

Original Research Article

AI-Driven Personalisation in Digital Payments: Examining Its Impact on Customer Trust

Dr Subhash Ramachandran Nadar,¹ Dr Shoba James,² Ms Deepa Muthumani,³ Ms Jagatheeshwari Deivamuthu Nadar⁴

¹*Researcher, K J Somaiya Institute of Management, India*

²*Associate Professor, Vijay Patil School of Business, India*

³*Research Scholar, Guru Nanak College, Mumbai, India*

⁴*Research Scholar, Guru Nanak College, Mumbai, India*

Received: 10 September, 2026 | Accepted: 24 September, 2026 | Published: 19 October, 2026

Abstract

Digital India programme over a decade shown an upward performance by setting a benchmark. It is a flagship initiatives of the Government of India. It has digitally empowering the society and digital economy. Digital economy is an economic activities enhanced with the digital transformation using the digital computing tools. It provided various opportunities in the Banking and Fintech sectors. In current scenario Artificial Intelligence (AI) playing a very significant pivotal role by integrating the technology in all the sectors. It is enhancing the opportunities for the service provider and customer.

Due to the rapid expansion of digital payment ecosystems, it has transformed the way how a consumers conduct their everyday financial transactions for purchasing their requirements either through online shopping i.e. e-commerce or visiting the store personal and using the digital banking or digital payment. In India, the digital payment especially using Unified Payments Interface (UPI) now has become a very important component of the digital financial ecosystem.

Alongside this growth, the payment service providers are progressively integrating with the Artificial Intelligence (AI) technology to personalise their customer experiences. This is providing an enhance features through transaction recommendations to the customers with amazing discount features or offers in the payments using the digital payments. It further enables the customers in identifying their spending insights and intelligent alerts and adaptive customer support.

This conceptual research proposes to examine the relationship between AI driven personalisation and customer trust in digital payment systems. The study propose to integrate from the perspectives of adopting the model Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) with the trust theory. The proposed model considers AI personalisation, perceived usefulness, perceived relevance, transparency as among the key explanatory variables, with customer trust as the principal dependent construct. Behavioural intention and continuance intention are considered as potential outcomes of trust.

The expected findings may provide very useful insight in the domain of digital banking, digital payment segment of the banks, fintech companies, and payment service providers to improve the trustworthy for the customer and responsible AI enabled payment ecosystems.

Keywords: Artificial Intelligence, AI-driven personalisation, digital payments, UPI, customer trust.

1. Introduction

Digital India programme over a decade shown an upward performance by setting a benchmark. It is a flagship initiatives of the Government of India. It has digitally empowering the society and digital economy in Digital transformation. Digital transformation has fundamentally changed the financial services industry. Mobile banking, digital wallets, contactless payments and real-time payment infrastructure have progressively reduced dependence on traditional cash based transactions. In India, this transformation has been more particularly very significant because of the instant development of the Unified Payments Interface (UPI). It has enabled the users in making the real time payments through with the aid of interoperable bank accounts and digital payment applications. NPCI statistics revealed that UPI processed 23,201.93 million transactions in May 2026 and valued at approximately ₹29,90,424.21 crore. Such a great scale of volume and value indicates that digital payments have moved beyond as being an alternative payment application. Now it has become an integral part of costumers' day-to-day financial processing.

The next advanced stage of digital payment development is progressively influenced by Artificial Intelligence (AI). Given the advancement in technologies have led the applications like AI and Machine Learning (ML) technologies implementation in all the sectors. Now AI and ML are being integrated into payment platforms to identify the customers' transaction by enabling to determine the transaction patterns, detection of fraud activities, predicting the needs of the customer, providing personalised recommendations to the costumer while using the e-Commerce, automating the customer service and generate the financial insights. RBI has also recognised the transformative potential of AI in financial services while highlighting risks associated with algorithmic bias, explainability and data privacy.

Personalisation represents one of the most visible customer facing applications of AI. Digital payment platforms now can analyse the customers activities with the features like transaction history, merchant preferences, frequency of payments the customer making the online payment. The customer way of spending in various

categories, providing the insight of classified categories and spending behavioural patterns to provide a unique customised experiences. For example, a digital payment application may identify recurring payments by recommending the customer on relevant offers, providing them the spending summaries, generating based on their spending personalised financial alerts or even customise the presentation of payment related information to the individual users.

In the point of view of consumer such personalisation helps to create a convenience and perceived value. When customer receives information that is more relevant to their financial behavior, it may leads them to perceive the digital payment platform as more useful and intelligent. Personalisation also helps the customer in reducing the information excess by presenting the appropriate recommendations instead of standard messages.

However, personalisation generates a fundamental tension. The system to deliver highly personalised services to the customers in their Digital payment the AI systems requires to retrieve substantial amounts of customer data. Data related to Financial transaction are mainly sensitive as it leads to provide an insight to consumption patterns, the lifestyle preferences of the customer. Further it helps in identifying the merchant relationships and aspects of an individual's economic behaviour. Therefore, the same data driven capabilities that may increase convenience but also leads to generate privacy concerns over the financial data.

This relevant data issue can be pronounced as the personalization privacy paradox. Customers may appreciate personalised services while simultaneously feeling uncomfortable about how much information the digital payment platforms collect and how the system algorithms is defined to use that information. Previous research studies on AI enabled digital services similarly identifies the rigidity between personalised value and privacy concerns. It also emphasis the transparency and user control as an important components of trust.

Trust is therefore particularly important in digital payment environments. Unlike many conventional digital services the payment platforms now mostly deal directly with users' money and financial information. A customer may be willing to use an digital payment application only when they believe that the system provide the necessary security, they are reliable, transparent and skillfully able to protect their information.

Previous research has established that trust is an important determinant of fintech adoption. An empirical study integrating UTAUT2 and trust theory found that trust significantly influenced both intention to use and actual use of fintech services. Similarly, research on Indian mobile payment adoption has incorporated trust, personal innovativeness, anxiety and grievance redressal into technology adoption models.

Recent research has begun to examine AI enabled digital payments specifically. In the study 2026 on AI in UPI usage reported that AI based personalization, security and customer support were associated with financial confidence and sustained UPI usage. Another recent study examined AI enhanced digital payment adoption using an extended UTAUT2 model incorporating trust and security. These studies demonstrate the emerging relevance of AI and trust but also indicate the need for more focused investigation into the specific mechanism through which personalisation affects trust.

Therefore, the present study focuses on the research problem:

Does AI-driven personalisation strengthen customer trust in digital payment systems, or do privacy and transparency concerns offset its perceived benefits?

The study proposes a conceptual model that combines AI personalisation, perceived relevance, perceived usefulness, transparency, perceived security and privacy concerns to explain customer trust.

The research is particularly relevant to India because digital payment adoption has reached very high levels while AI enabled financial services are simultaneously expanding. NPCI reported that UPI processed a record 21.70 billion transactions in January 2026, demonstrating the scale at which customer facing innovations can potentially operate.

2. Literature Review – Thematic Format

2.1 Digital Payments and Consumer Behaviour

Digital payments refer to electronically initiated and processed financial transactions using technologies such as mobile banking applications, digital wallets, cards, QR codes and realtime payment systems. The growth of smartphones, Internet connectivity and digital public infrastructure has significantly increased the accessibility of these services.

Consumer adoption of digital payments is influenced by convenience, perceived usefulness, ease of use, security, trust, social influence, perceived risk and facilitating conditions. The UTAUT2 framework provides a useful theoretical foundation for analysing consumer technology adoption because it incorporates performance expectancy, effort expectancy, social influence, facilitating conditions, hedonic motivation, price value and habit (Venkatesh et al., 2012).

Research conducted in India has shown that consumer adoption of mobile payments is influenced by behavioural and contextual factors. Patil et al. (2020), for example, extended the Meta-UTAUT framework by incorporating personal innovativeness, anxiety, trust and grievance redressal and demonstrated their relevance to mobile payment adoption.

2.2 Artificial Intelligence in Digital Payments

AI is increasingly being applied throughout the digital payment value chain. Applications include fraud detection, anomaly identification, transaction monitoring, customer service automation, credit assessment, behavioural prediction and personalisation.

AI can process large quantities of transaction data and identify patterns that may not be immediately observable through conventional rule based systems. RBI has acknowledged the potential of AI and machine learning to improve financial sector efficiency while also identifying algorithmic bias, explainability and privacy as important risks.

The increasing presence of AI means that payment applications are evolving from transaction processing tools into intelligent financial platforms capable of anticipating customer requirements.

2.3 AI Driven Personalisation

AI driven personalisation refers to the use of AI and machine learning techniques to tailor digital services, content, recommendations, offers, notifications or interactions to individual users based on their data and behavioural patterns.

Personalisation can improve perceived relevance because consumers receive information aligned with their individual needs. When consumers perceive that a digital service understands their preferences, they may develop stronger perceptions of usefulness and relationship quality.

Recent research examining AI driven personalisation has identified perceived personal relevance and trust as important components of AI-enabled customer relationships.

However, personalisation does not automatically produce positive outcomes. The effectiveness of personalisation depends on whether users understand and accept the underlying data practices.

2.4 Customer Trust in Digital Payments

Trust refers to the consumer's willingness to rely on a service provider despite uncertainty regarding future outcomes. In digital payment environments trust encompasses confidence in the platform's security, reliability, integrity and ability to protect financial information.

Trust is particularly important because financial transactions involve perceived financial risk. A consumer may understand how a payment application works but still hesitate to use it if the platform is perceived as unsafe.

Amnas *et al.* (2023) found that trust plays an important role in fintech adoption and influences both intention to use and actual use. In the Indian context research has similarly demonstrated the importance of trust in mobile payment adoption. Patil *et al.* (2020) found significant relationships among technology-adoption variables, trust related factors and mobile payment usage.

Recent research also shows that cybersecurity perceptions influence trust in digital payment environments. In a study conducted in 2026 focusing on North India examined trust formation in digital payment behaviour in relation to perceived cybersecurity risk, effort expectancy, performance expectancy and grievance redressal.

2.5 Perceived Security and Trust

Perceived security represents the degree to which consumers believe that digital payment systems protect their transactions and financial information against unauthorised access, fraud and misuse.

AI can improve security through real-time transaction monitoring and anomaly detection. However, security mechanisms can also affect user experience. Excessive authentication requirements or unexplained transaction blocks may create frustration.

A recent study of AI-enabled security features found that security-assurance mechanisms can shape users' perceptions of payment security and trust.

Thus, AI may contribute to trust through two interconnected pathways: first, by making the payment experience more personalised and useful; and second, by improving perceptions of security.

2.6 Privacy Concerns and the Personalisation Privacy Paradox

Privacy concerns arise when consumers perceive that organisations collect, store, analyse or share personal information in ways that exceed their expectations.

AI personalisation intensifies this issue because greater personalisation generally requires greater access to behavioural data. The customer may benefit from a personalised recommendation but simultaneously question how the platform obtained the information necessary to generate it.

The Indian regulatory environment further increases the importance of responsible data management. The Digital Personal Data Protection Act, 2023 establishes requirements concerning processing of personal data and consent-related practices.

Therefore, payment providers must balance personalisation with transparency, consent and user control.

2.7 Transparency, and Trust

Transparency refers to the extent to which consumers understand how their information is collected, processed and used. In AI-based systems, transparency also concerns the ability of users to understand why a particular recommendation, alert or decision has been generated.

For example, a payment application that displays “Recommended for you because you frequently shop at this merchant” may be perceived as more transparent than one that simply provides an unexplained recommendation.

RBI’s development of the free AI framework demonstrates the growing importance of responsible and ethical AI in the financial sector. The framework addresses concerns including privacy, bias and explainability.

3. Research Gap

The existing literature provides substantial evidence that trust, security, perceived usefulness and technology acceptance influence digital payment adoption. However, three important gaps remain.

The first one most of the digital payment literature focuses on **adoption intention**, whereas relatively less attention is given to how specific AI capabilities influence trust after consumers have already adopted digital payments.

Second AI research in financial services often concentrates on fraud detection, risk assessment and operational efficiency. The consumer facing dimension of AI driven personalisation remains comparatively underexplored.

The third gap is personalisation and privacy are frequently examined independently. There is a need for an integrated model examining whether personalisation creates trust when users perceive security and transparency, and whether privacy concerns weaken this relationship.

The present research addresses these gaps by proposing a model centred on **AI-driven personalisation leading to customer trust** by incorporating perceived usefulness, perceived relevance, transparency, security and privacy concerns.

4. Research Objectives

The primary objective is:

To examine the impact of AI-driven personalisation on customer trust in digital payment systems.

The specific objectives are:

1. To examine consumers’ perceptions of AI driven personalisation in digital payment applications.
2. To determine the influence of perceived relevance on customer trust.
3. To examine the effect of perceived usefulness of AI personalisation on customer trust.
4. To investigate the relationship between perceived security and customer trust.
5. To examine the effect of privacy concerns on customer trust.
6. To determine whether transparency in AI personalisation contributes to customer trust.

7. To examine the influence of customer trust on behavioural intention and continuance intention.

5. Hypothesis

H1: AI-driven personalisation positively influences customer trust.

H2: Perceived relevance positively influences customer trust.

H3: Perceived usefulness of AI personalisation positively influences customer trust.

H4: Perceived security positively influences customer trust.

H5: Privacy concerns negatively influence customer trust.

H6: Transparency in AI personalisation positively influences customer trust.

H7: Customer trust positively influences behavioural/continuance intention to use digital payment services.

H8: Privacy concerns negatively moderate the relationship between AI-driven personalisation and customer trust; higher privacy concern weakens the positive AIP → CT relationship.

6. Theoretical Framework

The research study integrates three complementary theoretical perspectives.

6.1. UTAUT2

UTAUT2 explains consumer technology acceptance through performance expectancy, effort expectancy, social influence, facilitating conditions, hedonic motivation, price value and habit (Venkatesh et al., 2012).

In this research, perceived usefulness is related to performance expectancy, while continued use represents a post-adoption outcome.

6.2. Trust Theory

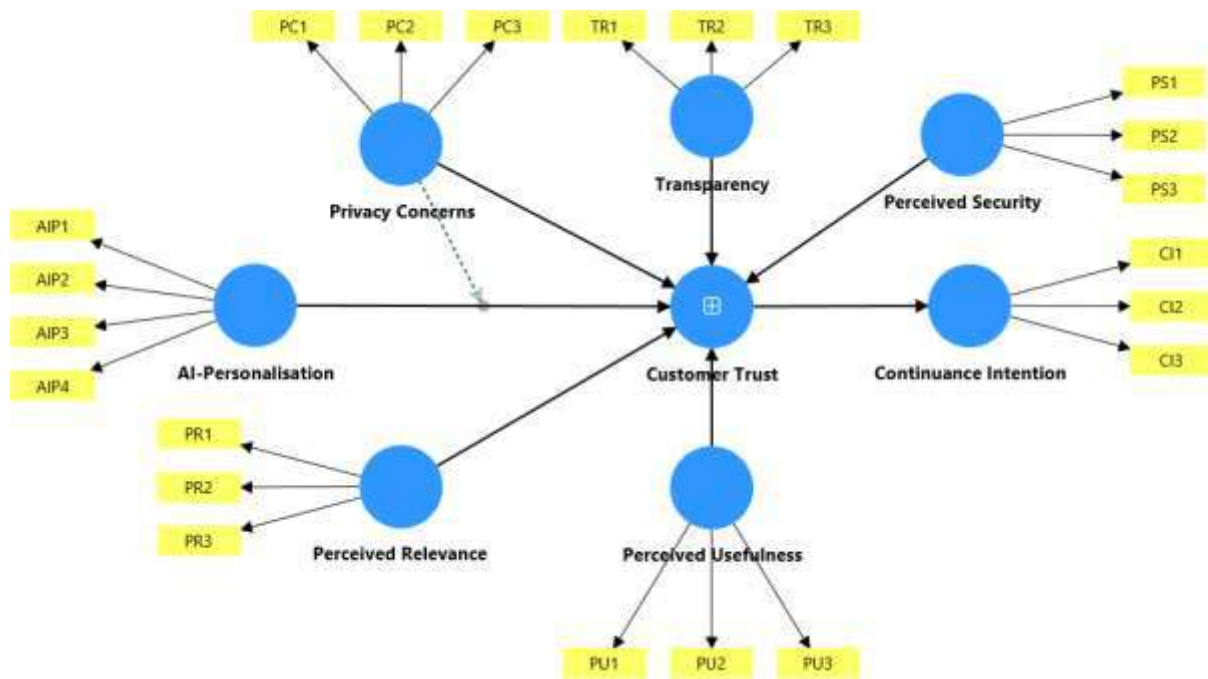
Trust theory explains why users are willing to depend on technology providers despite uncertainty. In digital payments, trust is particularly important because transactions involve financial and personal information.

Previous research supports the incorporation of trust into UTAUT-based fintech adoption models.

6.3. Privacy Calculus Perspective

Privacy calculus proposes that users compare perceived benefits against perceived privacy risks. AI personalisation provides benefits through relevance and convenience but may increase privacy concerns because of extensive data collection and processing.

The proposed model therefore assumes that:



7. Research Methodology

7.1. Research Design

The study adopted **quantitative research design**. In this research primary data is collected by way of questionnaire from customers who have experience using digital payment services.

7.2. Population

The target population comprises individuals who use digital payment services. The study is focused in Mumbai being a financial city with particular emphasis on urban digital payment users.

7.3. Sample Size

The questionnaire is presented to 400 respondents out of this 320 respondents have responded and they have filled the survey form.

7.4. Sampling Technique

A combination of purposive and convenience sampling used.

Respondents satisfied the following criteria:

1. age 18 years or above;
2. use at least one digital payment application;
3. have conducted digital payments within the previous six months; and
4. have experienced or noticed personalised features such as offers, recommendations, spending insights, alerts or AI-based support.

7.5 Data Collection Instrument

A structured questionnaire developed using a five-point Likert scale 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree. The questionnaire contains demographic questions followed by construct related questionnaire items as per the objectives.

8. Data Analysis Results and Findings

Demographics

Gender

Gender	Frequency	Percentage
Female	165	51.6
Male	153	47.8
Other/Prefer not to say	2	0.6

Age

Age	Frequency	Percentage
26–35	129	40.3
18–25	70	21.9
36–45	66	20.6
46–55	38	11.9
56+	17	5.3

Education

Education	Frequency	Percentage
Postgraduate	148	46.2
Graduate	108	33.8
Professional qualification	52	16.2
Other	12	3.8

Occupation

Occupation	Frequency	Percentage
Salaried employee	159	49.7
Student	56	17.5
Business/Self-employed	41	12.8
Professional	31	9.7
Homemaker	23	7.2
Other	10	3.1

Monthly Income

MonthlyIncome	Frequency	Percentage
₹25,001–50,000	99	30.9
₹50,001–75,000	77	24.1
Below ₹25,000	64	20.0
₹75,001–1,00,000	46	14.4
Above ₹1,00,000	34	10.6

Digital Payment Frequency

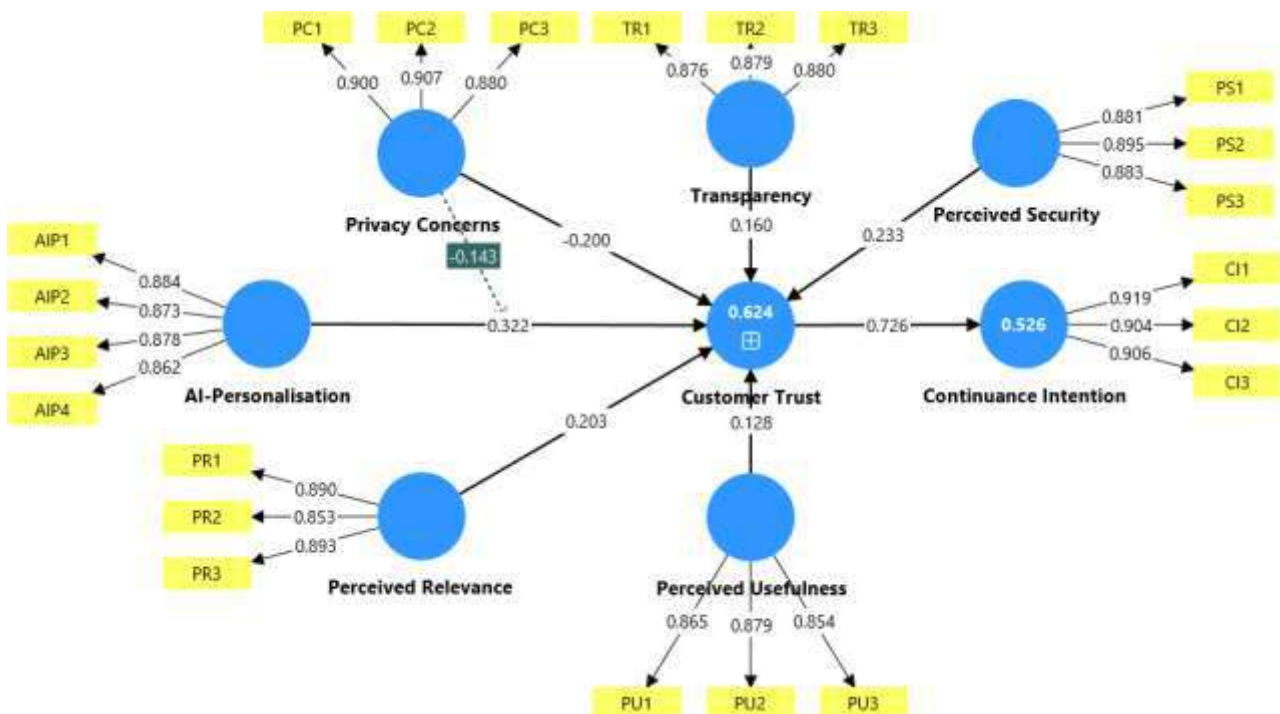
Digital_Payment_Frequency	Frequency	Percentage
Daily	146	45.6
Several times a week	106	33.1
Weekly	45	14.1
2–3 times a month	13	4.1
Less often	10	3.1

Digital Payment Experience

Digital Payment Experience	Frequency	Percentage
4–6 years	97	30.3
7–10 years	92	28.7
1–3 years	66	20.6
>10 years	48	15.0
<1 year	17	5.3

Measurement Model

The measurement model was treated as reflective. Indicator reliability was examined through outer loadings; internal consistency through Cronbach's alpha and composite reliability (CR); and convergent validity through AVE.



Reliability and Validity

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
AI-Personalisation	0.897	0.897	0.928	0.764
Continuance Intention	0.896	0.896	0.935	0.828
Customer Trust	0.907	0.908	0.935	0.781
Perceived Relevance	0.853	0.859	0.911	0.773
Perceived Security	0.864	0.864	0.917	0.786
Perceived Usefulness	0.833	0.837	0.900	0.750
Privacy Concerns	0.877	0.881	0.924	0.802
Transparency	0.852	0.852	0.910	0.772

Discriminant Validity

Discriminant validity was assessed using the Fornell Larcker criterion and HTMT. The diagonal values in the Fornell Larcker table are the square roots of AVE and are higher than the corresponding inter construct correlations.

Fornell Larcker Criteria

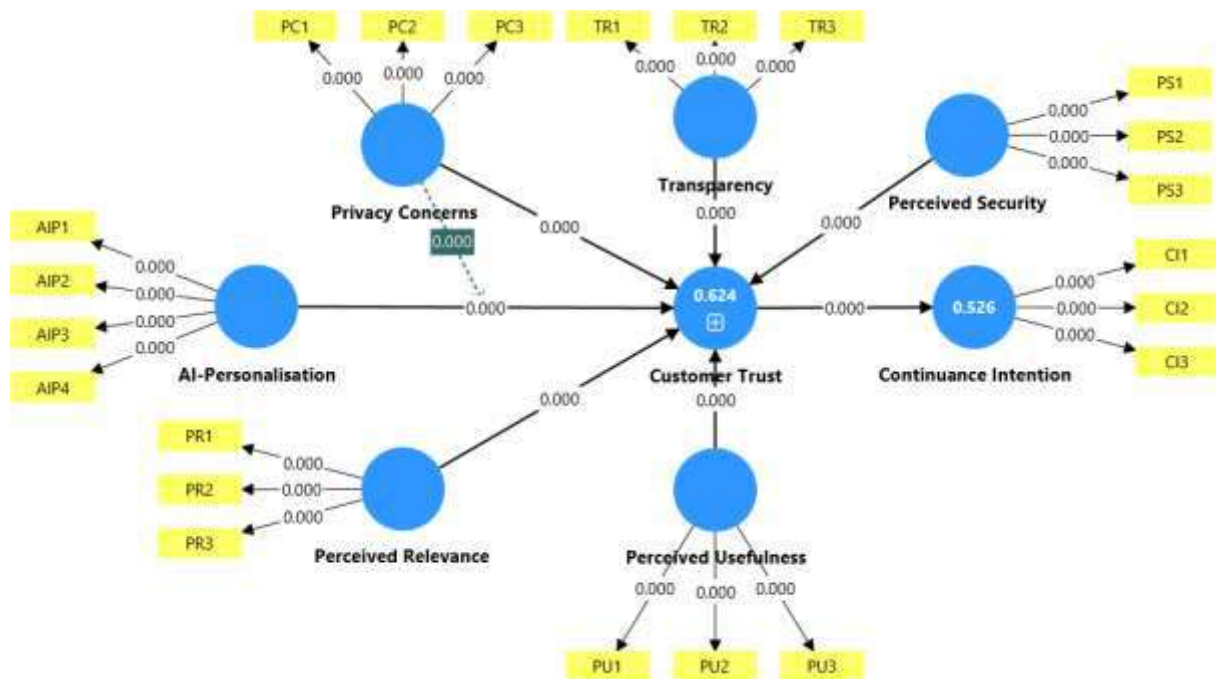
	AI-Personalisation	Continuance Intention	Customer Trust	Perceived Relevance	Perceived Security	Perceived Usefulness	Privacy Concerns	Transparency
AI-Personalisation	0.874							
Continuance Intention	0.461	0.910						
Customer Trust	0.623	0.726	0.884					
Perceived Relevance	0.388	0.345	0.461	0.879				
Perceived Security	0.312	0.381	0.487	0.215	0.886			
Perceived Usefulness	0.399	0.321	0.453	0.300	0.288	0.866		
Privacy Concerns	-0.182	-0.369	-0.363	-0.075	-0.206	-0.161	0.896	
Transparency	0.354	0.372	0.460	0.231	0.314	0.237	-0.204	0.878

HTMT

	AI- Personalis ation	Continu ance Intentio n	Custo mer Trust	Percei ved Releva nce	Percei ved Securi ty	Perceiv ed Useful ness	Privac y Conce rns	Transpar ency	Privacy Concerns x AI- Personalis ation
AI- Personalis ation									
Continuan ce Intention	0.514								
Customer Trust	0.688	0.804							
Perceived Relevance	0.441	0.394	0.522						
Perceived Security	0.354	0.433	0.550	0.249					
Perceived Usefulness	0.460	0.371	0.518	0.354	0.337				
Privacy Concerns	0.206	0.417	0.405	0.098	0.237	0.189			
Transpare ncy	0.406	0.425	0.522	0.268	0.366	0.282	0.235		
Privacy Concerns x AI- Personalis ation	0.040	0.065	0.095	0.058	0.133	0.013	0.090	0.050	

Path Analysis

Structural Model



	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values	Status
AI-Personalisation -> Customer Trust	0.322	0.322	0.044	7.387	0.000	Accepted
Customer Trust -> Continuation Intention	0.726	0.726	0.028	26.100	0.000	Accepted
Perceived Relevance -> Customer Trust	0.203	0.203	0.041	4.995	0.000	Accepted
Perceived Security -> Customer Trust	0.233	0.232	0.042	5.594	0.000	Accepted
Perceived Usefulness -> Customer Trust	0.128	0.129	0.036	3.574	0.000	Accepted
Privacy Concerns -> Customer Trust	-0.200	-0.201	0.040	5.042	0.000	Accepted
Privacy Concerns x AI-Personalisation -> Customer Trust	-0.143	-0.143	0.034	4.218	0.000	Accepted
Transparency -> Customer Trust	0.160	0.160	0.041	3.865	0.000	Accepted

Interpretation: all eight hypotheses are supported

The strongest positive predictor of trust is perceived security ($\beta = .233$), followed by AI-driven personalisation ($\beta = .319$), perceived relevance ($\beta = .204$), transparency ($\beta = .161$) and perceived usefulness ($\beta = .127$). Privacy concern has a statistically significant negative direct effect on trust ($\beta = -.198$). Customer trust has a strong positive

association with behavioural/continuance intention ($\beta = .725$). The AIP $\times$ PC interaction is negative ($\beta = -.144$), indicating that increasing privacy concern weakens the positive association between AI personalisation and trust.

R Square – Coefficient of Determination.

Constructs	R-square	R-square adjusted
Continuance Intention	0.526	0.525
Customer Trust	0.624	0.616

Customer Trust has $R^2 = 0.624$, meaning the antecedent set explains approximately 62.4% of the variance in trust. Continuance Intention has $R^2 = 0.526$, so customer trust explains approximately 52.6% of the variance in intention.

Findings

- **AI-driven personalisation and trust**

The positive AIP $\rightarrow$ CT path ($\beta = .319$, $p < .001$) supports H1. This suggests that when users perceive payment applications as understanding preferences and providing relevant personalised services, trust increases. This is consistent with trust based e-commerce research showing that trust helps users overcome uncertainty and perceived risk in digital transactions (McKnight et al., 2002; Kim et al., 2008). Recent AI-personalisation research also reports a positive association between AI-driven personalisation and consumer trust, although the exact effect depends on ethical safeguards.

- **Perceived relevance**

Perceived relevance significantly predicts trust ($\beta = .204$, $p < .001$). Relevant recommendations can signal that the system understands user needs and is delivering value rather than arbitrary promotional content. This result supports the broader personalisation literature in which relevance is a central source of perceived value. It should nevertheless be interpreted alongside privacy concerns because personalisation requires data use.

- **Perceived usefulness**

Perceived usefulness has a positive effect on trust ($\beta = .127$, $p < .001$). Although smaller than security and personalisation, usefulness remains significant. This is consistent with technology-acceptance logic: useful technology is more likely to be accepted and used. UTAUT2 also establishes the importance of consumer technology beliefs in explaining behavioural intention (Venkatesh et al., 2012).

- **Perceived security**

Perceived security is a significant positive predictor of trust ($\beta = .233$, $p < .001$), making it the strongest positive antecedent among the individual trust predictors. This aligns closely with mobile-payment evidence showing that perceived security protection positively influences trust and continuance intention (Nelloh et al., 2019).

- **Privacy concern**

Privacy concern negatively predicts trust ($\beta = -.198$, $p < .001$). This supports the idea that the benefits of personalisation are accompanied by perceived information-privacy risk. Culnan and Armstrong (1999) show how information practices and procedural fairness relate to privacy and impersonal trust, while Awad and Krishnan (2006) document the personalisation–privacy paradox. Thus, the synthetic result is theoretically consistent with the privacy-risk side of the paradox.

- **Transparency**

Transparency significantly improves trust ($\beta = .161, p < .001$). Clear explanations of data use and why a recommendation is generated can reduce uncertainty and improve perceived accountability. This is compatible with recent work emphasizing transparency and user control as important mechanisms for managing trust in AI personalisation.

- **Trust and continuance intention**

Customer trust has a strong positive relationship with behavioural/continuance intention ($\beta = .725, p < .001; R^2 = .525$). This is consistent with prior digital-commerce research showing that trust is a major determinant of consumers' transaction decisions and with mobile-payment evidence that trust is an important determinant of continuance.

- **Moderating role of privacy concern**

The interaction $AIP \times PC$ is negative and significant ($\beta = -.144, p < .001$). This means that the positive trust benefit of AI personalisation becomes weaker as privacy concern increases. The result directly addresses the consistent with the personalisation privacy paradox literature, where personalisation creates value while simultaneously increasing sensitivity to data collection and profiling.

9. Managerial implications

- **Design personalisation around customer value**

Banks and payment providers should make recommendations genuinely relevant to transaction patterns, preferences and user needs rather than maximising the volume of personalised offers.

- **Make security visible**

Security controls should not remain invisible back-end functions. Providers should communicate fraud monitoring, authentication, alerts and transaction-protection mechanisms in understandable language.

- **Build privacy-by-design**

Privacy should be incorporated into the AI personalisation architecture through data minimisation, purpose limitation, consent controls and easy-to-use privacy settings.

- **Give customers control**

Customers should be able to view, modify or opt out of certain personalisation features without losing access to essential payment services.

- **Segment privacy sensitive users**

The significant moderation result indicates that one personalisation strategy should not be applied uniformly. Users with higher privacy concerns may require lower-intensity personalisation and stronger control features.

- **Monitor trust as a KPI**

Banks and fintech firms should track trust alongside conversion, engagement and transaction-frequency metrics. High engagement with declining trust may create longer-term retention risk.

10. Outcome of the study

The integrated model provides a coherent explanation of how functional and ethical characteristics of AI personalisation shape trust in digital payment services. The central outcome is that personalisation creates trust when users perceive relevance, usefulness, security and transparency, but privacy concern creates a countervailing force. Trust then translates into stronger behavioural/continuance intention. This supports the proposed conceptual direction and provides a practical framework for responsible AI-enabled digital-payment design.

11. Conclusion

Based on the PLS-SEM analysis, the model is statistically well behaved the indicators demonstrate acceptable reliability and convergent validity, the constructs demonstrate discriminant validity and the structural model explains the substantial variance in customer trust and continuance intention. All the eight hypotheses are supported in the dataset. The results signify that AI-driven personalisation should not be evaluated only through the lens of convenience or engagement. Trust depends on a balance between personalisation value and responsible handling of personal data. Security and transparency therefore become strategic enablers of AI personalisation, while privacy concern represents a boundary condition that can reduce its trust-building effect.

References

- Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 30(1), 13–28. <https://doi.org/10.2307/25148715>
- Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104–115. <https://doi.org/10.1287/orsc.10.1.104>
- Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, 31(1), 2–24. <https://doi.org/10.1108/EBR-11-2018-0203>
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43, 115–135. <https://doi.org/10.1007/s11747-014-0403-8>
- Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, 44(2), 544–564. <https://doi.org/10.1016/j.dss.2007.07.001>
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334–359. <https://doi.org/10.1287/isre.13.3.334.81>
- Nelloh, L. A. M., Santoso, A. S., & Slamet, M. W. (2019). Will users keep using mobile payment? It depends on trust and cognitive perspectives. *Procedia Computer Science*, 161, 1156–1164. <https://doi.org/10.1016/j.procs.2019.11.228>
- RBI <https://www.rbi.org.in>

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36(1), 157–178.
<https://doi.org/10.2307/41410412>