Cybersecurity and Consumer Trust in India's Digital Payment Ecosystem

Sakshi Suhas Jadhav

College of Management and Computer Applications

MIT-ADT University

Neha Umesh Joshi

College of Management and Computer Applications

MIT-ADT University

Dr. Deepak Sahoo

College of Management and Computer Applications

MIT-ADT University

Abstract

India's digital payment ecosystem, anchored by the Unified Payments Interface (UPI), has grown into one of the largest real-time retail payment networks in the world, yet this expansion has been accompanied by a parallel rise in phishing, SIM-swap fraud, fake payment applications and social-engineering attacks that target ordinary consumers. This paper examines how perceived cybersecurity risk, security awareness and consumer trust jointly shape the continued usage intention of digital payment platforms among Indian consumers. Building on the technology acceptance and trust-risk literature, three hypotheses are proposed and tested using a synthetically generated dataset of 412 respondents constructed to reflect plausible response patterns reported in comparable Indian and cross-country fintech-adoption studies. Descriptive statistics, reliability analysis, correlation and hierarchical regression are used to examine the relationships between the constructs. The illustrative results indicate that perceived cybersecurity risk is negatively associated with consumer trust, that trust is a strong positive predictor of continued usage intention, and that security awareness moderates the risk-trust relationship. The paper discusses implications for payment service providers, regulators and financial literacy programmes, and positions the analysis as an illustrative academic template that can be re-estimated once primary survey data is collected.

Keywords: *cybersecurity, consumer trust, digital payments, UPI, fintech adoption, perceived risk, security awareness, India*

1. Introduction

Digital payments have moved from the margins to the mainstream of India's financial system over the past decade. The Unified Payments Interface, government-backed digital public infrastructure and an expanding smartphone base have together produced a payments ecosystem in which billions of low-value, high-frequency transactions are routed through mobile applications every month. Government-led design choices behind the UPI architecture, and the network effects this created, are widely credited with the pace of adoption observed in both urban and rural markets (Gopika et al., 2026), while digital public infrastructure more broadly has been linked to measurable gains in financial inclusion and economic activity (Balasundaram et al., 2026). Studies of UPI in rural India similarly document its role in extending formal

payment rails to previously underserved households (Haque et al., 2025), and digital financial literacy is repeatedly identified as a condition for these gains to translate into sustained financial well-being (Bhat et al., 2024).

This growth has an underside. As transaction volumes rise, so does the attack surface available to fraudsters, and cybercrime directed at digital-finance users has become an economically significant phenomenon rather than a peripheral nuisance. State-level evidence from India links the intensity of digital-economy activity to measurable increases in reported cybercrime (Anthony, 2026), older and less digitally fluent users have been shown to be disproportionately exposed to fraud tactics that exploit unfamiliarity with app interfaces (Kumar & Patel, 2025), and consumers who have themselves experienced cyber fraud report systematically different satisfaction and continuance patterns than those who have not (Kashyap et al., 2026). Sector-agnostic work on privacy risk in digital payment systems finds that country-level regulatory and infrastructural conditions shape the baseline risk consumers face before any single transaction is initiated (Akanfe et al., 2020), and reviews of cybersecurity awareness programmes in digital commerce suggest that awareness interventions can measurably change user behaviour, though effects are uneven across demographic groups (Isa et al., 2026).

Trust is the variable that sits between these two trends. A large and growing body of work treats trust, alongside perceived risk, as the proximate psychological mechanism through which security concerns are converted into adoption or abandonment decisions (Samuel et al., 2026) (Aracil et al., 2025) (Czechowska & Paduszyńska, 2025). Meta-analytic evidence on the diffusion of financial-technology services confirms that risk and trust are among the most consistently significant predictors of technology adoption across markets (Ladeira et al., 2026), and country-specific studies extend this logic to related domains such as Islamic banking following a cyberattack (Aisyah et al., 2025), cryptocurrency markets (Lee, 2026) (Perdana et al., 2025), and central bank digital currency (Khan et al., 2026). Despite this volume of research, comparatively few studies model the cybersecurity-trust-usage chain specifically for India's UPI-centred retail payment environment, where the combination of very high transaction frequency, low average transaction value and a still-maturing digital literacy base creates a distinctive risk profile. This paper addresses that gap by proposing and testing a parsimonious model linking perceived cybersecurity risk, security awareness and consumer trust to continued usage intention, using a synthetically generated dataset constructed to be illustrative of the analytical approach a full-scale primary survey would follow.

2. Literature Review

2.1 Growth and Architecture of Digital Payments in India

India's payment infrastructure has been deliberately engineered as public digital infrastructure rather than left purely to private-sector competition, and a time-series analysis of the factors associated with UPI's growth attributes the system's scale to this design choice combined with interoperability across banks and non-bank wallets (Gopika et al., 2026). This account is consistent with broader evidence that digital public infrastructure raises financial inclusion and rural economic growth (Balasundaram et al., 2026), and with case-study evidence that UPI has materially widened access to formal payment rails outside metropolitan India (Haque et al., 2025). The digital payment-financial inclusion relationship is not unique to India: cross-country evidence links payment-system innovation to inclusion outcomes more generally (Niankara & Traoret, 2023), while comparative work on buy-now-pay-later adoption suggests that new payment modalities introduce their own adoption barriers even where core payment rails are mature (Mukherjee, 2025). Underlying all of these accounts is a recognition that digital financial literacy is a precondition for translating access into sustained, welfare-improving use (Bhat et al., 2024) (Iqbal et al., 2025).

2.2 Cybersecurity Threats in the Digital Payments Environment

The same infrastructural features that make UPI convenient — instant settlement, minimal friction and interoperable identifiers — also make it attractive to fraudsters. Panel-data evidence from Indian states shows a positive association between the intensity of digital economic activity and reported cybercrime, suggesting that exposure scales with usage rather than being a fixed cost of digitisation (Anthony, 2026). Fraud-detection research using deep learning architectures on bank transaction data illustrates the technical arms race underway between payment providers and adversaries (Prashanth et al., 2026), while behavioural research on older adults finds that digital habits formed without adequate

security grounding leave this group specifically vulnerable to cyber fraud (Kumar & Patel, 2025). Adoption of personal cyber-insurance products in India remains low despite this exposure, with barrier-analysis research identifying cost, low awareness and weak enforcement as the principal obstacles (Mathur & Singh, 2026). Related infrastructure research on securing Internet-of-Things and connected-device ecosystems similarly emphasises that security is best treated as a systemic property of the ecosystem rather than a feature bolted onto individual applications (Siraparapu & Azad, 2024), a point echoed in earlier work on network-security situational awareness (Naik, n.d.) and context-aware wireless-network security (Mishra, 2013).

2.3 Perceived Risk, Trust and Technology Adoption

Trust and perceived risk are treated in the technology-adoption literature as competing forces that jointly determine whether a consumer moves from trial to habitual use. Recent work on digital payment adoption finds that ease of use influences satisfaction only when mediated through trust, with perceived risk acting as a countervailing force (Samuel et al., 2026). A systematic review of the trust-financial inclusion relationship concludes that trust operates both as an antecedent of adoption and as an outcome that is continuously renegotiated through each transaction experience (Aracil et al., 2025), while bibliometric analysis of the fintech-adoption literature confirms that trust has grown from a peripheral to a central construct in the field over the past decade (Czechowska & Paduszyńska, 2025). A meta-analysis spanning multiple financial-technology categories similarly finds that risk and trust variables outperform most other predictors of adoption intention in explanatory power (Ladeira et al., 2026). Sector-specific evidence extends this logic: trust rebuilding after a cyberattack has been shown to be a slow and uneven process in Islamic banking contexts (Aisyah et al., 2025), and cross-country research on cryptocurrency markets finds that cultural and ethical framing of trustworthiness shapes willingness to transact even where objective security features are held constant (Perdana et al., 2025) (Lee, 2026). Work on central bank digital currency shows that perceived risk operates through both a hard-trust channel (confidence in technical safeguards) and a soft-trust channel (confidence in the issuing institution), a distinction that maps closely onto the risk constructs used in the present study (Khan et al., 2026).

2.4 Security Awareness and Consumer Behaviour

Security awareness is increasingly treated as a distinct construct from trust and risk perception, capturing what consumers know rather than how they feel. Factor-analytic work on cybersecurity awareness programmes in digital commerce finds that awareness interventions shift self-protective behaviour more reliably than they shift trust directly, implying an indirect or moderating pathway (Isa et al., 2026). Structural modelling of Sharia-compliant digital banking adoption finds that financial literacy and digital literacy jointly condition the strength of the risk-adoption relationship, with more literate users discounting risk signals less but also reacting to them more decisively (Nugraha et al., 2026). Gamification and engagement-design research on mobile payment applications suggests that interface design choices can inadvertently reduce the salience of security cues, with implications for how awareness translates into behaviour in practice (Neiva et al., 2026). A structured review of the mobile-payment research field identifies user-side knowledge gaps as one of the more persistent themes in the literature, despite more than a decade of applied research on the topic (Shiau et al., 2025).

2.5 Regulation, Governance and Emerging Payment Technologies

Regulatory design shapes the baseline security environment within which individual trust judgements are formed. Comparative analysis of AI and data-governance regulation in China and India finds substantially different philosophies toward platform oversight, with consequences for how quickly security standards can be imposed on payment intermediaries (Zhang et al., 2025), while research on platform-compatibility strategy under data-security regulation shows that regulatory stringency can reshape competitive dynamics among payment providers themselves (Wu et al., 2025). Blockchain-based approaches to identity and transaction verification are frequently proposed as a partial technical remedy: evidence from blockchain-enabled digital-currency adoption studies (Bhatnagr et al., 2024), blockchain security research more broadly (Mishra & Phansalkar, 2025), and green and adoption-oriented blockchain research (Phansalkar et al., 2023) together suggest that distributed-ledger mechanisms can reduce certain categories of fraud while introducing new governance questions of their own. Public-private partnership models for blockchain-enabled financial infrastructure are examined in (Shah & Raj, 2025), DEMATEL-based barrier analyses of blockchain adoption appear in (Aggarwal & Shah, 2026) and related sector studies, and the FinTech-microfinance interface is reviewed from a

regulatory perspective in (Sebai & Bouzadi, 2025). Systematic reviews of FinTech adoption drivers more generally converge on the finding that regulatory clarity, security infrastructure and consumer trust are mutually reinforcing rather than independent levers (Rajpal & Manglani, 2026) (Ghosh & Golder, 2026) (Bhowal & Shil, 2026) (Ullah et al., 2026) (Xu et al., 2025) (Trotta et al., 2026) (Meraj et al., 2026) (Ramayanti et al., 2026) (Griffiths et al., 2023) (Chotia et al., 2025) (Almoghayer & Mahmoud, 2025) (Karami & Moghadam, 2026) (Jhankar et al., 2026) (Bajwa et al., 2025) (Liaw & Godinho, 2026). Adjacent quantitative finance research on sentiment-driven forecasting (Dash & Mishra, 2024) (Dash & Mishra, 2024) (Mishra & Dash, 2025) (Mishra & Deshmukh, 2023) and on risk analysis of banking and mutual-fund products (Mishra & Raje, 2019) illustrates the same underlying theme from a market-risk rather than a payment-security angle: consumer-facing financial technologies are only as effective as the trust infrastructure — technical, regulatory and psychological — built around them.

3. Research Gap and Objectives

Three gaps emerge from this review. First, most trust-risk-adoption studies are estimated on data from mature digital-payment markets outside India or on India-adjacent but non-payment domains such as banking or insurance; very few isolate the UPI-specific consumer experience. Second, security awareness is usually treated as a control variable rather than as a moderator of the risk-trust relationship, despite theoretical reasons to expect that awareness changes how strongly perceived risk translates into distrust. Third, few studies connect perceived cybersecurity risk all the way through to continued usage intention within a single model, instead stopping at either the trust stage or the initial-adoption stage. This paper addresses these gaps with three specific objectives: (i) to quantify the association between perceived cybersecurity risk and consumer trust among Indian digital-payment users; (ii) to test whether consumer trust translates into continued usage intention; and (iii) to examine whether security awareness moderates the strength of the risk-trust relationship.

4. Conceptual Framework and Hypotheses

The proposed model treats perceived cybersecurity risk (PCR) and security awareness (SA) as antecedents of consumer trust (CT), and consumer trust as the proximate driver of continued usage intention (CUI). Security awareness is additionally modelled as a moderator of the PCR-CT path, consistent with the awareness-behaviour evidence reviewed in Section 2.4 (Isa et al., 2026) (Nugraha et al., 2026). On this basis, the following hypotheses are proposed.

H1. Perceived cybersecurity risk has a significant negative effect on consumer trust in digital payment platforms.

H2. Consumer trust has a significant positive effect on continued usage intention of digital payment platforms.

H3. Security awareness significantly moderates the relationship between perceived cybersecurity risk and consumer trust, such that the negative effect of risk on trust is weaker among consumers with higher security awareness.

5. Research Methodology

5.1 Research Design and Synthetic Data Note

The study adopts a quantitative, cross-sectional design typical of technology-adoption research in this stream (Samuel et al., 2026) (Ladeira et al., 2026). Because no primary survey has yet been fielded, the dataset analysed in Section 6 is synthetically generated: response distributions, inter-item correlations and demographic proportions were constructed to be plausible and internally consistent with patterns reported in comparable Indian and cross-country digital-payment and fintech-adoption studies cited throughout this paper, rather than drawn from actual respondents. The dataset and results are presented for illustrative and methodological purposes — to demonstrate the analytical pipeline a live study would follow — and should be re-estimated on primary data before any substantive claim is drawn from them.

5.2 Sample and Procedure

The synthetic sample comprises 412 records structured to represent adult digital-payment users across six Indian cities spanning three tiers of urbanisation (metro, tier-2 and tier-3), reflecting the geographic spread emphasised in rural-

inclusion research on UPI (Haque et al., 2025) (Balasundaram et al., 2026). Table 1 summarises the demographic composition of the synthetic sample.

Table 1. Demographic Profile of the Synthetic Sample (N = 412)

Category	Segment	n	%
Gender	Male	231	56.1
	Female	178	43.2
	Other / prefer not to say	3	0.7
Age group	18–25 years	104	25.2
	26–35 years	142	34.5
	36–45 years	97	23.5
	46 years and above	69	16.8
City tier	Metro	168	40.8
	Tier-2	146	35.4
	Tier-3	98	23.8
Monthly UPI transactions	Fewer than 10	88	21.4
	10–30	179	43.4
	More than 30	145	35.2
Prior fraud experience	Yes	97	23.5
	No	315	76.5

5.3 Measures

Four constructs were operationalised using multi-item, seven-point Likert-type scales adapted from the trust-risk-adoption literature reviewed above: Perceived Cybersecurity Risk (5 items, adapted from privacy- and risk-focused digital-payment research; (Akanfe et al., 2020) (Khan et al., 2026)), Security Awareness (4 items, adapted from cybersecurity awareness research; (Isa et al., 2026) (Nugraha et al., 2026)), Consumer Trust (5 items, adapted from digital-payment trust research; (Samuel et al., 2026) (Aracil et al., 2025)), and Continued Usage Intention (4 items, adapted from technology-continuance research; (Mukherjee, 2025) (Shiau et al., 2025)). Table 2 reports the synthetic reliability statistics for each construct.

Table 2. Constructs, Items and Reliability (Synthetic)

Construct	Items	Cronbach's α	Composite Reliability	AVE
Perceived Cybersecurity Risk (PCR)	5	0.86	0.89	0.62
Security Awareness (SA)	4	0.81	0.87	0.63
Consumer Trust (CT)	5	0.88	0.91	0.67
Continued Usage Intention (CUI)	4	0.84	0.89	0.66

6. Data Analysis and Results

6.1 Descriptive Statistics

Table 3 reports the means, standard deviations and skewness of the four study constructs. Perceived cybersecurity risk shows the widest dispersion of the four constructs, consistent with the heterogeneous fraud-exposure patterns reported across age and literacy groups in the literature (Kumar & Patel, 2025) (Mathur & Singh, 2026). Consumer trust and continued usage intention are both left-skewed, indicating that the majority of synthetic respondents report moderately favourable trust and usage-continuance scores, again broadly consistent with the high observed UPI transaction volumes documented in adoption research (Gopika et al., 2026).

Table 3. Descriptive Statistics (Synthetic, N = 412)

Construct	Mean	SD	Min	Max	Skewness
Perceived Cybersecurity Risk (PCR)	3.82	1.24	1.00	7.00	0.18
Security Awareness (SA)	4.65	1.09	1.00	7.00	-0.32
Consumer Trust (CT)	4.91	1.02	1.20	7.00	-0.47
Continued Usage Intention (CUI)	5.08	0.97	1.40	7.00	-0.55

6.2 Correlation Analysis

Table 4 presents the bivariate correlation matrix. Perceived cybersecurity risk correlates negatively with both consumer trust and continued usage intention, while security awareness correlates positively with trust. Consumer trust and continued usage intention are strongly and positively correlated, foreshadowing the regression results reported below.

Table 4. Bivariate Correlation Matrix (Synthetic)

Construct	1. PCR	2. SA	3. CT	4. CUI
1. Perceived Cybersecurity Risk	1.00			
2. Security Awareness	-0.22**	1.00		
3. Consumer Trust	-0.46**	0.34**	1.00	
4. Continued Usage Intention	-0.29**	0.31**	0.58**	1.00

*Note. **p < .01 (synthetic values, two-tailed).*

6.3 Hypothesis Testing

Hypotheses were tested using hierarchical multiple regression. Model 1 regresses consumer trust on perceived cybersecurity risk and security awareness (testing H1); Model 2 regresses continued usage intention on consumer trust, controlling for perceived cybersecurity risk (testing H2); and Model 3 introduces the risk × awareness interaction term to test the moderating role of security awareness (testing H3). Table 5 reports standardised coefficients, t-values, significance levels and variance inflation factors (VIF) for all three models.

Table 5. Hierarchical Regression Results (Synthetic)

Predictor	Model 1 (DV: CT) β	Model 2 (DV: CUI) β	Model 3 (DV: CT, moderation) β	VIF
Perceived Cybersecurity Risk (PCR)	-0.41***	-0.09*	-0.39***	1.18
Security Awareness (SA)	0.26***	—	0.24***	1.15
Consumer Trust (CT)	—	0.52***	—	1.22
PCR × SA (interaction)	—	—	0.19**	1.31
R^2	0.29	0.35	0.33	
Adjusted R^2	0.28	0.34	0.32	
F	82.4***	108.7***	66.9***	

*Note. *p < .05, **p < .01, ***p < .001 (synthetic values). Model 2 controls for PCR.*

Across the three models, perceived cybersecurity risk is a significant negative predictor of consumer trust (β = -0.41, p < .001), supporting H1 and consistent with risk-trust findings reported for digital payments more broadly (Samuel et al., 2026) (Aracil et al., 2025). Consumer trust is a significant positive predictor of continued usage intention (β = 0.52, p < .001) even after controlling for perceived risk, supporting H2 and mirroring the trust-continuance relationship documented in technology-continuance research on mobile and buy-now-pay-later payment products (Mukherjee, 2025) (Shiau et al., 2025). The risk × awareness interaction term is significant and positively signed (β = 0.19, p < .01), indicating that the negative effect of perceived risk on trust is attenuated among consumers with higher security awareness, supporting H3 and aligning with awareness-moderation evidence from the cybersecurity and digital-banking literature (Isa et al., 2026) (Nugraha et al., 2026). All VIF values remain below the conventional threshold of 5, indicating

that multicollinearity is unlikely to be distorting the coefficient estimates. Table 6 summarises the hypothesis-testing outcomes.

Table 6. Summary of Hypothesis Testing

Hypothesis	Path	Result (synthetic)	Decision
H1	PCR → CT (negative)	$\beta = -0.41$, $p < .001$	Supported
H2	CT → CUI (positive)	$\beta = 0.52$, $p < .001$	Supported
H3	SA moderates PCR → CT	β(interaction) = 0.19, $p < .01$	Supported

7. Discussion

The pattern of results is consistent with the trust-centred view of digital-payment adoption that dominates the recent literature: perceived cybersecurity risk erodes trust, and trust — rather than risk directly — is what carries through to continued usage intention (Samuel et al., 2026) (Ladeira et al., 2026) (Aracil et al., 2025). This mediated structure has a practical implication that is sometimes underweighted in policy discussions of digital-payment security: interventions that reduce objective risk (better fraud detection, stronger authentication) matter primarily to the extent that they are visible enough to shift consumers' trust judgements, a point consistent with findings on trust rebuilding after a cyberattack in banking contexts (Aisyah et al., 2025) and with hard-trust/soft-trust distinctions drawn in CBDC research (Khan et al., 2026). The moderating role of security awareness found here (H3) suggests that financial-literacy and cyber-hygiene campaigns are not merely additive to technical security investment but interact with it: the same objective risk level appears to erode trust less among more aware consumers, a finding that parallels literacy-moderation effects reported in Sharia digital-banking adoption research (Nugraha et al., 2026) and in the broader digital financial literacy literature (Bhat et al., 2024) (Iqbal et al., 2025). These findings should be read as illustrative given the synthetic nature of the underlying data, but the analytical structure — and the direction of the hypothesised effects — is grounded in a substantial and largely convergent body of prior empirical work.

8. Implications

8.1 Theoretical Implications

The study extends the trust-risk-adoption framework used widely in the fintech literature (Samuel et al., 2026) (Aracil et al., 2025) (Ladeira et al., 2026) (Czechowska & Paduszyńska, 2025) by explicitly modelling security awareness as a moderator rather than a direct predictor, offering a more precise account of how literacy interventions are likely to operate. It also extends this framework to the UPI-specific Indian context, complementing digital-public-infrastructure and rural-inclusion research that has so far emphasised access and usage volume over the psychological mechanisms underlying continued use (Gopika et al., 2026) (Balasundaram et al., 2026) (Haque et al., 2025) (Niankara & Traoret, 2023).

8.2 Managerial and Policy Implications

For payment-service providers, the results suggest that visible, easily understood security communication may do more to sustain usage than incremental improvements to back-end fraud detection that remain invisible to the consumer, echoing awareness-programme findings from digital-commerce cybersecurity research (Isa et al., 2026). For regulators and financial-inclusion policymakers, the moderating role of awareness implies that digital and financial literacy programmes should be sequenced alongside, rather than after, the rollout of new payment infrastructure, particularly in the tier-2 and tier-3 markets where UPI's most recent growth has been concentrated (Haque et al., 2025) (Balasundaram et al., 2026) (Bhat et al., 2024). Cyber-insurance providers may also find in these results an argument for bundling awareness content with policy sign-up, given the low baseline adoption of personal cyber-insurance documented in barrier-analysis research (Mathur & Singh, 2026).

9. Limitations and Future Research

The principal limitation of this study is that the dataset analysed is synthetic rather than collected from actual digital-payment users; the descriptive statistics, correlations and regression coefficients reported in Section 6 are illustrative of the analytical pipeline rather than empirical findings, and should not be cited as evidence of real-world effect sizes. Future research should re-estimate the proposed model on a probability-based or quota-based primary sample of Indian digital-payment users, ideally with longitudinal follow-up to capture how trust evolves after a security incident, in the spirit of the pre-post cyberattack designs used in Islamic-banking trust research (Aisyah et al., 2025). Extensions could also incorporate objective fraud-exposure data alongside self-reported risk perception, following fraud-detection approaches used in transaction-level modelling (Prashanth et al., 2026), and could test whether the moderating role of awareness generalises to emerging payment modalities such as central bank digital currency (Khan et al., 2026) and cryptocurrency-linked payment rails (Lee, 2026) (Perdana et al., 2025).

10. Conclusion

This paper proposes and tests a model in which perceived cybersecurity risk reduces consumer trust in digital payment platforms, consumer trust drives continued usage intention, and security awareness moderates the risk-trust relationship. Using an illustrative synthetic dataset constructed to reflect patterns documented in the wider fintech-adoption, digital-payment and cybersecurity-awareness literature, all three hypotheses receive support. The findings reinforce a trust-centred reading of digital-payment sustainability in India: as UPI and related infrastructure continue to scale, the durability of consumer engagement is likely to depend less on the sheer volume of security investment than on whether that investment is communicated in a way that measurably shifts consumer trust, and on whether digital and financial literacy programmes keep pace with the infrastructure they are meant to protect.

References

Aggarwal, M., & Shah, M.A. (2026). Blockchain adoption in agri-food supply chain: a DEMATEL-based analysis of interdependent barriers and strategic imperatives. *Journal of Agribusiness in Developing and Emerging Economies*. https://doi.org/10.1108/JADEE-06-2025-0275

Aisyah, M., Sesunan, Y.S., & Wicaksono, A.T.S. (2025). Customers' trust in Islamic banking post-cyberattack leads to digital service breakdowns in Indonesia. *Sustainable Futures*, *10*, 101530. https://doi.org/10.1016/j.sftr.2025.101530

Akanfe, O., Valecha, R., & Rao, H.R. (2020). Assessing country-level privacy risk for digital payment systems. *Computers & Security*, *99*, 102065. https://doi.org/10.1016/j.cose.2020.102065

Almoghayer, W.J., & Mahmoud, H.A. (2025). The adoption of cross-border payment: A comparative study of belt and road countries. *Borsa Istanbul Review*, *25*(6), 1626–1644. https://doi.org/10.1016/j.bir.2025.10.011

Anthony, B. (2026). Economic determinants of cybercrime in India: a state-level panel data analysis. *Safer Communities*, *25*(2), 109–121. https://doi.org/10.1108/SC-03-2025-0020

Aracil, E., Fernández-Méndez, L., Roch-Dupré, D., & Fuertes, F.J. (2025). Trust and financial inclusion: A literature review with reference to the digital transformation. *Heliyon*, *11*(16), e44128. https://doi.org/10.1016/j.heliyon.2025.e44128

Bajwa, F.A., Fu, J., Bajwa, I.A., Ahmad, S., & Mahmood, F. (2025). Factors influencing usage and loyalty for payment app customers in Saudi Arabia. *Acta Psychologica*, *255*, 104961. https://doi.org/10.1016/j.actpsy.2025.104961

Balasundaram, E., V., A., Navalgund, N., P., A., & Hanji, S. (2026). The impact of digital public infrastructure on financial inclusion and economic growth in rural India: evidence from the UPI revolution. *Indian Growth and Development Review*, *19*(1), 109–126. https://doi.org/10.1108/IGDR-12-2024-0213

Bhat, S.A., Lone, U.M., SivaKumar, A., & Krishna, U.G. (2024). Digital financial literacy and financial well-being -- evidence from India. *International Journal of Bank Marketing*, *43*(3), 522–548. https://doi.org/10.1108/IJBM-05-2024-0320

Bhatnagr, P., Rajesh, A., & Misra, R. (2024). The impact of Fintech innovations on digital currency adoption: a blockchain-based study in India. *International Journal of Accounting and Information Management*, *33*(2), 313–333. https://doi.org/10.1108/IJAIM-11-2023-0275

Bhowal, P., & Shil, P. (2026). Exploring FinTech adoption: A systematic literature review on user acceptance. *Telematics and Informatics Reports*, *22*, 100343. https://doi.org/10.1016/j.teler.2026.100343

Chiwhane, S., Deepa, M., & Shweta, K. (2017). IoT based fuel monitoring for future vehicles. *International Journal of Advanced Research in Computer and Communication Engineering*, *6*, 295–297.

Chotia, V., Alghafes, R., Sharma, M., & Virmani, N. (2025). Chronocraft: unveiling enablers and overcoming barriers in Fintech-driven logistics and supply chain management in the digital era. *Technological Forecasting and Social Change*, *217*, 124168. https://doi.org/10.1016/j.techfore.2025.124168

Czechowska, I.D., & Paduszyńska, M. (2025). The Role of Trust in Fintech Adoption and Development: Bibliometric Analysis. *Procedia Computer Science*, *270*, 2790–2798. https://doi.org/10.1016/j.procs.2025.09.401

Dash, A. S., & Mishra, U. (2024). Application of NLU based sentiment analysis in the hybrid stock price forecasting model using deep learning model. *2024 IEEE Pune Section International Conference (PuneCon)*, 1–6.

Dash, A. S., & Mishra, U. (2024). Stock market trend prediction model using deep learning based sentiment analysis of financial data. *2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS)*, 1–7.

Deepa Mishra, T. Y. (2017). Secure IoT based healthcare system with BSN. *International Engineering Research Journal*, *2*(9), 3208–3011.

Ghosh, P., & Golder, U. (2026). Exploring the effects of FinTech adoption on traditional banking: A systematic literature review on opportunities and challenges. *Digital Business*, *6*(1), 100163. https://doi.org/10.1016/j.digbus.2026.100163

Gopika, C.G., Biju, A.V., Sasidharan, A., & Sarpong-Kumankoma, E. (2026). Government-led design and growth of India's UPI ecosystem: a time series analysis of associated factors. *Journal of Science and Technology Policy Management*. https://doi.org/10.1108/JSTPM-07-2024-0284

Griffiths, P.D.R., Mukherjee, A., & Sinha, P.N. (2023). Determinants of Fintech diffusion in emerging markets: a service ecosystem perspective. *International Journal of Emerging Markets*, *20*(13), 356–376. https://doi.org/10.1108/IJOEM-04-2024-0678

Haque, M.I., N.P., A.A., & Akhtar, S.J. (2025). UPI and financial inclusion in rural India: A case study. *Development and Sustainability in Economics and Finance*, *6*, 100056. https://doi.org/10.1016/j.dsef.2025.100056

Iqbal, Z., Rao, Z.R., Akram, M., & Ahmad, M. (2025). Bridging the gap: how knowledge sharing, individual values, financial literacy and incentives drive digital payment adoption in Pakistan. *South Asian Journal of Business Studies*, *15*(2), 165–184. https://doi.org/10.1108/SAJBS-06-2024-0253

Isa, R.A., Setiawan, B., & Pakaja, F. (2026). Cybersecurity awareness in the digital commerce ecosystem: factor analysis, program impact and future trends for consumers and MSMEs. *Information and Computer Security*. https://doi.org/10.1108/ICS-11-2025-0468

Jhankar, S.C., Sethi, S.R., Bal, G.R., Sharma, A., & Maharana, K.C. (2026). Digital finance and socio-economic empowerment: Quantifying research gaps and policy-induced structural change. *Strategic Business Research*, *2*(1), 100195. https://doi.org/10.1016/j.sbr.2026.100195

Karami, A., & Moghadam, H.E. (2026). Digital transformation and risk dynamics: The inverted U-shaped impact of FinTech on Iranian banks' risk-taking behavior. *International Journal of Information Management Data Insights*, *6*(1), 100418. https://doi.org/10.1016/j.jjimei.2026.100418

Kashyap, A.K., Priyanka, & Gupta, P. (2026). Do cyber fraud experiences matter? Revisiting user motivations and satisfaction in driving FinTech continuance. *Journal of Financial Crime*, *33*(1), 94–113. https://doi.org/10.1108/JFC-09-2025-0300

Khan, F.N., Zohaib, M., & Arshad, M.U. (2026). The role of perceived risk factors in willingness to use CBDC: mediating role of hard trust and soft trust. *International Journal of Bank Marketing*, *44*(4), 738–773. https://doi.org/10.1108/IJBM-03-2025-0252

Kumar, S., Tripathi, K., & Das, S. (2025). Chapter Ten - Cybersecurity of energy systems. *Method of Process Systems in Energy Systems: Emerging Energy Systems Part II*, *9*, 297–339. https://doi.org/10.1016/bs.mcps.2025.06.003

Kumar, S., & Patel, M. (2025). Digital habits and cyber vulnerabilities among older victims of cyber fraud. *Working with Older People*, *29*(4), 433–443. https://doi.org/10.1108/WWOP-04-2025-0018

Ladeira, W.J., Jafar, S.H., & Santini, F.d.O. (2026). A meta-analysis of technological adoption of financial services: investigating risk and trust perception effects. *International Journal of Bank Marketing*, *44*(3), 393–421. https://doi.org/10.1108/IJBM-02-2025-0156

Lee, J. (2026). Cryptocurrency travel revolution: Unraveling the mystery of consumer trust in market environment volatility. *International Journal of Hospitality Management*, *133*, 104506. https://doi.org/10.1016/j.ijhm.2025.104506

Liaw, S., & Godinho, M.A. (2026). Chapter 8 - Governance, trust, and reciprocity to advance digital health maturity. *Digital Health Maturity: Quality, Interoperability, and Innovation*, 195–219. https://doi.org/10.1016/B978-0-323-95260-6.00008-3

Mathur, T., & Singh, K. (2026). Barriers and drivers to the adoption of personal cyber insurance in India: a DEMATEL approach. *Information and Computer Security*, *34*(1), 141–169. https://doi.org/10.1108/ICS-12-2024-0315

Meraj, M., Ishrat, I., & Kaur, M. (2026). FinTech adoption in the UAE: total interpretive structural modeling of drivers and challenges. *Qualitative Research in Financial Markets*, *18*(3), 640–671. https://doi.org/10.1108/QRFM-02-2024-0024

Mishra, D. (2013). Knowledge based context awareness network security for wireless networks. *International Journal of Computer Trends and Technology*, *4*(10), 3751–3757.

Mishra, U., & Deshmukh, A. (2023). Sentiment analysis using machine learning for forecasting Indian stock trend: A brief survey. *Finance: Theory and Practice*, *27*(6), 136–147.

Mishra, D., & Phansalkar, S. (2025). Blockchain security in focus: A comprehensive investigation into threats, smart contract security, cross-chain bridges, vulnerabilities detection tools & techniques. *IEEE Access*.

Mishra, U., & Dash, A. S. (2025). A novel approach of stock price forecasting model using NLU-based sentiment analysis and deep learning LSTM model. *Neural Computing and Applications*, 1–30.

Mishra, U., & Raje, H. (2019). Fundamental analysis of selected banks for investment decisions. *International Journal of Research in Social Sciences*, *9*(2).

Mishra, D. U., & Kadale, N. K. (2017). Mining association rules using R environment. *International Journal of Computer Applications*, *157*(4).

Mukherjee, S. (2025). Factors impeding buy now, pay later (BNPL) adoption in India: A mixed-method approach. *Journal of Retailing and Consumer Services*, *87*, 104402. https://doi.org/10.1016/j.jretconser.2025.104402

Naik, D. T. (n.d.). Knowledge based network security situation awareness for computer networks.

Neiva, R., Ferreira, H., & Azevedo, A. (2026). Understanding the impact of gamification features on user retention: evidence from a mobile payment app. *International Journal of Bank Marketing*, *44*(3), 547–570. https://doi.org/10.1108/IJBM-07-2025-0567

Niankara, I., & Traoret, R.I. (2023). The digital payment-financial inclusion nexus and payment system innovation within the global open economy during the COVID-19 pandemic. *Journal of Open Innovation: Technology, Market, and Complexity*, *9*(4), 100173. https://doi.org/10.1016/j.joitmc.2023.100173

Nugraha, Y.D., Permana, R.M.T., Saraswati, N., Gumelar, E.T., Rohandi, M.M.A., & Wirayudha, A. (2026). Barriers, literacy and well-being in Sharia digital banking adoption: a structural model with gender-based multi-group analysis. *Journal of Islamic Accounting and Business Research*. https://doi.org/10.1108/JIABR-11-2025-0834

Perdana, A., Lee, W.E., Lim, C.Y., Pan, G., & Seow, P. (2025). Effects of ethics and culture on one's trust in cryptocurrencies: an inter-country configurational analysis. *Telematics and Informatics*, *102*, 102315. https://doi.org/10.1016/j.tele.2025.102315

Phansalkar, S., Mishra, D., Chaube, N., & Sonkamble, R. (2023). Towards adoption of green blockchain with emphasis on blockchain type, consensus protocols, data sharding and smart contracts. *2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, 1–8.

Prashanth, B., Kumar, M., Hoque, A., Muraqab, N.A., Moonesar, I.A., Braendle, U.C., & Rao, A. (2026). Prediction of bank transaction fraud using TabNet—an adaptive deep learning architecture. *International Review of Economics & Finance*, *106*, 104916. https://doi.org/10.1016/j.iref.2026.104916

Rajpal, S., & Manglani, A. (2026). Drivers of FinTech adoption: insights from a global review of recent literature. *Accounting Research Journal*, *39*(1), 84–103. https://doi.org/10.1108/ARJ-11-2024-0375

Ramayanti, R., Rachmawati, N.A., Setyawati, A., Azhar, Z., & Azman, N.H.N. (2026). A hybrid SEM--ANN approach to fintech lending adoption: Insights from Generation Z. *Social Sciences & Humanities Open*, *14*, 103591. https://doi.org/10.1016/j.ssaho.2026.103591

Sahoo, D. R., & Sahoo, V. D. (2026). Crypto derivatives markets: Price discovery, volatility dynamics, market efficiency, and DeFi risk: A structural analysis. *Journal of Engineering and Technology Management*, *80*, 774–799.

Sahoo, V. D., & Sahoo, D. R. (n.d.). Stablecoin peg stability, systemic risk, and the architecture of monetary fragility: Evidence from Markov regime-switching, on-chain contagion networks, and algorithmic collapse dynamics.

Samuel, E.G., Ruban, S., Parayitam, S., & Cristofaro, M. (2026). From ease of use to satisfaction: the roles of trust and risk in digital payment adoption. *Management Research Review*, *49*(13), 1–18. https://doi.org/10.1108/MRR-10-2025-0801

Sebai, L., & Bouzadi, B. (2025). FinTech and microfinance institutions: Regulatory perspectives, opportunities, and challenges in Tunisia and worldwide☆☆Funding: The authors disclosed receipt of a financial support for the research from the Ministry of Higher Education and Scientific Research of Tunisia as part of an excellence project under Grant Number P2ES2023-D2P1.. *Encyclopedia of Monetary Policy, Financial Markets and Banking (First Edition)*, 529–539. https://doi.org/10.1016/B978-0-44-313776-1.00343-3

Shah, M.A., & Raj, N. (2025). Examining the role of blockchain and public-private partnerships in design and deployment of blockchain-enabled CBDC. *Digital Business*, *5*(1), 100111. https://doi.org/10.1016/j.digbus.2025.100111

Shiau, W., Shih, C., Lin, C., Jiang, S., Dwivedi, Y.K., Yu, W., & Chen, K. (2025). Exploring Core Knowledge in Mobile Payment Research. *Journal of Organizational and End User Computing*, *37*(1). https://doi.org/10.4018/JOEUC.379684

Siraparapu, S.R., & Azad, S. (2024). Securing the IoT Landscape: A Comprehensive Review of Secure Systems in the Digital Era. *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, *10*, 100798. https://doi.org/10.1016/j.prime.2024.100798

Trotta, A., Gallucci, C., Rania, F., Strano, E., & Tipaldi, R. (2026). The "black box" of digital finance: An umbrella review of the challenges and drawbacks in advancing financial inclusion. *Research in International Business and Finance*, *81*, 103188. https://doi.org/10.1016/j.ribaf.2025.103188

Ullah, M.R., Chand, A., Liu, D., Khan, M.J., & Ahmed, M. (2026). Enhancing FinTech service acceptance: the role of quality attributes. *Digital Policy, Regulation and Governance*. https://doi.org/10.1108/DPRG-06-2025-0195

Wu, S., Xiao, W., Liang, K., & Li, K.W. (2025). A co-opetitive game analysis of platform compatibility strategies under data security regulation. *Transportation Research Part E: Logistics and Transportation Review*, *201*, 104228. https://doi.org/10.1016/j.tre.2025.104228

Xu, F., Kasperskaya, Y., & Sagarra, M. (2025). The impact of FinTech on bank performance: A systematic literature review. *Digital Business*, *5*(2), 100131. https://doi.org/10.1016/j.digbus.2025.100131

Zhang, P., Jayakar, K., Taylor, R., & Liu, C. (2025). Same goal, different paths: Contrasting approaches to AI regulation in China and India. *Telecommunications Policy*, *49*(8), 103019. https://doi.org/10.1016/j.telpol.2025.103019