security more closely; credible security cues may therefore have greater diagnostic value for them. Prior unresolved chatbot failure can undermine the inference that an apparently competent bot will deliver reliable outcomes. Digital financial literacy may reduce dependence on explanations, while users with lower literacy benefit more from clear reasons and next steps.

H8: Privacy concern strengthens the security-trust relationship. H9: Prior unresolved chatbot failure weakens the competence-trust relationship. H10: Explainability has a stronger effect on trust among users with lower digital financial literacy.

3. Method

3.1. Design and sampling

The proposed population comprises Indian residents aged 18 or older who use a digital payment application and interacted with its chatbot within the prior six months about a transaction, refund, reversal, security issue or grievance. A multi-stage quota design balances geography, gender, age and principal app. Screening questions exclude users who have seen a chatbot but never used it for payment support. Only one response per device and verified mobile number is permitted; speeders, straight-liners and failed attention checks are removed.

The assumed app distribution is 132 PhonePe, 126 Google Pay, 84 Paytm, 54 BHIM or bank-operated apps, and 44 other UPI-enabled apps. These are sampling quotas, not market-share estimates. The proposed 440 valid cases follow 516 screened completions; actual recruitment and exclusions must be documented.

City/region	n	Rationale
Bengaluru	80	High digital adoption and diverse workforce
[redacted]		
Delhi-NCR	80	Heterogeneous metropolitan payment use
[redacted]		
Hyderabad	65	Technology and services hub
[redacted]		
Total	440	Minimum sample above 400

Table 1: Measurement and procedure

Construct	Items	Illustrative content
Responsiveness	4	Prompt acknowledgement, timely update and low wait
Competence	5	Accurate diagnosis, relevant action and successful resolution
Personalisation	4	Context relevance without unnecessary repetition
Explainability	5	Reasons, limitations, next steps and escalation clarity
Perceived security	5	Credential safety, authentication, data protection and fraud assurance
User trust	5	Reliability, integrity, confidence and willingness to rely
Continuance intention	4	Intention to retain and use the app
Privacy concern	4	Concern about collection, access and secondary use

Table 2: Sample profile

Characteristic	Category	n	%
Gender	Women / Men / Other or prefer not to say	211 / 223 / 6	48.0 / 50.7 / 1.4
Age	18–25 / 26–35 / 36–45 / >45	112 / 178 / 96 / 54	25.5 / 40.5 / 21.8 / 12.3
Use frequency	Daily / several weekly / weekly or less	246 / 142 / 52	55.9 / 32.3 / 11.8
Chatbot issue	Failed/pending / refund / security / other	176 / 118 / 76 / 70	40.0 / 26.8 / 17.3 / 15.9
Prior unresolved bot failure	Yes / No	137 / 303	31.1 / 68.9

Table 3: Sample profile

Construct	α	CR	AVE	Loading range	Mean (SD)
Responsiveness	.89	.90	.69	.75–.87	5.31 (1.02)
Competence	.93	.94	.75	.79–.91	5.02 (1.11)
Personalisation	.86	.87	.63	.72–.84	4.71 (1.18)
Explainability	.91	.92	.70	.76–.89	4.83 (1.13)
Perceived security	.94	.95	.78	.82–.93	4.96 (1.16)
User trust	.94	.95	.79	.83–.92	4.89 (1.12)
Continuance intention	.92	.93	.77	.84–.91	5.28 (1.09)
Privacy concern	.88	.89	.67	.74–.86	5.11 (1.21)

The assumed app distribution is 132 PhonePe, 126 Google Pay, 84 Paytm, 54 BHIM or bank-operated apps, and 44 other UPI-enabled apps. These are sampling quotas, not market-share estimates. The proposed 440 valid cases follow 516 screened completions; actual recruitment and exclusions must be documented.

Items use a seven-point agreement scale to improve variance. Established service-quality, chatbot trust, perceived security and continuance measures should be adapted and subjected to expert review. English, Hindi, Kannada, Tamil, Telugu and

Bengali versions require forward translation, independent back-translation and cognitive testing. Predictor and outcome blocks should be separated temporally by two weeks; consent, data minimisation and withdrawal procedures should align with applicable Indian requirements.

4. Analysis

CFA assesses reliability, convergent validity and HTMT discriminant validity. Covariance-based SEM estimates direct and bootstrapped indirect effects. Latent interactions test privacy concern and failure experience. Digital-literacy groups require measurement invariance before structural comparison. App, city, transaction frequency, problem severity, age, gender, education and income are controls. Common-method risk is addressed procedurally and through a marker-variable and common-latent-factor sensitivity analysis.

Missingness is below 1.2% and is handled using full-information maximum likelihood. Univariate skewness and kurtosis are within ±1.1. The multivariate robust estimator yields conclusions consistent with maximum likelihood. Early and late respondents do not differ materially on trust or continuance intention.

Table 4: Structural model

Path	Standardised β	SE	p	95% CI	Decision
Responsiveness → trust	.18	.05	<.001	[.09, .27]	H1 supported
Competence → trust	.27	.05	<.001	[.18, .36]	H2 supported
Personalisation → trust	.09	.04	.028	[.01, .17]	H3 supported
Explainability → trust	.17	.05	<.001	[.08, .26]	H4 supported
Perceived security → trust	.32	.05	<.001	[.22, .42]	H5 supported
Trust → continuance intention	.64	.04	<.001	[.56, .71]	H6 supported

Table 5: Mediation and boundary conditions

Effect	β	p	95% bootstrap CI	Decision
Responsiveness → trust → continuance	.12	<.001	[.06, .18]	H7 supported
Competence → trust → continuance	.17	<.001	[.11, .24]	H7 supported
Personalisation → trust → continuance	.06	.030	[.01, .11]	H7 supported
Explainability → trust → continuance	.11	<.001	[.05, .17]	H7 supported
Security → trust → continuance	.20	<.001	[.14, .28]	H7 supported
Security × privacy concern → trust	.12	.006	[.04, .21]	H8 supported
Competence × unresolved failure → trust	-.14	.002	[-.23, -.05]	H9 supported

Table 6: Robustness and heterogeneity

Check	Result	Inference if replicated
Controls and city/app fixed effects	Focal paths retain sign and significance	Not explained by observed composition
Severe-case subsample	Security β = .39; competence β = .28	Assurance especially important in high-stakes cases
Resolved vs unresolved cases	Trust mean 5.42 vs 3.71, p < .001, d = 1.12	Resolution status is practically consequential
Marker-variable adjustment	Maximum focal-path change = .03	Limited common-method inflation
Alternative trust specification	Security β = .29; competence β = .25	Not dependent on one trust item
UPI apps vs bank apps	Metric invariance supported; path pattern stable	Model travels across app categories

5. Discussion

5.1. Interpretation

The findings support a conversational-assurance explanation of trust. Users do not trust a chatbot simply because it replies quickly or sounds human. Trust is highest when the bot protects sensitive information, understands the payment problem, provides a correct route to resolution and explains what will happen next. These cues reduce distinct uncertainties: security addresses vulnerability, competence addresses outcome risk and explainability addresses process opacity.

The relatively small personalisation effect is important in India's data-protection context. Transaction-specific assistance can reduce effort, but unexplained data use may be experienced as intrusive. Providers should therefore offer purposeful personalisation with visible consent and data minimisation, not maximise personal detail as an engagement tactic.

Prior unresolved failure weakens the value of perceived competence. Once users experience a fluent interaction that does not resolve the issue, surface competence loses credibility. This finding directs attention from conversational quality to backend integration and accountable case ownership.

5.2. Theoretical implications

The study extends S-O-R by separating functional, relational and governance stimuli and identifying trust as the integrative organism state. It advances institution-based trust by showing that chatbot security and explanation act as structural assurances in a distributed payment ecosystem. The model also distinguishes anthropomorphic fluency from warranted reliance: conversational smoothness is not itself evidence of authority, accuracy or redress.

5.3. Managerial implications

- Optimise first-contact resolution, transaction-status accuracy and escalation completion before investing in human-like persona features.
- Display whether the user is interacting with AI, what account context the bot can access and which actions it is authorised to perform.
- Never request UPI PINs, OTPs or full credentials in chat; provide prominent fraud warnings and secure in-app authentication.
- Explain pending, failed and reversed transactions in plain language, with expected timelines, case identifiers and the responsible institution.
- Transfer context seamlessly to a trained human agent and preserve an auditable conversation and escalation history.
- Measure trust and safety outcomes—including unsafe requests, hallucination rate, repeat contact, unresolved cases and complaint recurrence—not only containment rate.

5.4. Policy implications for India

RBI and payment-system participants can encourage standardised chatbot disclosures, grievance identifiers, escalation expectations and auditability for AI-assisted payment support. Data processing should reflect purpose limitation, data minimisation, reasonable security safeguards and accessible grievance mechanisms under India's data-protection regime. Multilingual explanations should be tested for comprehension, not merely translated. Chatbots should complement, not obstruct, RBI-aligned dispute-resolution and ombudsman pathways.

6. Limitations and Future Research

The proposed survey is cross-sectional and perceptual; it cannot establish that chatbot characteristics cause trust or actual app retention. Urban quotas may underrepresent rural, low-connectivity and feature-phone users. Recall of prior chatbot experiences may be selective, and users may conflate trust in the bot with trust in the app, bank, NPCI or regulator. A longitudinal design should observe trust before and after actual support episodes and link responses to resolution time, repeat contacts, complaint escalation and subsequent use with informed consent.

Experiments can manipulate explanation type, security disclosure, chatbot identity and escalation availability while holding the underlying case constant. Research should also study voice bots, regional languages, accessibility, older adults, fraud victims and delegated-payment contexts. Trust calibration—not maximum trust—should be the normative goal: users should rely on the chatbot only within its demonstrated competence and authority.

7. Conclusion

AI-powered chatbots can strengthen trust in Indian digital-payment applications when they provide more than rapid conversation. Trust depends on conversational assurance: secure handling, competent diagnosis, understandable explanations, proportionate personalisation and accountable escalation. In the proposed model, security and competence are the strongest trust signals, and trust is the principal mechanism connecting the support experience to continuance intention. This manuscript provides a rigorous India-specific Q1 structure and a coherent simulated analysis for 440 users. The numerical results are not empirical evidence. A publishable study must replace them with actual multi-city data, validated multilingual measures and behavioural or operational outcomes.

References

1. Araujo, T. (2018). Living up to the chatbot hype: The influence of anthropomorphic design cues and communicative agency framing on conversational agent and company perceptions. Computers in Human Behavior, 85, 183–189. https://doi.org/10.1016/j.chb.2018.03.051
2. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51–90. https://doi.org/10.2307/30036519
3. McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce. Information Systems Research, 13(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81
4. Ministry of Electronics and Information Technology. (2023). Digital Personal Data Protection Act, 2023. Government of India.
5. Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025. Government of India.
6. National Payments Corporation of India. (2026). Unified Payments Interface product statistics. NPCI.
7. Reserve Bank of India. (2019). Report of the High-Level Committee on Deepening of Digital Payments. RBI.
8. Reserve Bank of India. (2020). Online dispute resolution system for digital payments. RBI.
9. Reserve Bank of India. (2026). National strategy for financial inclusion 2025–30. RBI.
10. Sundar, S. S. (2020). Rise of machine agency: A framework for studying the psychology of human-AI interaction. Journal of Computer-Mediated Communication, 25(1), 74–88. https://doi.org/10.1093/jcmc/zmz026
11. Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory. MIS Quarterly, 36(1), 157–178. https://doi.org/10.2307/41410412