Trust and cybersecurity in digital payment adoption: socioeconomic insights from India

Aya Aljaradat and Sandeep K. Shukla
Indian Institute of Technology Kanpur, Kanpur, India

Received 20 April 2025
Revised 19 May 2025
27 May 2025
14 June 2025
Accepted 14 June 2025

Abstract

Purpose – This study examines the behavioral and contextual determinants influencing digital payment trust and perceived cybersecurity (DPTS) in India, focusing on the roles of ease of use, perceived benefits, social influence and grievance redressal mechanisms. It further explores how DPTS, along with ease of use and perceived benefits, affects actual digital payment usage (DPU) and investigates how prior cybercrime experience (CE) moderates the relationship between DPTS and DPU.

Design/methodology/approach – Data were collected from 650 digital payment users across India's western, eastern and central regions. Structural equation modeling (SEM) was conducted using IBM SPSS and AMOS to test the proposed model. Multi-group analysis was employed to assess the moderating role of cybercrime experience by comparing users with and without prior exposure to cyber incidents.

Findings – Perceived benefits, ease of use, grievance redressal and social influence significantly enhance users' trust and cybersecurity perceptions, which in turn strongly predict digital payment systems adoption. Cybercrime experience significantly weakens the trust-usage link, indicating that digital trauma can override system strengths and suppress adoption behavior.

Social implications – These findings highlight the broader socioeconomic implications of digital trust, particularly its role in advancing financial inclusion, economic participation and digital literacy in emerging economies.

Originality/value – This research contributes theoretically by integrating cybercrime experience as a behavioral moderator in technology adoption models. It extends the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT) frameworks by introducing a dynamic trust perspective shaped by prior adverse experiences. The study advances understanding of digital payment behavior in high-risk environments and offers practical insights for developing trust-centric, resilient financial technologies.

Keywords Digitalization, Digital payments, Trust, Cybersecurity, Cybercrime, SEM, India

Paper type Research paper

1. Introduction

The adoption of digital payment systems (DPS) has significantly reshaped financial transactions in emerging economies, particularly in India. Fueled by proactive government initiatives, widespread smartphone usage, and expanding internet access, digital payments have emerged as a key enabler of financial inclusion and modernization. Platforms such as the Unified Payments Interface (UPI) and mobile wallets have revolutionized transactions by offering greater speed, accessibility, and convenience. As India advances toward becoming a digitally empowered society, the diffusion of DPS plays a central role in transforming consumer behavior and market operations.

Despite this progress, digital ecosystems remain vulnerable to both behavioral and technological frictions. Trust and cybersecurity perceptions are critical enablers of adoption, particularly in contexts characterized by technological volatility and uneven digital literacy

Journal of Business and Socio-economic Development
Vol. 5 No. 4, 2025
pp. 372-386
Emerald Publishing Limited
e-ISSN: 2635-1692
p-ISSN: 2635-1374
DOI 10.1108/JBSED-04-2025-0119

Funding: This research was supported by C3i Hub at IIT Kanpur.

(Kumar *et al.*, 2023). Theoretical frameworks such as the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT) emphasize constructs like perceived ease of use, perceived usefulness, and social influence in shaping technology adoption (Venkatesh *et al.*, 2003; Davis, 1989). Institutional factors, such as grievance redressal mechanisms, also play a vital role in trust-building, particularly within evolving regulatory environments (Kumar *et al.*, 2018).

However, these models often overlook the psychological and behavioral impacts of cybercrime. While trust and security perceptions are acknowledged drivers of DPS adoption, few studies have examined how prior exposure to cybercrime influences this relationship. This omission is especially significant in high-risk environments like India, where cybersecurity incidents surged from 6,168 in 2019 to over 429,000 in 2023 (PwC, 2024; CERT-In, 2024). Cybercriminals exploit system vulnerabilities and user inexperience through phishing, malware, SIM-swapping, and counterfeit apps (Aljaradat *et al.*, 2024). In light of this escalating threat landscape, a more nuanced understanding of behavioral responses to digital risk is needed.

This study addresses that gap by integrating cybercrime experience (CE) as a moderating variable within established technology adoption frameworks. Prior exposure to cybercrime may trigger fear, distrust, and heightened risk perception —concepts rooted in Risk Perception Theory (Slovic, 1987) and Protection Motivation Theory (Rogers, 1975). These emotional and cognitive reactions can inhibit rational decision-making, potentially leading users to disengage from DPS or revert to cash-based transactions (Apau and Koranteng, 2019; Verma *et al.*, 2023). As such, CE is not merely a contextual variable; it constitutes a behavioral inflection point that moderates how users assess the trustworthiness and security of digital financial platforms.

This research bridges a critical theoretical gap and situates India within a broader discourse on digital inclusion and cybersecurity resilience. Across the Global South—from Indonesia to Nigeria—low levels of digital trust, fragile grievance systems, and increasing cybercrime pose shared challenges (Cele and Kwenda, 2025). Understanding how cybercrime experience moderates trust-based decision-making offers transferable insights for policymakers and fintech innovators seeking to design safer, more inclusive financial infrastructures.

Accordingly, this study examines how perceived benefits, social influence, ease of use, and grievance redressal shape digital payment trust and cybersecurity (DPTS), and how DPTS — along with perceived benefits and ease of use — influences usage behavior. It further explores how cybercrime experience moderates the relationship between DPTS and user behavior. By grounding this inquiry within established models and extending them with behavioral insights, the study offers a novel and timely contribution to the digital finance literature.

2. Literature review and hypotheses development

The adoption of digital payment systems (DPS) has been extensively examined through established theoretical frameworks such as the Technology Acceptance Model (TAM) (Davis, 1989) and the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh *et al.*, 2003). These models identify key drivers—perceived usefulness, ease of use, social influence, and facilitating conditions—that influence users' intentions and behaviors. While these frameworks offer a solid foundation, emerging digital ecosystems, particularly in developing countries like India, call for more nuanced models that also account for institutional trust, cybersecurity concerns, and contextual risks. Given the growing scale and sophistication of cyber threats, digital payment adoption must be understood not only as a function of perceived utility and usability but also as a response to evolving security dynamics and post-incident behavior.

Recent studies have extended traditional adoption models by incorporating trust-related constructs such as perceived security, privacy assurance, and institutional credibility (Zhou, 2014; Rana *et al.*, 2019). In parallel, behavioral research increasingly highlights the role of past

negative experiences — particularly cybercrime incidents —in shaping user decision-making. Psychological theories, including Risk Perception Theory (Slovic, 1987) and Protection Motivation Theory (Rogers, 1975), suggest that individuals assess threats not solely based on technical knowledge but also through affective and cognitive responses. These insights are particularly valuable in explaining why trust and cybersecurity perceptions do not always translate into consistent usage behavior, especially among users who have experienced financial fraud or identity theft. Accordingly, this section reviews relevant literature underpinning the conceptual framework and formulates hypotheses that reflect both established theoretical constructs and the evolving realities of digital ecosystems.

Among the most influential factors shaping trust and security perceptions in digital payment systems are perceived benefits. These include convenience, transaction speed, ease of access, and financial incentives such as cashback or discounts (Gefen *et al.*, 2003). When users perceive high functional and economic value, they are more likely to view the platform as secure and trustworthy. This relationship is especially critical in contexts with limited financial literacy, where tangible benefits may serve as cognitive proxies for abstract technical concepts such as encryption or multi-factor authentication (Chawla and Joshi, 2019).

In developing economies such as India, perceived benefits play a key role in bridging gaps in both digital literacy and institutional trust. Kumar *et al*. (2018) found that users are more inclined to engage with platforms they perceive as rewarding or capable of simplifying financial transactions. Perceived benefits thus signal a service provider's commitment to quality and security, thereby reinforcing user confidence in the platform's reliability and integrity. Based on the reviewed literature, the following hypothesis is proposed:

H1. Perceived benefits positively influence digital payment trust and cybersecurity.

Perceived benefits also have a direct influence on behavioral usage, serving as motivational cues that drive engagement with digital payment systems. According to TAM, perceived usefulness is a strong predictor of technology adoption (Davis, 1989). In the digital finance context, studies by Shankar and Datta (2018) and Kumar *et al*. (2018) found that financial incentives, transaction speed, and ease of access are primary motivators behind users' shift from cash to digital payment methods.

Supporting this, Liébana-Cabanillas *et al*. (2017) demonstrated that in mobile commerce contexts, both perceived functional and emotional benefits significantly predict adoption and continued use. These findings align with prospect theory, which posits that individuals evaluate alternatives based on perceived gains rather than objective probabilities. In the Indian context, such perceived benefits have been instrumental in scaling digital payment adoption, particularly among users with limited prior experience in formal banking systems. Therefore, the second hypothesis is proposed:

H2. Perceived benefits positively influence digital payment usage.

Ease of use is a cornerstone of both TAM and UTAUT models and is particularly influential in digital payment systems, where user experience shapes perceptions of competence and safety. Systems perceived as simple to use are often trusted more because they reduce the cognitive burden on users and minimize the chances of error (Zhou, 2014). This association has been verified in the Indian context, where Kanojia and Lal (2020) observed that ease of navigation significantly enhanced trust in digital payment platforms.

Internationally, Almaiah *et al*. (2022) confirmed that in Saudi Arabia, perceived ease of use plays a significant role in building trust in NFC-based mobile payment systems. Similarly, Martins *et al*. (2014) emphasized that in Internet banking, ease of use fosters trust by making system interactions more transparent and manageable. The evidence supports that intuitive interface design and user-centric architecture are vital trust-enabling features. Drawing from these insights, the third hypothesis is suggested:

H3. Ease of use positively influences digital payment trust and cybersecurity.

Ease of use also has a direct effect on digital payment system adoption. Venkatesh *et al*. (2003) argue that technologies that minimize learning effort and operational complexity are more likely to be adopted. This is particularly relevant in India, where digital literacy levels vary widely across regions. In such contexts, intuitive mobile wallets and banking apps have enabled first-time users to embrace digital platforms with minimal guidance (Sivathanu, 2019).

Supporting this, Luarn and Lin (2005) found that perceived ease of use significantly influences the intention to adopt mobile banking services in Taiwan. In India, Chawla and Joshi (2019) demonstrated that user-friendliness is a primary factor influencing both initial adoption and continued use of mobile wallets. Thus, usability emerges as a key enabler of mass adoption in developing digital ecosystems. In light of the above, the fourth hypothesis is proposed:

H4. Ease of use positively influences digital payment usage.

Social influence, as conceptualized in the UTAUT model, denotes the impact of societal and peer approval on an individual's behavioral intentions. This influence is particularly salient in collectivist societies or among users with limited personal experience or digital literacy. Recommendations from peers serve as powerful behavioral validators that increase trust in unfamiliar technologies (Kim *et al.*, 2009; Gupta and Arora, 2017).

In India, several studies have confirmed this trend. Lakhaiyar and Mani (2022) and Hasan *et al*. (2024) observed that social influence significantly shapes trust and behavioral intentions during COVID-19-induced digital acceleration. Manrai *et al*. (2021) found that in semi-urban areas, digital payment adoption often follows the behavior of influential peers. As social proof substitutes for institutional trust, it helps reduce perceived risk and fosters a favorable environment for digital payment engagement. Given the supporting evidence, the fifth hypothesis is advanced:

H5. Social influence positively influences digital payment trust and cybersecurity.

Grievance redressal mechanisms provide users with structured pathways to resolve issues, thereby reinforcing system transparency and institutional accountability. Trust in digital systems is significantly enhanced when users feel assured that their complaints will be handled fairly and efficiently (Liu *et al.*, 2005; Pavlou, 2003). This is particularly important in emerging markets, where legal and regulatory enforcement may be inconsistent.

In India, institutional innovations such as the Reserve Bank of India (RBI)'s Online Dispute Resolution (ODR) framework and the complaint modules integrated within Unified Payments Interface (UPI) platforms exemplify how grievance redressal can enhance trust (Reserve Bank of India, 2020). Kumar *et al*. (2018) found that users' perceptions of effective grievance handling positively influence their continued intention to use mobile wallets. Transparent redressal processes reduce uncertainty, strengthen user confidence, and encourage digital loyalty. Based on these insights, the sixth hypothesis is proposed as follows:

H6. Grievance redressal positively influences digital payment trust and cybersecurity.

Trust and perceived cybersecurity form the foundation of digital payment usage. Users are unlikely to adopt or consistently use digital platforms if they doubt the safety of their financial data or transactions (Rana *et al.*, 2019). In contrast, users who trust the platform's security features are more likely to engage with it actively. Secure authentication protocols, encryption, and fraud protection are perceived as strong motivators of user confidence (Gupta and Hakhu, 2021).

This pattern has also been observed internationally. Krishna *et al*. (2023) emphasized the role of visible cybersecurity policies and national-level commitments in shaping trust. Similarly, Sharma *et al*. (2024) noted that transparent risk communication and fraud prevention mechanisms significantly impact digital payment adoption in India. These findings reinforce the importance of combining technical defenses with user-centered trust-building

practices. Based on the theoretical reasoning and empirical findings, the seventh hypothesis is proposed as follows:

H7. Trust and perceived cybersecurity positively influence digital payment usage.

Cybercrime experience introduces a powerful contextual variable that can alter users' psychological and behavioral responses to digital platforms. Exposure to fraud, phishing, or identity theft increases user sensitivity to risk, leading to heightened skepticism and reduced engagement. Risk Perception Theory (Slovic, 1987) and Protection Motivation Theory (Rogers, 1975) provide theoretical frameworks to explain these behaviors, suggesting that perceived vulnerability and fear inhibit continued usage even when the system is objectively secure.

Apau and Koranteng (2019) and Gomes *et al*. (2022) found that individuals exposed to cybercrime perceived digital platforms as inherently less trustworthy. In the Indian context, Jadhav (2024) reported that recurring fraud reports have eroded public trust in otherwise reliable payment systems. This mirrors findings from other regions: Riek *et al*. (2015) observed that prior cybercrime victims in Europe are less likely to use online services again, while Lestari *et al*. (2024) found similar trends in Southeast Asia, where distrust lingers long after security measures are enhanced.

Such users may require targeted interventions, awareness campaigns, support mechanisms, and personalized reassurance to overcome their trauma and re-engage with digital systems. Thus, cybercrime experience significantly moderates the strength of the trust–usage relationship, with potentially long-lasting behavioral consequences. Accordingly, the eighth hypothesis is presented as follows:

H8. Cybercrime experience negatively moderates the relationship between DPTS and DPU.

Figure 1 outlines the proposed research framework based on the constructs and relationships established in the preceding sections. It integrates traditional variables—Digital Payment Perceived Benefits (DPPB), Ease of Use (DPEU), Grievance Redressal (DPGR), Social Influence (DPSI), and Trust and Cybersecurity (DPTS)—with the moderating influence of Cybercrime Experience (CE) on Digital Payment Usage (DPU). Grounded in TAM, UTAUT,

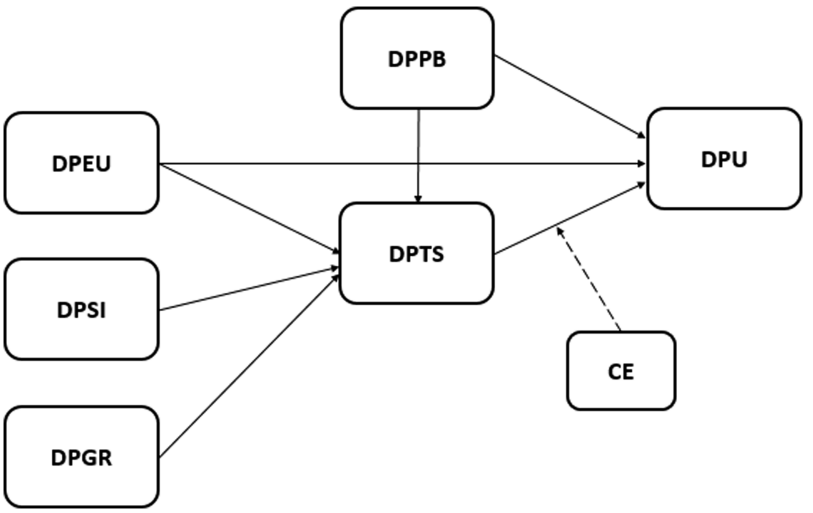

Figure 1. The proposed model. Source: The authors

Risk Perception Theory, and Protection Motivation Theory, the model provides a robust structure for understanding digital payment adoption in environments with varying degrees of trust, cybercrime exposure, and risk.

3. Methodology

3.1 Questionnaire design

This study employed a structured and theory-driven questionnaire to collect primary data. The instrument design was developed based on an extensive review of the digital payment adoption literature, incorporating constructs from TAM and UTAUT. The questionnaire consisted of four main sections: user context, digital payment usage constructs, cybercrime experience, and demographic and socioeconomic information.

The first section collected contextual information, including the number of bank accounts held, access to credit/debit cards, and the frequency of using various digital payment methods (e.g. UPI, mobile banking, e-wallets). The second section captured digital payment system usage behaviors through 21 items spanning six constructs: Digital Payment Perceived Benefits (DPPB), Ease of Use (DPEU), Grievance Redressal (DPGR), Social Influence (DPSI), Trust and Cybersecurity (DPTS), and Digital Payment Usage (DPU). Each construct was measured using three to five reflective indicators, adapted from prior studies (e.g. Bhattacherjee, 2012; Venkatesh *et al.*, 2003; Kumar *et al.*, 2018), rated on a 5-point Likert scale ranging from "Strongly Disagree" (1) to "Strongly Agree" (5). Details are provided in Appendix A.

The third section measured cybercrime experience (CE) using a structured and standardized approach, based on cyber fraud classifications outlined by the Indian Computer Emergency Response Team (CERT-In, 2022) and the Reserve Bank of India (Reserve Bank of India, 2016). Respondents were presented with ten scenario-based items reflecting common digital payment-related cybercrimes in India. These included phishing, vishing (OTP fraud), spoofing/pharming, QR code scams, credit card skimming, investment fraud, fake advertisements, remote access fraud, loan app extortion, and matrimonial/custom fraud. Each scenario was described in user-friendly terms, and respondents indicated whether they or any household member had experienced a similar incident in the past year (Yes/No). A binary CE variable was then constructed (1 = experienced at least one type; 0 = none), which was subsequently used in a multi-group analysis to explore the moderating effect of cybercrime experience on the relationship between DPTS and DPU. This approach aligns with Hair *et al.*'s (2010) recommendations on the validity of dichotomous moderators in structural models. A detailed mapping of cybercrime scenarios to fraud types is provided in Appendix B.

The final section captured demographic and socioeconomic data (e.g. age, education, employment, income) to account for background heterogeneity and sample diversity. To ensure instrument validity and reliability, a multi-stage pretesting process was undertaken, in line with best practices for survey-based research (Hair *et al.*, 2010; Weerakkody *et al.*, 2017). Initial feedback was obtained from domain experts at the Indian Institute of Technology Kanpur (IITK). A pilot version was then distributed online to 150 individuals to assess clarity, relevance, and wording; these responses were excluded from the final dataset. The questionnaire was subsequently translated into Hindi to enhance inclusivity and was administered in both English and Hindi. A formal pilot study involving 50 participants was conducted at IITK to test internal consistency, leading to minor refinements before full-scale deployment.

3.2 Data collection

To mitigate common limitations associated with online surveys —such as low response rates, self-selection bias, and limited control over respondent authenticity (Evans and Mathur, 2005) — this study employed a face-to-face survey approach. This method enhanced data reliability, improved response quality, and provided greater control over sampling conditions

(Bhattacherjee, 2012). Data collection was conducted over seven months, spanning from September 2023 to March 2024, targeting respondents from three major geographical zones in India: the western, eastern, and central regions. Specifically, the sample comprised 150 respondents from Madhya Pradesh, 50 each from Bihar, Chhattisgarh, and Jharkhand, 100 from West Bengal, 150 from Maharashtra, and 100 from Gujarat, resulting in a total of 650 completed responses.

The research model included 21 observed indicators across multiple constructs. The sample of 650 respondents substantially exceeds the minimum requirement suggested by the "thumb rule" for quantitative research and Structural Equation Modeling (SEM) (Hair *et al*., 2010). Moreover, the results showed that no single factor accounted for the majority of the variance, indicating that common method bias (CMB) was not a significant concern in this study (Podsakoff *et al*., 2003).

3.3 Data preparation

Prior to statistical analysis, the dataset underwent a comprehensive screening process to ensure its accuracy and reliability. This process included the identification and removal of incomplete responses, logical inconsistencies, and statistical outliers. Questionnaires with substantial sections left unanswered or containing uniformly neutral responses across all items were excluded, following best practices for handling survey-based data (Hair *et al*., 2010). Additionally, responses exhibiting straight-lining patterns or internal contradictions were flagged as unreliable and removed to enhance data consistency.

Eliminating such anomalies helped mitigate potential sources of bias and ensured that the data used for analysis accurately reflected the target population. Following the data screening process, 550 valid and complete responses remained, comprising the final sample for empirical analysis. This preprocessing step was essential for enhancing the reliability of the study's results while minimizing the risk of bias introduced by data errors or non-representative responses (Kline, 2016).

3.4 Data analysis strategy

This study employed SEM as the primary analytical technique to evaluate the proposed research model. SEM is a powerful multivariate statistical method that facilitates the analysis of complex relationships between observed and latent variables. By integrating factor analysis and multiple regression within a cohesive framework, SEM allows for the simultaneous assessment of both measurement and structural components, thereby offering comprehensive insights into construct validity and the strength of inter-variable associations (Kline, 2016).

SEM is particularly beneficial in disciplines such as marketing, social sciences, and digital technology adoption, where research models frequently involve mediating variables and latent constructs (Iacobucci, 2009). Its ability to account for measurement error and validate the theoretical foundations of constructs enhances both the precision and credibility of empirical findings (Gefen *et al*., 2000).

To perform the SEM analysis, IBM SPSS AMOS version 29 was used due to its intuitive graphical interface and robust capabilities for handling complex models. AMOS facilitated the estimation of latent variables, incorporated measurement error, and generated a comprehensive array of goodness-of-fit indices, all of which contributed to assessing the adequacy and validity of the proposed model (Blunch, 2012).

4. Results

4.1 Descriptive findings

The analysis was conducted using data from 550 completed and valid survey responses, which provided demographic and behavioral insights relevant to digital payment adoption. The majority of respondents belonged to the Millennial age group (25–40 years),

accounting for 61.09% of the sample, followed by Gen X (41–56 years) at 19.09%, and Gen Z (≤24 years) at 18%. Representation from Baby Boomers (57–75 years) was minimal (1.82%). This age distribution suggests that digital payment adoption is most prevalent among younger and middle-aged adults. The sample was predominantly well-educated, with most respondents holding a bachelor's degree (48.73%) or a master's degree (16.36%).

Respondents were also asked about their use of various digital payment services in the past month. The most commonly used platform was mobile payment apps (e.g. UPI, mobile banking), reported by 43.5% of participants. This was followed by banking card usage (26.1%), internet banking (21.7%), and e-wallets (e.g. Paytm and PhonePe) at 8.7%. These findings indicate a strong preference for mobile-based digital payment options over more traditional methods. In terms of experience, approximately half of the participants had been using digital payment systems for between 2.5 and 6.5 years, which highlights a strong adoption trend. Participants also reported the proportion of their digital transactions completed during the seven days before the survey. Approximately 33.6% of respondents indicated that 51%–75% of their transactions were conducted via digital payments, while 26.3% reported digital usage levels of 76%–100%. Conversely, 25.6% reported moderate use (26%–50%), and only 14.5% reported low usage (less than 25%). These results suggest a significant shift toward digital payments among the majority of users.

To assess digital awareness, participants were asked about their familiarity with institutional support (bank training), law enforcement presence (cybercrime police), and national initiatives (RBI campaigns). Results showed that over 54% of participants demonstrated a high level of awareness by answering two out of three questions affirmatively, while only 5.45% reported complete unawareness. This distribution suggests a moderately informed population, with room for targeted awareness campaigns.

4.2 The measurement model results

Confirmatory factor analysis (CFA) was employed to assess the measurement model, focusing on the reliability and construct validity of the latent variables. The analysis examined convergent validity, discriminant validity, and overall model fit in line with established structural equation modeling criteria (Hair *et al.*, 2019).

Convergent validity was assessed using standardized factor loadings (FL), composite reliability (CR), and average variance extracted (AVE). As shown in Table 1, all factor loadings surpassed the minimum threshold of 0.50, ranging from 0.607 to 0.960, indicating strong indicator reliability. CR values for all constructs surpassed the recommended benchmark of 0.70, and AVE values were above 0.50 (Fornell and Larcker, 1981), confirming that the items adequately represent their respective latent constructs.

Discriminant validity was examined using the Fornell-Larcker criterion. As presented in Table 2, the square roots of AVE (diagonal elements) for each construct were greater than the corresponding inter-construct correlations, supporting discriminant validity. Additionally, for each construct, both the average shared variance (ASV) and maximum shared variance (MSV) were lower than their respective AVE values. For example, the DPU construct had an AVE of 0.669, an MSV of 0.632, and an ASV of 0.325, demonstrating stronger internal consistency than external overlap.

The overall model fit was evaluated using standard SEM fit indices. The model exhibited a satisfactory fit with the data, as indicated by the following results: the chi-square divided by degrees of freedom (CMIN/DF) was 2.556 (<3.0), the adjusted goodness-of-fit index (AGFI) was 0.909 (>0.80), the comparative fit index (CFI) was 0.966 (>0.90), the parsimony normed fit index (PNFI) was 0.757 (>0.50), and the root mean square error of approximation (RMSEA) was 0.053 (≤0.06) (Hu and Bentler, 1999). These values confirm that the measurement model appropriately represents the underlying theoretical structure and provides a robust foundation for further structural analysis.

Table 1. Convergent validity results

Factor	FL > 0.5	CR > 0.70	AVE>0.5
DPU		0.858	0.669
DPU1	0.808		
DPU2	0.813		
DPU3	0.832		
DPEU		0.859	0.605
DPEU1	0.733		
DPEU2	0.769		
DPEU3	0.863		
DPEU4	0.738		
DPSI		0.798	0.570
DPSI1	0.825		
DPSI2	0.732		
DPSI3	0.703		
DPTS		0.901	0.653
DPTS1	0.941		
DPTS2	0.960		
DPTS3	0.684		
DPTS4	0.607		
DPTS5	0.788		
DPGR		0.879	0.710
DPGR1	0.820		
DPGR2	0.934		
DPGR3	0.765		
DPPB		0.847	0.649
DPPB1	0.769		
DPPB2	0.804		
DPPB3	0.843		

Note(s): Factor Loading (FL), Composite Reliability (CR), and Average Variance Extracted (AVE)
Source(s): Created by authors

Table 2. Discriminant validity: Fornell-Larcker criterion

	CR	AVE	MSV	ASV	DPTS	DPEU	DPSI	DPGR	DPU	DPPB
DPTS	0.901	0.653	0.228	0.128	*0.808*					
DPEU	0.859	0.605	0.415	0.223	0.477	*0.778*				
DPSI	0.798	0.570	0.416	0.204	0.201	0.382	*0.755*			
DPGR	0.879	0.710	0.077	0.034	0.250	0.278	0.065	*0.843*		
DPU	0.858	0.669	0.632	0.325	0.396	0.644	0.645	0.059	*0.818*	
DPPB	0.847	0.649	0.632	0.294	0.388	0.502	0.643	0.145	0.795	*0.806*

Source(s): Created by authors

4.3 The structural model results (hypothesis test)

The structural model was evaluated to test the proposed hypotheses and assess the relationships among key constructs. Model fit indices indicated satisfactory alignment with the data: CMIN/DF = 2.584 (<3), AGFI = 0.908, CFI = 0.956 (both surpassing their respective benchmarks of 0.80 and 0.90, respectively), PNFI = 0.752, and RMSEA = 0.054. These values confirm the model's adequacy in representing the observed data.

Hypothesis testing results demonstrated significant relationships among the key constructs, as summarized in Table 3. DPPB had a positive and significant influence on DPTS (β = 0.308), supporting H1. Additionally, DPEU (β = 0.347), DPSI (β = 0.154), and DPGR

Table 3. Hypothesis test results

Hypothesis	Independent construct	Dependent construct	R^2	β	*p*-value	Support?
H1	DPPB	DPTS	0.53	0.308	***	Yes
H3	DPEU			0.347	***	Yes
H5	DPSI			0.154	*	Yes
H6	DPGR			0.254	**	Yes
H7	DPTS	DPU	0.77	0.432	***	Yes
H4	DPEU			0.314	***	Yes
H2	DPPB			0.667	***	Yes

Note(s): ***$p < 0.001$, *$p < 0.05$, **$p < 0.01$
Source(s): Created by authors

(β = 0.254) were all significant predictors of DPTS, jointly explaining 53% of its variance ($R^2 = 0.53$).

Regarding the usage of digital payments (DPU), DPTS significantly predicted DPU (β = 0.432), corroborating H7. Furthermore, DPEU (β = 0.314; H4) and DPPB (β = 0.667; H2) also positively impacted DPU. The model accounted for 77% of the variance in DPU ($R^2 = 0.77$), demonstrating strong predictive power. All seven hypothesized paths were statistically supported, confirming the theoretical framework and highlighting the roles of perceived benefits, ease of use, social influence, trust, cybersecurity, and grievance redressal in promoting digital payment adoption.

Despite explaining a substantial proportion of variance in DPU ($R^2 = 0.77$), the model remains parsimonious, incorporating only six constructs and one moderator, each theoretically grounded. Multicollinearity diagnostics revealed no serious issues as all variance inflation factor (VIF) values were below the commonly accepted threshold of 5, with a maximum of 2.94. These results indicate that the explanatory power of the model is not achieved at the expense of overfitting or redundancy and that the structural estimates are statistically robust and interpretable.

To further explore contextual influences, a multi-group analysis (MGA) was conducted using AMOS to assess the moderating effect of cybercrime experience (CE). The dataset was divided into two groups: users with cybercrime experience (CE = 1) and those without it (CE = 0). An unconstrained model was first estimated, allowing path coefficients to differ across groups, followed by a constrained model in which the path from DPTS to DPU was fixed across both groups. A chi-square difference test ($\Delta\chi^2 = 4.21$, $\Delta df = 1$, $p < 0.05$) indicated a statistically significant difference between models, confirming a moderating effect. Specifically, the relationship between DPTS and DPU was stronger for individuals without cybercrime experience (β = 0.41, $p < 0.001$) than those with such experience (β = 0.23, $p < 0.05$). This suggests that users who have previously encountered cybercrime may place less emphasis on trust and cybersecurity perceptions when deciding whether to use digital payment systems.

To better understand the practical implications of the structural model, the relative strength of each significant predictor of digital payment usage (DPU) was examined. Notably, perceived benefits (DPPB) emerged as the strongest predictor (β = 0.667, $p < 0.001$), indicating that functional and economic advantages are critical drivers of adoption. This was followed by trust and cybersecurity (DPTS) (β = 0.432, $p < 0.001$) and ease of use (DPEU) (β = 0.314, $p < 0.001$), both of which had significant but comparatively weaker effects. These findings suggest that while trust and usability are essential, users are primarily motivated by tangible, value-oriented benefits. This underscores the need for digital payment providers to enhance not only system security and user confidence but also to offer compelling, value-driven incentives that support sustained adoption.

5. Discussion and implications

This study offers empirical insights into digital payment adoption behavior in India, highlighting how trust and perceived cybersecurity are shaped by ease of use, perceived benefits, social influence, and grievance redressal. These findings reaffirm the relevance of the TAM and UTAUT frameworks, underscoring that user-centric design and institutional support are critical for fostering digital trust (Venkatesh *et al.*, 2003; Davis, 1989; Sivathanu, 2019). Notably, the proposed model explains 77% of the variance in usage, emphasizing that trust and perceived utility are dominant predictors of adoption (Gupta and Hakhu, 2021). The significant roles of grievance redressal and social influence suggest that institutional responsiveness and peer endorsement enhance perceived credibility (Kumar *et al.*, 2018; Singh *et al.*, 2020). These insights have far-reaching implications for promoting financial inclusion and digital participation, especially among populations vulnerable to exclusion due to perceived or experienced risk.

The moderating role of cybercrime experience (CE) reveals that users with prior digital trauma exhibit weaker trust-usage relationships, even when system attributes are favorable. This supports findings by Riek *et al*. (2015) and Lestari *et al*. (2024), emphasizing that the emotional and psychological consequences of cybercrime —such as fear, distrust, and avoidance— deter engagement with digital financial platforms. The results suggest that policy and design interventions must go beyond enhancing technical security to address emotional recovery and user reassurance.

These findings challenge static assumptions embedded in traditional adoption models. While TAM and UTAUT posit rational decision-making based on perceived utility and ease, the influence of CE suggests that trust is dynamic and shaped by emotional memory and perceived risk. Hence, future models should integrate behavioral economics and psychological constructs like risk aversion and loss sensitivity to more accurately capture real-world adoption behavior. A dual imperative emerges: while secure system design remains foundational, it must be complemented by inclusive, trust-rebuilding communication strategies, particularly for users previously affected by cybercrime. This is particularly critical in emerging economies, where socioeconomic disparities and digital literacy gaps make trust more fragile.

5.1 Theoretical implications

This study extends behavioral technology adoption frameworks—specifically TAM and UTAUT—by introducing cybercrime experience (CE) as a moderating factor. Traditional models often assume stable, rational user behavior; however, our findings suggest that trust is a dynamic construct, shaped by past digital trauma, emotional responses, and perceived risk. This challenges the assumption of purely rational evaluation and aligns with Risk Perception Theory and Protection Motivation Theory.

Incorporating CE enhances the contextual sensitivity of adoption models, offering a more realistic portrayal of digital behavior in risk-prone environments. Future research could further benefit from integrating concepts from behavioral economics (e.g. loss aversion, perceived vulnerability) or dual-process theories to capture both rational and experiential pathways in technology adoption. Additionally, the proposed framework presented can be tested across countries and sectors to evaluate its generalizability in varied cultural, regulatory, and digital maturity contexts.

5.2 Practical and socio-economic implications

The findings yield several actionable recommendations for fintech developers, digital payment providers, and policymakers. First, post-cybercrime trust recovery should be central to digital payment strategies. Institutions must implement transparent remediation protocols including follow-up communication, compensation, and user support, to restore confidence.

Second, interventions should be demographically and culturally tailored. Younger users may benefit from gamified awareness tools and intuitive interfaces, while older or less digitally literate populations may require community-based education and in-person outreach. Such differentiation is essential for promoting inclusive digital finance, especially among underserved populations. Third, user-centric design is crucial for building trust. Features such as simple navigation, visible security cues, and real-time alerts can reduce anxiety and enhance perceived system credibility.

Finally, the results call for experience-sensitive policy frameworks. Regulatory bodies should complement preventive strategies with responsive mechanisms that recognize trust as experience-dependent, particularly in regions where cybersecurity concerns limit financial inclusion. As previously discussed, the socio-economic value of digital payments lies in their capacity to foster broader participation in the formal economy, especially among marginalized communities.

6. Conclusion

This study offers critical insights into the behavioral and psychological factors influencing digital payment adoption in emerging economies, with India as a focal case. Grounded in the TAM and the UTAUT and enriched by Risk Perception and Protection Motivation theories, the study highlights how traditional adoption drivers, such as perceived benefits, ease of use, grievance redressal, and social influence, converge to foster trust and perceived cybersecurity, which are essential precursors to usage behavior. These results reaffirm the importance of user experience, system transparency, and institutional credibility in digital financial ecosystems.

A notable contribution is the integration of cybercrime experience as a moderating factor, revealing that trust is dynamic and shaped by prior exposure to digital threats. Users with a history of cybercrime exhibit a weakened trust-usage relationship, challenging static assumptions in conventional adoption models and highlighting the need to incorporate emotional and risk-related dimensions into digital behavior frameworks.

From a practical standpoint, the study offers actionable guidance for fintech developers, financial institutions, and policymakers. It underscores the importance of trust-recovery strategies, such as post-incident communication, transparent grievance handling, and demographic-specific education programs, to rebuild confidence among cybercrime-affected users. Additionally, intuitive app design and visible security features are shown to mitigate perceived risks and promote sustained engagement.

Finally, the proposed model lays a foundation for future research across diverse regulatory and socio-cultural environments. Its applicability to sectors such as healthcare, education, and public utilities, as well as to other emerging markets with similar cyber risk profiles, can enhance the generalizability and policy relevance of digital trust frameworks.

References

Aljaradat, A., Sarkar, G. and Shukla, S.K. (2024), "Modelling cybersecurity impacts on digital payment adoption: a game theoretic approach", *Journal of Economic Criminology*, Vol. 5, 100089, doi: 10.1016/j.jeconc.2024.100089.

Almaiah, M.A., Al-Khasawneh, A., Althunibat, A., Al-Khasawneh, M., Lutfi, A., Alrawad, M., Alkhalaf, S., Al-Rahmi, W.M., Al-sharaieh, S. and Aldhyani, T.H.H. (2022), "Exploring the acceptance of mobile payment system using NFC technology in Saudi Arabia: a modified TAM approach", *Electronics*, Vol. 11 No. 23, p. 3926, doi: 10.3390/electronics11233926.

Apau, R. and Koranteng, F.N. (2019), "Impact of cybercrime and trust on the use of e-commerce technologies: an application of the theory of planned behavior", *International Journal of Cyber Criminology*, Vol. 13 No. 2, pp. 228-254, doi: 10.5281/zenodo.3697886.

Bhattacherjee, A. (2012), *Social Science Research: Principles, Methods and Practices*, University of South Florida, Tampa, FL.

Blunch, N.J. (2012), *Introduction to Structural Equation Modelling Using IBM SPSS Statistics and AMOS*, Sage, London.

Cele, N.N. and Kwenda, S. (2025), "Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review", *Journal of Financial Crime*, Vol. 32 No. 1, pp. 31-48, doi: 10.1108/JFC-10-2023-0263.

Chawla, D. and Joshi, H. (2019), "Consumer attitude and intention to adopt mobile wallet in India – an empirical study", *International Journal of Bank Marketing*, Vol. 37 No. 7, pp. 1590-1618, doi: 10.1108/IJBM-09-2018-0256.

Davis, F.D. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS Quarterly*, Vol. 13 No. 3, pp. 319-340, doi: 10.2307/249008.

Evans, J.R. and Mathur, A. (2005), "The value of online surveys", *Internet Research*, Vol. 15 No. 2, pp. 195-219, doi: 10.1108/10662240510590360.

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39-50, doi: 10.1177/002224378101800104.

Gefen, D., Straub, D. and Boudreau, M.C. (2000), "Structural equation modeling and regression: guidelines for research practice", *Communications of the Association for Information Systems*, Vol. 4, doi: 10.17705/1cais.00407.

Gefen, D., Karahanna, E. and Straub, D.W. (2003), "Trust and TAM in online shopping: an integrated model", *MIS Quarterly*, Vol. 27 No. 1, pp. 51-90, doi: 10.2307/30036519.

Gomes, L., Deshmukh, A. and Anute, N. (2022), "Cyber security and internet banking: issues and preventive measures", *Journal of Information Technology and Sciences*, Vol. 8 No. 2, pp. 31-42, doi: 10.46610/JOITS.2022.v08i02.005.

Gupta, A. and Arora, N. (2017), "Consumer adoption of m-banking: a behavioral reasoning theory perspective", *International Journal of Bank Marketing*, Vol. 35 No. 4, pp. 733-747, doi: 10.1108/IJBM-11-2016-0162.

Gupta, P. and Hakhu, R. (2021), "Impact of perceived security and perceived trust on intention to use digital payments – a study on Indian customers", *Webology*, Vol. 18 No. 6, pp. 169-181.

Hair, J., Anderson, R., Babin, B. and Black, W. (2010), *Multivariate Data Analysis: A Global Perspective*, Pearson Education, Upper Saddle River, NJ.

Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (2019), *Multivariate Data Analysis*, Cengage, Hampshire.

Hasan, A., Sikarwar, P., Mishra, A., Raghuwanshi, S., Singhal, A., Joshi, A., Singh, P.R. and Dixit, A. (2024), "Determinants of behavioral intention to use digital payment among indian youngsters", *Journal of Risk and Financial Management*, Vol. 17 No. 2, p. 87, doi: 10.3390/jrfm17020087.

Hu, L.T. and Bentler, P.M. (1999), "Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives", *Structural Equation Modeling: A Multidisciplinary Journal*, Vol. 6 No. 1, pp. 1-55, doi: 10.1080/10705519909540118.

Iacobucci, D. (2009), "Structural equations modeling: fit indices, sample size, and advanced topics", *Journal of Consumer Psychology*, Vol. 20 No. 1, pp. 90-98, doi: 10.1016/j.jcps.2009.09.003.

Indian Computer Emergency Response Team (CERT-In) (2022), *'Open, Safe and Trusted and Accountable Internet', Ministry of Electronics and Information Technology*, Government of India, available at: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf (accessed 11 May 2025).

Indian Computer Emergency Response Team (CERT-In) (2024), "Annual Report 2023", available at: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT (accessed 9 April 2025).

Jadhav, Y.M. (2024), "Analyzing efficacy and enhancing accessibility: a study of India's national cybercrime reporting portal in addressing financial cybercrimes", *International Journal of Scientific Research in Engineering and Management (IJSREM)*, Vol. 8 No. 3, pp. 1-5, doi: 10.55041/IJSREM29563.

Kanojia, R. and Lal, M. (2020), "Impact of trust on customer adoption of digital payment systems: a study of selected districts of Madhya Pradesh", *International Journal of Recent Technology and Engineering*, Vol. 8 No. 5, pp. 16-42, doi: 10.4018/978-1-7998-2398-8.ch002.

Kim, D.J., Ferrin, D.L. and Rao, H.R. (2009), "Trust and satisfaction, two stepping stones for successful e-commerce relationships: a longitudinal exploration", *Information Systems Research*, Vol. 20 No. 2, pp. 237-257, doi: 10.1287/isre.1080.0188.

Kline, R.B. (2016), *Principles and Practice of Structural Equation Modeling*, Guilford Press, New York, NY.

Krishna, B., Krishnan, S. and Sebastian, M. (2023), "Understanding the process of building institutional trust among digital payment users through national cybersecurity commitment trustworthiness cues: a critical realist perspective", *Information Technology and People*, Vol. 38 No. 2, pp. 714-756, doi: 10.1108/ITP-05-2023-0434.

Kumar, A., Adlakaha, A. and Mukherjee, K. (2018), "The effect of perceived security and grievance redressal on continuance intention to use m-wallets in a developing country", *International Journal of Bank Marketing*, Vol. 36 No. 7, pp. 1170-1189, doi: 10.1108/IJBM-04-2017-0077.

Kumar, R., Singh, R., Kumar, K., Khan, S. and Corvello, V. (2023), "How does perceived risk and trust affect mobile banking adoption? Empirical evidence from India", *Sustainability*, Vol. 15 No. 5, p. 4053, doi: 10.3390/su15054053.

Lakhaiyar, S. and Mani, M. (2022), "Factors influencing adoption of digital payment systems during COVID-19", *International Journal of Sociotechnology and Knowledge Development*, Vol. 14 No. 1, pp. 1-21, doi: 10.4018/IJSKD.315292.

Lestari, S., Adawiyah, W.R., Alhamidi, A.L., Prayogi, J. and Haryanto, R. (2024), "Navigating perilous seas: unmasking online banking frauds, perceived usefulness, fear of cybercrime and distrust in online banking", *Safer Communities*, Vol. 23 No. 4, pp. 444-464, doi: 10.1108/SC-04-2024-0018.

Liébana-Cabanillas, F., Marinković, V. and Kalinić, Z. (2017), "A SEM-neural network approach for predicting antecedents of m-commerce acceptance", *International Journal of Information Management*, Vol. 37 No. 2, pp. 14-24, doi: 10.1016/j.ijinfomgt.2016.10.008.

Liu, C., Marchewka, J.T., Lu, J. and Yu, C.-S. (2005), "Beyond concern-a privacy–trust–behavioral intention model of electronic commerce", *Information and Management*, Vol. 42 No. 2, pp. 289-304, doi: 10.1016/j.im.2004.01.003.

Luarn, P. and Lin, H.H. (2005), "Toward an understanding of the behavioral intention to use mobile banking", *Computers in Human Behavior*, Vol. 21 No. 6, pp. 873-891, doi: 10.1016/j.chb.2004.03.003.

Manrai, R., Goel, U. and Yadav, P.D. (2021), "Factors affecting adoption of digital payments by semi-rural Indian women: extension of UTAUT-2 with self-determination theory and perceived credibility", *Aslib Journal of Information Management*, Vol. 73 No. 6, pp. 814-838, doi: 10.1108/AJIM-12-2020-0396.

Martins, C., Oliveira, T. and Popovič, A. (2014), "Understanding the Internet banking adoption: a unified theory of acceptance and use of technology and perceived risk application", *International Journal of Information Management*, Vol. 34 No. 1, pp. 1-13, doi: 10.1016/j.ijinfomgt.2013.06.002.

Pavlou, P.A. (2003), "Consumer acceptance of electronic commerce: integrating trust and risk with the Technology Acceptance Model", *International Journal of Electronic Commerce*, Vol. 7 No. 3, pp. 101-134, doi: 10.1080/10864415.2003.11044275.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y. and Podsakoff, N.P. (2003), "Common method biases in behavioral research: a critical review of the literature and recommended remedies", *Journal of Applied Psychology*, Vol. 88 No. 5, pp. 879-903, doi: 10.1037/0021-9010.88.5.879.

PricewaterhouseCoopers (PwC) (2024), "Beyond the cloud: navigating FinTech cyber threats and fortifying defences", available at: https://www.pwc.in/assets/pdfs/consulting/beyond-the-cloud-navigating-fintech-cyber-threats-and-fortifying-defences-v3.pdf (accessed 9 April 2025).

Rana, N.P., Luthra, S. and Rao, H.R. (2019), "Key challenges to digital financial services in emerging economies: the Indian context", *Information Technology and People*, Vol. 33 No. 1, pp. 198-229, doi: 10.1108/ITP-05-2018-0243.

Reserve Bank of India (2016), "Cyber security framework in banks", available at: https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/NT41802062016.pdf (accessed 10 May 2025).

Reserve Bank of India (2020), "Online Dispute resolution (ODR) system for digital payments", available at: https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=3194 (accessed 10 April 2025).

Riek, M., Bohme, R. and Moore, T. (2015), "Measuring the influence of perceived cybercrime risk on online service avoidance", *IEEE Transactions on Dependable and Secure Computing*, Vol. 13 No. 2, pp. 261-273, doi: 10.1109/TDSC.2015.2410795.

Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change1", *The Journal of Psychology*, Vol. 91 No. 1, pp. 93-114.

Shankar, A. and Datta, B. (2018), "Factors affecting mobile payment adoption intention: an Indian perspective", *Global Business Review*, Vol. 19 No. 3, pp. 72-89, doi: 10.1177/0972150918757870.

Sharma, P., Gallani, V. and Maheria, S. (2024), "Digital payments and fraud connection: insights from the Indian economy", *International Journal of Management, Economics and Commerce*, Vol. 1 No. 2, pp. 102-111, doi: 10.62737/spqxve67.

Singh, N., Sinha, N. and Liébana-Cabanillas, F.J. (2020), "Determining factors in the adoption and recommendation of mobile wallet services in India: analysis of the effect of innovativeness, stress to use and social influence", *International Journal of Information Management*, Vol. 50, pp. 191-205, doi: 10.1016/j.ijinfomgt.2019.05.022.

Sivathanu, B. (2019), "Adoption of digital payment systems in the era of demonetization in India: an empirical study", *Journal of Science and Technology Policy Management*, Vol. 10 No. 1, pp. 143-171, doi: 10.1108/JSTPM-07-2017-0033.

Slovic, P. (1987), "Perception of risk", *Science*, Vol. 236 No. 4799, pp. 280-285, doi: 10.1126/science.3563507.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003), "User acceptance of information technology: toward a unified view", *MIS Quarterly*, Vol. 27 No. 3, pp. 425-478, doi: 10.2307/30036540.

Verma, S., Sharma, J., Kaushik, K. and Vyas, V. (2023), "Mounting cases of cyber-attacks and digital payment", in Saini, H.S. and El-Khatib, K. (Eds), *Cybersecurity Issues, Challenges, and Solutions in the Business World*, IGI Global, pp. 59-80.

Weerakkody, V., Irani, Z., Kapoor, K., Sivarajah, U. and Dwivedi, Y.K. (2017), "Open data and its usability: an empirical view from the Citizen's perspective", *Information Systems Frontiers*, Vol. 19 No. 2, pp. 285-300, doi: 10.1007/s10796-016-9679-1.

Zhou, T. (2014), "An empirical examination of initial trust in mobile payment", *Wireless Personal Communications*, Vol. 77 No. 2, pp. 1519-1531, doi: 10.1007/s11277-013-1596-8.

Further reading

Data Security Council of India (DSCI) (2024), "India Cybersecurity Domestic Market 2023", available at: https://www.dsci.in/files/content/knowledge-centre/2024/India%20Cybersecurity%20Domestic%20Market%202023.pdf (accessed 9 April 2025).

Sharma, S.K. and Sharma, M. (2019), "Examining the role of trust and quality dimensions in the actual usage of mobile banking services: an empirical investigation", *International Journal of Information Management*, Vol. 44, pp. 65-75, doi: 10.1016/j.ijinfomgt.2018.09.013.

Supplementary material

The supplementary material for this article can be found online.

Corresponding author

Aya Aljaradat can be contacted at: aljaradat20@iitk.ac.in