International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Digital Innovation & Transformation in India-Awareness and customer trust in banking and insurance sector-DPDP act Perspective

Mrs. Roopa B V
Research Scholar, Department of Management Studies and Research Centre,
B.M.S. College of Engineering, Bangalore – 560019
Email: roopa.shivaram@gmail.com Mobile: 7899825662

Dr. Prathima Bhat K
Professor, Department of Management, B.M.S. College of Engineering, Bangalore – 560019 Email: prathimabhat.mba@bmsce.ac.in Mobile: 9242187131

Dr.Nijaguna G
Professor, Department of Business Administration , Acharya Institute of Technology, Soldevanahally, Bengaluru-560107
Email: nijaguna@acharya.ac.in Mobile: +91 9900944552

Abstract
India's Digital Personal Data Protection (DPDP) Act, 2023 gives customers of banks and insurers enforceable rights over their personal data, yet whether awareness of the Act and of institutional safeguards translates into trust and continued digital use is an open question. This paper develops a five-stage conceptual model (DPDP awareness → data privacy, cybersecurity and consent/data-control practices → perceived data security → customer trust → continued use) and sets out six objectives and eight hypotheses. Because no field data were available, the analytical workflow is demonstrated on a simulated sample of 100 respondents with varied age, gender, education, occupation and income and 30 five-point Likert items; the data are synthetic and the results are illustrative only. In the simulated data, reliability was acceptable (α = .75–.84), privacy practices, cybersecurity practices and awareness predicted perceived security (R^2 = .36), perceived security predicted trust, and trust predicted continued use (β = .43). Both indirect effects were significant in bootstrap tests, while the consent/data-control effect on trust was marginal (p = .057). The paper closes with findings, suggestions and limitations, and stresses that the numerical results must be re-estimated on genuine survey data before any substantive claim is made.

Keywords: *DPDP Act 2023; data privacy; cybersecurity; consent; perceived data security; customer trust; digital banking; insurance*

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

1. Introduction

Digital channels have become the default way in which Indian customers transact with banks and insurers. Unified Payments Interface (UPI) payments, mobile banking, online policy purchase, e-KYC and digital claims all require customers to share identity, financial and, for insurance, health information. This concentration of sensitive data in a few institutions makes data protection a precondition for sustained digital adoption, not merely a compliance matter.

The Digital Personal Data Protection Act, 2023 (Government of India, 2023) is India's first comprehensive statute on digital personal data. It obliges organisations (data fiduciaries) to process personal data lawfully, to obtain clear and specific consent, to apply reasonable security safeguards, and to notify breaches, while granting individuals (data principals) rights to information, correction, erasure and grievance redress. The Digital Personal Data Protection Rules, 2025 were notified on 14 November 2025 and are being phased in: provisions on the Data Protection Board took effect immediately, consent-manager provisions follow after twelve months (November 2026), and the main operational duties on notice, consent, security safeguards and breach reporting apply from May 2027. Banks and insurers are therefore in a transition period in which customers' experience of data handling, and their understanding of their new rights, will shape how they respond to digital services.

For an institution, the commercial question is whether better privacy, security and consent practices are noticed by customers and whether they convert into trust and continued digital use. For a regulator, it is whether a rights-based law changes customer perceptions or whether awareness remains thin. This paper addresses these questions through a structured conceptual model and a set of testable hypotheses.

2. Research Framework

The framework draws on three established ideas. Trust is commonly understood as a willingness to be vulnerable to another party based on perceived ability, benevolence and integrity (Mayer, Davis and Schoorman, 1995); data security perceptions speak to ability, while transparent privacy and consent practices speak to benevolence and integrity. The commitment–trust view of relationship marketing treats trust as a precursor of relationship continuity (Morgan and Hunt, 1994). Technology-acceptance research treats intention to keep using a system as the main outcome of its perceived qualities (Davis, 1989). Combining these, the study proposes that customers' awareness of the DPDP Act shapes how they evaluate institutional practices; that practices in three areas (data privacy, cybersecurity, and consent/data control) shape perceived data security and trust; and that trust, in turn, drives continued use of digital financial services.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

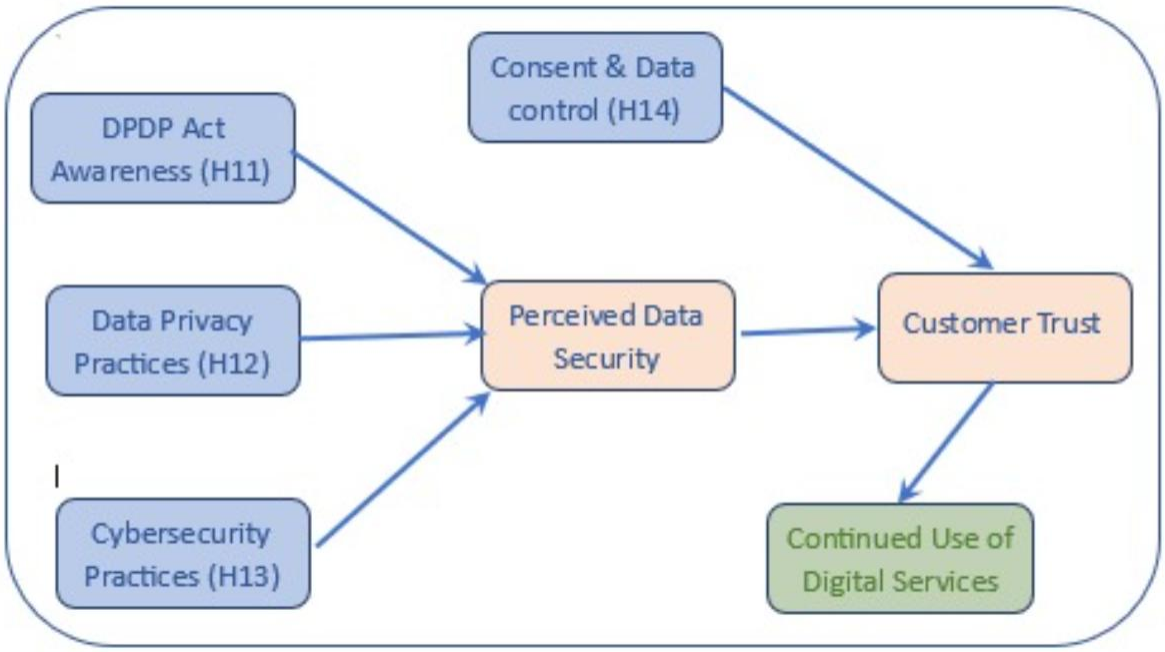


Figure 1. Conceptual model with standardised path estimates from the data (H11–H16; mediation paths H17–H18 are in Table 7).

The sequence is: DPDP awareness → (data privacy practices + cybersecurity practices + consent/data control) → perceived data security → customer trust → continued use of digital financial services. Perceived data security and customer trust occupy mediating positions, which gives rise to the two mediation hypotheses H17 and H18.

3. Research GAP

Discussion of the DPDP Act has so far been dominated by legal and compliance perspectives, which concentrate on what organisations must do. The customer side of the relationship is less visible in this discussion: how far customers know about their rights, how they judge institutional privacy, security and consent practices, and whether these judgements carry through to trust and continued digital use. The present study identifies four gaps that the framework is designed to address, and that should be confirmed against a systematic literature review before submission, because none has been verified here:

- Awareness gap: little is known about customer-level awareness of the DPDP Act in banking and insurance, particularly after the 2025 Rules.
- Mechanism gap: awareness, institutional practices, perceived security and trust are usually studied separately; a sequential model linking them is needed.
- Mediation gap: it is unclear whether perceived data security and trust transmit the effect of practices to behavioural outcomes, or whether practices act directly.
- Sector gap: banking and insurance customers are rarely analysed together although both rely on shared KYC and financial data and are regulated under the same Act.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

4. Problem Statement

Indian banks and insurers are expanding digital services while a new rights-based data-protection regime comes into force. If customers are unaware of their rights, find privacy notices and consent requests unclear, doubt the adequacy of cybersecurity, or fail to feel that their data are secure, trust may erode and customers may limit or abandon digital use. Institutions lack evidence on which practices matter most for perceived security and trust, and on whether awareness of the Act has any role in this chain. This study therefore asks: how do DPDP awareness and institutional data privacy, cybersecurity and consent practices affect perceived data security, customer trust, and continued use of digital banking and insurance services?

5. Research Objectives and Hypotheses

Table 1. Research objectives and corresponding hypotheses

No.	Objective	Hypothesis
O1	Assess the level of awareness of the DPDP Act among banking and insurance customers	Descriptive profile of awareness. H11: DPDP awareness significantly influences perceived data security.
O2	Examine the relationship between data privacy practices and perceived data security	H12: Data privacy practices significantly influence perceived data security.
O3	Analyse the influence of cybersecurity practices on perceived security	H13: Cybersecurity practices significantly influence perceived data security.
O4	Examine the influence of consent and data-control mechanisms on customer trust	H14: Consent and data-control mechanisms significantly influence customer trust.
O5	Examine whether perceived data security influences customer trust	H15: Perceived data security significantly influences customer trust. H17: Perceived data security mediates the effect of data privacy practices on trust.
O6	Assess whether customer trust influences intention to continue using digital services	H16: Customer trust significantly influences continued use. H18: Trust mediates the effect of perceived data security on continued use.

Source: objectives and hypotheses supplied for the study. H11 is placed with O1 because it tests the consequence of awareness; it is estimated together with H12 and H13.

6. Research Methodology

6.1 Design and Instrument

The study uses a cross-sectional survey design. The questionnaire has five demographic items (age group, gender, highest education, occupation, monthly household income) and 30 statements on a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree) across seven constructs: DPDP awareness (5 items), data privacy practices (4), cybersecurity practices (5), consent and data control (4), perceived data security (4), customer trust (4) and continued digital usage (4). All items are positively worded, so no reverse coding is needed. Construct scores are the mean of their items.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

6.2 Sample and Data Collection

A sample of 100 respondents was created by computer simulation (Python; random seed 20261015) so that the analysis can be demonstrated in the absence of field data. Demographic profiles were drawn to be varied and internally plausible (for example, students are mostly aged 18–25 with low household income, and retirees are aged 51 or over). Likert responses were generated from a latent structural model following the direction of the hypothesised paths, with item-level random error so that all five response categories occur and respondents differ. The structural coefficients are design choices; the analysis therefore recovers the specified model by construction and does not test it against real behaviour. The parameters were fixed once, and results were not re-drawn to obtain significance. The data set is provided in Excel (DPDP_Simulated_Dataset_n100.xlsx) and can be replaced by real responses in the same layout.

6.3 Analytical Procedure

Internal consistency was assessed with Cronbach's alpha (≥ .70 accepted). Descriptive statistics, frequency tables and Kruskal–Wallis tests (awareness by demographic group) addressed O1. Pearson correlations screened relationships and multicollinearity. H11–H13 were tested by multiple linear regression of perceived data security on awareness, privacy practices and cybersecurity practices; H14–H15 by regression of customer trust on consent/data control and perceived data security; and H16 by regression of continued use on trust. For H17 and H18, indirect effects were estimated as the product of path coefficients with a 5,000-resample percentile bootstrap confidence interval (Preacher and Hayes, 2008), with a Sobel test as a check. The significance level was $\alpha = .05$ (two-tailed). Analyses were run in Python (numpy, scipy); the results are static values in the Excel workbook.

7. Data Analysis and Results

7.1 Respondents Profile

Table 2. Demographic profile of the simulated respondents (n = 100)

Characteristic / category	n	%
Age group		
18–25 years	21	21
26–35 years	33	33
36–50 years	21	21
51–65 years	19	19
Above 65 years	6	6
Gender		
Male	49	49
Female	49	49
Non-binary	2	2
Education		
High School or below	14	14
Undergraduate / Bachelor's Degree	35	35
Postgraduate / Master's Degree	34	34

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Characteristic / category	n	%
Professional Degree (e.g., CA, LLB, MBBS)	10	10
Doctorate / Ph.D	7	7
Occupation		
Salaried / Employed (Private sector)	41	41
Salaried / Employed (Public / Government sector)	17	17
Self-employed / Business Owner	16	16
Student	10	10
Homemaker	5	5
Retired	7	7
Other	4	4
Monthly household income		
Less than ₹30,000	14	14
₹30,000 – ₹75,000	38	38
₹75,001 – ₹1,50,000	30	30
More than ₹1,50,000	8	8
Prefer not to say	10	10

The simulated sample is spread across all age groups (26–35 years: 33%; 18–25: 21%; 36–50: 21%; 51–65: 19%; above 65: 6%) and is 49% male, 49% female and 2% non-binary. Undergraduate (35%) and postgraduate (34%) degrees are the most common education levels, private-sector employees the largest occupational group (41%), and household income is concentrated in the ₹30,000–₹75,000 band (38%); 10% preferred not to disclose income. The profile is deliberately varied rather than representative of the national customer base.

7.2 Reliability and Descriptive Analysis

Table 3. Reliability and descriptive statistics of construct scores (n = 100)

Construct	Items	Mean	SD	Median	% ≥ 3.5	α	t (vs 3)	p
DPDP Awareness	5	3.51	.81	3.6	52	.80	6.26	< .001
Data Privacy Practices	4	3.29	.81	3.2	43	.75	3.57	< .001
Cybersecurity Practices	5	3.30	.86	3.2	42	.84	3.42	< .001
Consent & Data Control	4	3.10	.83	3.2	40	.80	1.23	.221
Perceived Data Security	4	3.46	.85	3.5	54	.80	5.49	< .001
Customer Trust	4	3.42	.85	3.5	53	.80	5.00	< .001
Continued Digital Usage	4	3.75	.81	3.8	73	.79	9.19	< .001

Scores are item means on a 1–5 scale. % ≥ 3.5 = share of respondents with a favourable construct score. t is a one-sample test against the scale mid-point (3), df = 99.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

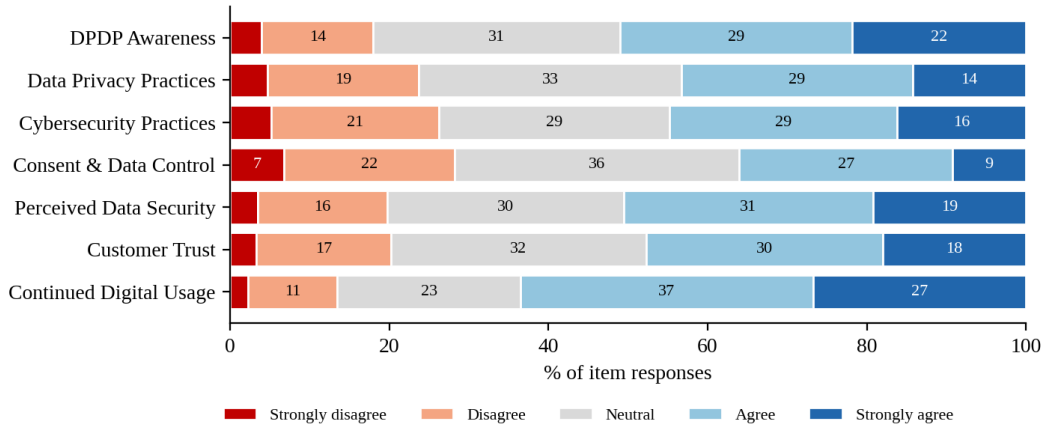


Figure 2. Distribution of item responses by construct (% of responses),

All seven scales exceed the conventional .70 threshold (α = 0.75–0.84), so composite scores are used. Mean scores are highest for continued digital usage (M = 3.75) and awareness (M = 3.51), and lowest for consent and data control (M = 3.10), which does not differ significantly from the neutral point (p = .221). Privacy practices (M = 3.29) and cybersecurity practices (M = 3.30) are rated only slightly above neutral. In the simulated data, therefore, customers lean towards continued use and some awareness, but are ambivalent about how well institutions explain data use and give them control. Figure 2 shows that agree and strongly agree responses are most frequent for usage (64% of responses), whereas neutral or disagreeing responses make up 65% of answers on consent items and 57% on privacy items.

7.3 Level of Awareness of DPDP act(Objective1)

Table 4. Item-level DPDP awareness (n = 100)

Awareness item	Mean	SD	% Agree (4–5)	% Disagree (1–2)
Aware of organisations' obligations to protect data	3.58	1.07	54	16
Aware of own data rights	3.45	1.18	53	23
Understand why institutions collect data	3.70	1.02	56	12
Aware of the right to seek information	3.61	1.02	51	12
Aware of grievance mechanisms	3.20	1.15	41	27

Overall awareness is moderate to high (M = 3.51, SD = .81); 52% of respondents have a high awareness score (≥ 3.5), 36% a moderate score (2.5 to below 3.5) and 12% a low score (< 2.5). Item results (Table 4) show that agreement is highest for understanding why institutions collect personal data and lowest for awareness of grievance mechanisms, the most procedural of the rights. Awareness differs by age group (Kruskal–Wallis H = 12.82, p = .012): respondents aged 26–35 score highest (M = 3.78) and those aged 51–65 lowest (M = 3.02). No significant differences were found by education (p = .359), occupation (p = .867), income (p = .915) or gender (p = .470). Objective 1 is thus met: in the simulated sample, awareness is generally moderate to high but weaker among older customers.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

7.4 Correlation Analysis

Table 5. Pearson correlations among construct scores (n = 100)

Construct	1	2	3	4	5	6	7
1 Awareness	1						
2 Privacy	.12	1					
3 Cybersec.	.33***	.22*	1				
4 Consent	.15	.26**	.17	1			
5 Security	.34***	.42***	.47***	.23*	1		
6 Trust	.09	.33***	.47***	.27**	.41***	1	
7 Usage	.12	.08	.14	.16	.16	.43***	1

** p < .05, ** p < .01, *** p < .001 (two-tailed). 1 Awareness, 2 Privacy, 3 Cybersecurity, 4 Consent/control, 5 Perceived security, 6 Trust, 7 Continued use.*

All correlations are positive. Perceived data security correlates most strongly with cybersecurity practices (r = .47) and privacy practices (r = .42), and trust correlates with cybersecurity practices (r = .47), perceived security (r = .41) and continued use (r = .43). Awareness is related to perceived security (r = .34) and cybersecurity practices but only weakly to trust (r = .09) and continued use (r = .12). The pattern matches the sequential logic of the model: associations are stronger between adjacent stages than between distant ones. No pair of predictors exceeds r = .50, and all variance inflation factors in the regressions are below 1.2, so multicollinearity is not a concern. Correlations do not imply causation.

7.5 Regression Analysis and Results of H11 to H16

Table 6. Multiple regression results (n = 100)

Predictor	B	SE	β	t	p
Model 1. DV: Perceived data security (H11–H13)	*R^2 = .36, adj. R^2 = .34, F(3, 96) = 17.70, p < .001*				
DPDP Awareness	.19	.09	.18	2.10	.039
Data Privacy Practices	.34	.09	.32	3.84	< .001
Cybersecurity Practices	.33	.09	.34	3.83	< .001
Model 2. DV: Customer trust (H14–H15)	*R^2 = .20, adj. R^2 = .18, F(2, 97) = 11.95, p < .001*				
Consent & Data Control	.18	.09	.18	1.93	.057
Perceived Data Security	.37	.09	.37	3.92	< .001
Model 3. DV: Continued digital usage (H16)	*R^2 = .19, adj. R^2 = .18, F(1, 98) = 22.34, p < .001*				
Customer Trust	.41	.09	.43	4.73	< .001

B = unstandardised coefficient; β = standardised coefficient; merged panel rows give model fit. 95% confidence intervals and VIFs are in the Excel file (Analysis_Results).

Model 1 explains 35.6% of the variance in perceived data security (adjusted R^2 = .34) and is significant. Data privacy practices (B = .34, β = .32, p < .001) and cybersecurity practices (B = .33, β = .34, p < .001) are the strongest predictors, and DPDP awareness has a smaller but significant effect (B = .19, β = .18, p = .039, 95% CI [.01, .37]). H11, H12 and H13 are therefore supported. Awareness appears to matter less than the institution's visible conduct, which fits the view that customers judge security mainly on what organisations actually do.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Model 2 explains 19.8% of the variance in trust. Perceived data security is a significant predictor (B = .37, β = .37, p < .001), supporting H15. Consent and data control has a positive coefficient (B = .18, β = .18) that is marginally non-significant at α = .05 (p = .057, 95% CI [−.01, .37]), although its simple correlation with trust is significant (r = .27). H14 is therefore not supported at the 5% level in the multivariable model; the effect is in the expected direction and may be partly absorbed by perceived security, since consent practices also raise perceived security (r = .23). With n = 100, power to detect an effect of this size is limited. Model 3 shows that trust explains 18.6% of the variance in continued use (B = .41, β = .43, p < .001); H16 is supported.

7.6 Mediation Analysis (H17 to H18)

Table 7. Bootstrap mediation results (5,000 resamples; unstandardised coefficients)

Path	a	b	Total c	Direct c′ (p)	Indirect a×b	95% bootstrap CI
H17: Privacy → Security → Trust	.438	.329	.339	.194 (.066)	.144	[.049, .243]
H18: Security → Trust → Continued use	.407	.421	.153	−.019 (.845)	.171	[.075, .286]

a = effect of X on mediator; b = effect of mediator on outcome controlling for X; c = total effect; c′ = direct effect. An indirect effect is significant when the bootstrap CI excludes zero.

For H17, the indirect effect of data privacy practices on trust through perceived data security is .144 (95% CI .049 to .243; Sobel z = 2.67, p = .008). The total effect is significant (c = .339) and the direct effect is no longer significant once security is included (c′ = .194, p = .066), so the effect operates largely, and perhaps wholly, through perceived security; H17 is supported. For H18, the indirect effect of perceived security on continued use through trust is .171 (95% CI .075 to .286; Sobel z = 3.11, p = .002), while the direct effect is near zero (c′ = −.019, p = .845) and the total effect alone is not significant (c = .153, p = .113). Security thus influences usage only by building trust, an indirect-only pattern, and H18 is supported. Because the data are cross-sectional and simulated, mediation here describes statistical consistency with the model, not proof of a causal sequence.

7.7 Summary of Hypothesis Results

Table 8. Summary of hypothesis testing (simulated data)

H	Relationship	Result	Decision
H11	Awareness → Perceived security	β = .18, p = .039	Supported
H12	Privacy practices → Perceived security	β = .32, p < .001	Supported
H13	Cybersecurity practices → Perceived security	β = .34, p < .001	Supported
H14	Consent/data control → Trust	β = .18, p = .057	Not supported at α = .05 (marginal)
H15	Perceived security → Trust	β = .37, p < .001	Supported
H16	Trust → Continued use	β = .43, p < .001	Supported
H17	Security mediates Privacy → Trust	a×b = .144, CI [.049, .243]	Supported
H18	Trust mediates Security → Continued use	a×b = .171, CI [.075, .286]	Supported (indirect-only)

Decision rule: α = .05, two-tailed. Results illustrate the method on simulated data.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

8. Discussion

The simulated results show how the proposed chain would be read if the pattern held in real data. Visible institutional conduct, in the form of clear privacy practices and strong cybersecurity, carries the largest weight for perceived security, with awareness of the Act playing a smaller supporting part. Perceived security then feeds trust, and trust feeds continued use, with security acting on usage only through trust. The consent and data-control path is the weakest link; in the data the consent score is also the lowest-rated construct, so the result is consistent with consent mechanisms being the least developed in practice rather than the least important. Because the structural coefficients were specified in advance when creating the data, these patterns confirm the analytical procedure and not the theory. Whether real customers behave this way, and whether awareness remains secondary once the 2025 Rules are fully in force, is an empirical question for the field survey.

9. Key Findings

- Awareness of the DPDP Act is moderate to high (M = 3.51); 52% of respondents score high, and awareness is lowest among customers aged 51–65 and for the grievance-redress mechanism.
- Data privacy and cybersecurity practices are the strongest predictors of perceived data security (β = .32 and .34); awareness has a smaller effect (β = .18).
- Perceived data security significantly increases trust (β = .37), and trust significantly increases continued digital use (β = .43).
- Consent and data control is the lowest-rated area (M = 3.10) and its effect on trust is positive but marginal (p = .057).
- Perceived security affects trust and privacy practices affect trust largely through perceived security; security reaches continued use only through trust (indirect effects .144 and .171).
- Continued-use intention is high (M = 3.75), but fewer than half of respondents are clearly favourable on privacy practices (43%) and consent/data control (40%), leaving room for improvement.

10. Suggestions

- Make privacy notices short, layered and in plain language, with a one-screen summary of what data are collected and why, so that customers can see the privacy practice they are being asked to trust.
- Publish security measures customers can see: transaction alerts, authentication options, phishing advisories and breach-response commitments, and report on them regularly.
- Build granular consent dashboards (purpose-wise toggles, easy withdrawal) and prepare for consent managers, so that consent is experienced as real control rather than a click-through.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

- Run awareness campaigns on data-principal rights and grievance channels, targeted at older customers and at the least-known procedural rights.
- Use customer perception of security and trust as tracked indicators, since trust is the gateway to continued digital use.
- Regulators and industry bodies should issue practical guidance and sector templates for notices and consent, and monitor customer awareness as the Rules are phased in.

11. Limitation and Scope for Further Research

The principal limitation is that the data are simulated: every coefficient reflects the model used to generate the data, so no result may be generalised or cited as an empirical finding. Even with

real data, the design would be cross-sectional and self-reported, so mediation can only be consistent with, not proof of, causal order. The sample size (n = 100) limits the power of tests for small effects such as H14, and the combined bank-and-insurance sample does not allow a comparison between the two sectors. Future work should collect real responses through stratified sampling, test the measurement model with confirmatory factor analysis and structural equation modelling, compare banking and insurance, and repeat the survey after the full DPDP Rules take effect in 2027.

12. Conclusion

The study set out a conceptual model that links DPDP awareness, institutional privacy, cybersecurity and consent practices, perceived data security, customer trust and continued use

of digital financial services, together with six objectives and eight hypotheses. Applied to a simulated sample of 100 respondents with varied backgrounds, the analytical workflow produced the expected pattern: seven of the eight hypotheses were supported at the 5% level and one (H14) was marginal, with all constructs reliable and no multicollinearity concern. The main practical message is that customers appear to build trust through visible privacy and

security conduct, and that trust in turn sustains digital use. The numerical results are illustrative; they provide a template to be rerun on genuine survey data before the model is accepted or

used to guide policy.

References

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.

Government of India. (2023). The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). Ministry of Electronics and Information Technology.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), 709–734.

Ministry of Electronics and Information Technology. (2025). The Digital Personal Data Protection Rules, 2025 (notified 14 November 2025).

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. Journal of Marketing, 58(3), 20–38.

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and compari

(This work is licensed under a Creative Commons Attribution 4.0 International License.)