International Journal of Economic Practices and Theories (IJEPT)
ISSN: 2247-7225
Volume 2026, Issue 1

Beyond Access: Cybersecurity Assurance and the Access–Assurance Asymmetry in Sustainable Digital Financial Participation—A PLS-SEM Study

Shreya Srinate[1], Anil Kumar[2], Prof. Leena Sharad Shimpi[3] & Prof. Amit Kumar Singh[4]

Research Scholar[1 & 2], Department of Commerce, Babasaheb Bhimrao Ambedkar University, Lucknow

Supervisor/Professor[3], Department of Commerce, Babasaheb Bhimrao Ambedkar University, Lucknow

Professor[4], Department of Management Studies, Babasaheb Bhimrao Ambedkar University, Lucknow

Corresponding author: Shreya Srinate

Abstract:

Digital access does not necessarily produce sustained digital financial participation when users remain uncertain about security, privacy and redress. This study compares the associations of Digital Financial Inclusion Readiness (DFIR) and Cybersecurity Assurance (CA) with Sustainable Digital Adoption Behaviour (SDAB) among 123 digitally active financial-service users recruited across six districts of Uttar Pradesh, India. A reflective PLS-SEM was estimated in SmartPLS 4 and assessed with 5,000-subsample, two-tailed BCa bootstrapping. Indicator loadings ranged from .748 to .910, composite reliability from .929 to .953 and average variance extracted from .685 to .772. Together, DFIR and CA explained 71.9% of SDAB variance. CA had a large, statistically supported association with SDAB (β=.667, t=5.143, p<.001), whereas DFIR did not make a statistically reliable unique contribution in the bootstrapped PLS model (β=.215, t=1.569, p=.117). A construct-mean regression reproduced the ordering but yielded a significant DFIR coefficient, making that smaller path method-sensitive. The CA–SDAB HTMT value of .910, evidence of invariant responding and same-source measurement further limit interpretation. The results therefore support cybersecurity assurance as the more consistent correlate of post-access participation in this sample, not as a universal or causal gatekeeper. The study develops a broadly applicable access–assurance perspective while identifying measurement and sampling requirements for confirmatory research in other populations.

Keywords: Digital financial inclusion; Cybersecurity assurance; Digital banking; Post-access participation; PLS-SEM; India.

Introduction

Digital financial inclusion is entering a different phase. The first phase was largely about reach: opening accounts, extending connectivity, reducing transaction costs and making digital payment tools available to users who were poorly served by branch-based finance. The next phase is about durable use. A person can be formally included, own a smartphone, know how to make a payment and still retreat from digital finance after a suspicious transaction, a failed reversal, a privacy concern or an unresolved complaint. The central policy problem is therefore no longer simply whether people can enter a digital financial system, but whether they have enough confidence in that system to remain active within it.

India makes this distinction especially visible. The Reserve Bank of India's National Strategy for Financial Inclusion 2025–30 explicitly places greater emphasis on usage and quality while continuing to improve access, and it identifies trust, consumer protection and grievance redress as core elements of effective inclusion (Reserve Bank of India [RBI], 2026). The Global Findex 2025 likewise expands the measurement frontier beyond account ownership to digital connectivity and digital safety (World Bank, 2025). At the transaction level, UPI processed 23,658.35 million transactions worth ₹29,87,880.49 crore in July 2026, illustrating the scale at which inclusion and cybersecurity now intersect (National Payments Corporation of India [NPCI], 2026).

That scale changes the behavioural meaning of cybersecurity. Security is often treated as a backend technical function, but users experience it through visible cues: whether authentication feels dependable, whether personal

data appear protected, whether fraud warnings are credible, whether a failed payment is reversed promptly and whether there is an intelligible path to redress. In this sense, cybersecurity assurance is not merely a technical property. It is a behavioural signal that can influence willingness to rely on digital finance repeatedly. Cyber incidents and operational failures can therefore weaken inclusion even when access infrastructure remains intact (Bouveret, 2018; Aldasoro et al., 2020).

Technology-adoption research explains initial acceptance through usefulness, facilitating conditions, effort, social influence and habit (Venkatesh et al., 2003; Venkatesh et al., 2012). Continuance research adds a temporal distinction: using an information system once and continuing to rely on it are different decisions (Bhattacherjee, 2001). Mobile-banking studies identify usefulness, ease of use and perceived risk as important adoption antecedents (Alalwan et al., 2016), while evidence from young Indian consumers highlights perceived credibility and structural assurance (Priya et al., 2018). More recent Indian evidence also connects perceived risk, trust and satisfaction with sustained mobile-payment use (Yadav et al., 2024). Even so, financial-inclusion readiness and cybersecurity assurance are still rarely compared directly as conditions of post-access participation.

This paper addresses that gap with a parsimonious explanatory framework linking Digital Financial Inclusion Readiness (DFIR) and Cybersecurity Assurance (CA) to Sustainable Digital Adoption Behaviour (SDAB). Its contribution lies in comparing two policy logics within one model. The first emphasises access, usability and capability; the second emphasises the protective conditions that make continued reliance possible. The analysis evaluates their relative structural associations while keeping statistical inference, construct validity and response quality separate.

The relative pattern is described as Access–Assurance Asymmetry: within the fitted model and this sample, assurance has the larger and more statistically consistent association with the post-access outcome. This is a bounded comparative interpretation, not a causal or universal claim. The corresponding policy proposition is that digital financial inclusion should be evaluated as secure participation rather than access alone.

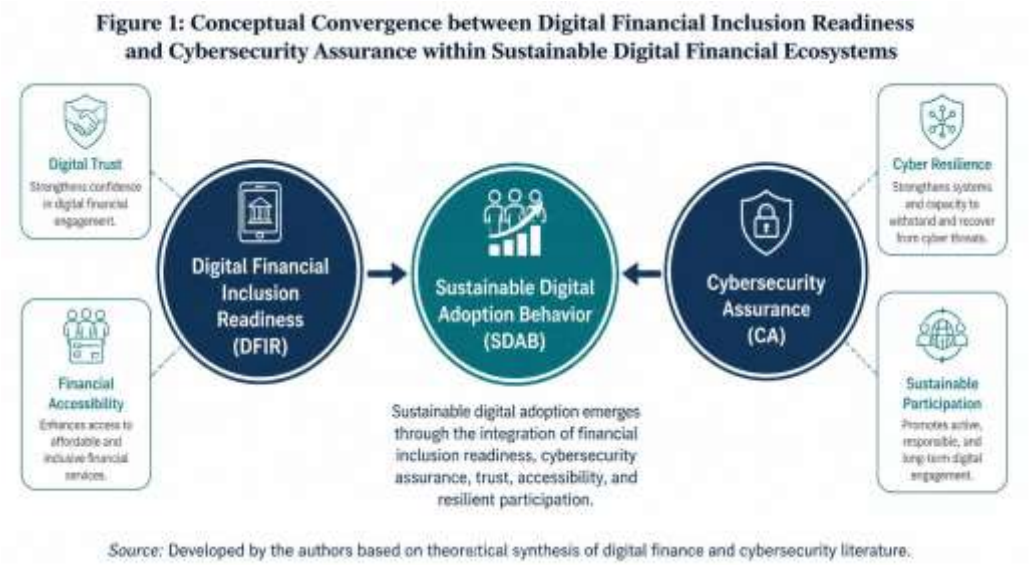


Figure 1. Conceptual convergence of digital financial inclusion readiness and cybersecurity assurance in sustainable digital participation.

Source: Authors' conceptual synthesis of the access–assurance perspective.

2. Conceptual Foundations and Hypotheses

2.1 Digital financial inclusion readiness: from access to usable participation

Digital financial inclusion extends financial access into a technology-mediated environment. Digital platforms

can reduce distance and transaction costs, widen service availability and connect users to payments, transfers, savings, credit and government benefits without requiring constant physical access to a branch (Ozili, 2018; Lee & Shin, 2018). Formal access, however, is not identical to practical readiness. A service can be available yet remain difficult to use because of limited familiarity, confidence, connectivity or perceived relevance.

DFIR therefore captures the user-side condition that makes participation feasible: convenient access, regular use, affordability, confidence in independent use, improved access to formal finance and awareness of available digital tools. This treatment is consistent with the facilitating-condition logic of UTAUT and with the growing digital-financial-literacy literature, which stresses that knowledge, skills and behaviour matter alongside connectivity and account ownership (Venkatesh et al., 2003; Lyons & Kass-Hanna, 2021; Koskelainen et al., 2023).

Readiness should support sustained use because it lowers everyday friction. Users who can access and navigate digital services are more likely to integrate those services into routine financial activity. The first hypothesis is therefore:

H1. Digital Financial Inclusion Readiness is positively associated with Sustainable Digital Adoption Behaviour.

2.2 Cybersecurity assurance: security as a behavioural institution

Cybersecurity assurance represents the confidence users derive from their understanding and experience of digital safeguards. It includes recognition of phishing, protection of credentials, software updating, avoidance of insecure networks, multi-factor authentication and awareness of fraud-reporting mechanisms. The construct differs from an engineering audit: it captures what users know and perceive about the protective environment in which they transact.

That distinction matters because digital financial exchange requires users to accept vulnerability. They cannot directly observe encryption, settlement architecture, fraud-detection algorithms or data-sharing arrangements. Instead, they infer dependability from institutional and technological signals. Institution-based trust research describes structural assurance as confidence that safeguards, legal structures and other protections make digital transactions dependable (McKnight et al., 2002). Cybersecurity assurance operationalises a related logic within the present digital-finance setting.

Perceived risk can suppress mobile-banking adoption even when usefulness is high (Alalwan et al., 2016). Studies of mobile payments further show that perceived security, risk and trust add explanatory value to technology-adoption models (Widyanto et al., 2022), while structural assurance has been linked to mobile-banking adoption among young Indian consumers (Priya et al., 2018). Cyber risk is also recognised as an operational and financial-stability concern (Bouveret, 2018; Aldasoro et al., 2020). The second hypothesis is therefore:

H2. Cybersecurity Assurance is positively associated with Sustainable Digital Adoption Behaviour.

2.3 Sustainable digital adoption behaviour

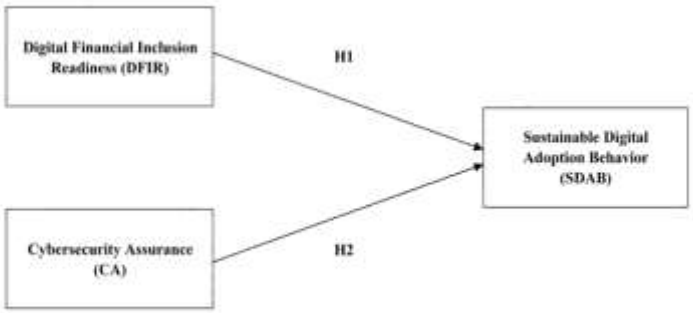
SDAB is used as a post-access orientation reflecting confidence, preference, perceived reliability and recommendation of digital financial services. It should not be interpreted as directly observed transaction behaviour. This distinction follows continuance research separating initial adoption from continued reliance (Bhattacherjee, 2001). Several SDAB items also contain security- and trust-related wording; consequently, the construct is conceptually close to CA. The resulting discriminant-validity limitation is treated as a boundary on interpretation rather than as a satisfactory measurement result.

2.4 Access–Assurance Asymmetry as the focal contribution

The two antecedents operate on different sides of the same participation decision. DFIR reduces the practical friction of entering and using the ecosystem, whereas CA addresses the perceived danger of relying on it. The framework therefore compares their unique structural associations without assuming in advance that either condition must dominate. A larger coefficient is interpreted only in conjunction with bootstrap uncertainty and construct-validity evidence.

The term Access–Assurance Asymmetry is used as a descriptive theoretical lens, not as a new statistical estimator. It refers to a situation in which two enabling conditions show similarly respectable performance levels, yet one exhibits substantially greater structural and strategic importance for continued use. This is especially relevant in mature or rapidly scaling digital-payment environments, where marginal policy value may shift from additional access toward dependable protection, recovery and trust.

Figure 2: Proposed Research Framework



Source: Developed by the authors based on technology adoption, cybersecurity, and digital financial behavior literature.

Figure 2. Empirical research framework tested through PLS-SEM.

Source: Authors' original framework. DFIR and CA are modelled as exogenous antecedents of SDAB.

3. Research Methodology

3.1 Design, data source and analytical sample

The study uses a quantitative, cross-sectional survey design. The unit of analysis is the individual user of digitally enabled financial services. The questionnaire captured demographic and usage characteristics, financial-inclusion conditions, cybersecurity knowledge and practices, and the focal reflective indicators used in the PLS-SEM model.

Responses to the focal constructs were recorded on five-point agreement scales.

The final empirical analysis uses 123 complete respondent records from multiple districts in Uttar Pradesh. The sample includes urban, semi-urban and rural users, but is concentrated in Lucknow and among younger, highly educated and digitally active respondents. Geography is therefore treated as the empirical setting rather than the theoretical boundary of the model, and no state-level or national representativeness is claimed. All reported respondent-based statistics use these same 123 records, with no missing values on the 18 focal indicators.

The final analytical file contains 123 records, each labelled observed. The item-level responses reproduce all three stored construct means exactly, and the SmartPLS import screen confirms 123 cases with no missing values.

Table 1. Profile of the analytical sample (n=123)

Characteristic	Category	n	%
District	Lucknow	93	75.6
District	Other districts	30	24.4
Area	Urban	89	72.4
Area	Semi-urban	17	13.8
Area	Rural	17	13.8
Gender	Male	80	65.0

Characteristic	Category	n	%
Gender	Female	43	35.0
Age group	18-25	83	67.5
Age group	26-35	36	29.3
Age group	Other	4	3.3
Education	Postgraduate or higher	64	52.0
Education	Graduate	52	42.3
Education	Class 12 or below	7	5.7
UPI use	Yes	120	97.6
Internet banking	Yes	108	87.8

Note: Percentages are based on the final empirical sample of 123 respondents.

3.2 Sample-size justification

Sample adequacy was assessed through statistical power and a PLS-SEM-specific minimum-sample check rather than the ten-times rule. The most complex endogenous equation contains two predictors of SDAB. Under a noncentral-F multiple-regression approximation, α=.05, power=.80 and a small-to-moderate planning effect of f^2=.10 require approximately 100 observations (Cohen, 1988). With n=123, achieved power is approximately .883 and the 80% sensitivity point is $f^2 \approx .080$. As a second check, the inverse-square-root method proposed by Kock and Hadaya (2018), using a conservative anticipated minimum path of β_min=.20, gives n=100. The sample therefore meets the stated planning assumptions for the parsimonious two-predictor model, although the non-significant DFIR path remains imprecisely estimated.

Calculation uses a noncentral-F approximation for the two-predictor endogenous equation. The analysis does not use the ten-times rule as the primary justification.

3.3 Construct operationalisation

The empirical model contains three reflectively specified constructs with six indicators each. Appendix A reproduces the complete wording used for DFIR, CA and SDAB. Reflective estimation is retained for consistency with the analysed SmartPLS specification, while the heterogeneous content of SDAB and its proximity to CA are explicitly considered when interpreting construct validity.

Table 3. Construct specification used in the empirical PLS-SEM

Construct	Role	Indicative content	Items
Digital Financial Inclusion Readiness (DFIR)	Exogenous	Access, regular use, affordability, independent-use confidence, access to formal finance, awareness of tools	6
Cybersecurity Assurance (CA)	Exogenous	Phishing recognition, credential protection, updates, safe networks, multi-factor authentication, fraud reporting	6
Sustainable Digital Adoption Behaviour (SDAB)	Endogenous	Confidence, data protection, reliability/accessibility, preference, institutional initiatives, recommendation	6

All constructs are estimated reflectively. Security-related wording in SDAB creates potential overlap with CA and is evaluated through HTMT.

3.4 Why PLS-SEM was used

PLS-SEM was selected because the model contains multiple-indicator latent constructs and the research question concerns their relative associations with explained variance in a post-access outcome. The method permits joint evaluation of the measurement model and structural relationships. It is not justified merely by sample size. The reported sequence covers indicator reliability, internal consistency, convergent validity, discriminant validity, path estimates, bootstrap inference and R^2 (Hair et al., 2022; Henseler et al., 2015).

SmartPLS 4 was used to estimate the reflective measurement and structural models. Statistical inference used 5,000 bootstrap subsamples, a two-tailed test, a .05 significance level and bias-corrected and accelerated (BCa) bootstrapping with a fixed random seed. We report the original estimates, bootstrap means, standard deviations, t statistics and p values generated by that run. A construct-mean regression and response-quality sensitivity analysis were used only as supplementary checks; hypothesis decisions follow the bootstrapped PLS results.

3.5 Ethics and response quality

Participation was voluntary, responses were used for academic research and no personally identifiable financial information is reported. The analytical file contains no missing focal responses and all 123 cases are labelled observed. Thirteen respondents selected the same scale point for all 18 focal items; these cases were retained because response time and attention-check fields were not available to justify selective deletion. A sensitivity analysis excluding them is reported in Section 4.4. The applicable institutional ethics approval or exemption status must be confirmed from the study records before journal submission.

4. Results

4.1 Indicator reliability and measurement model

The SmartPLS model shows loadings above the commonly used .70 reference point for all 18 indicators. DFIR loadings range from .828 to .910; CA loadings range from .815 to .870; and SDAB loadings range from .748 to .894. These values indicate that the indicators contribute meaningfully to their intended constructs.

Table 4. Indicator loadings from the SmartPLS model

Indicator	Construct	Outer loading
DFIR1	DFIR	0.865
DFIR2	DFIR	0.910
DFIR3	DFIR	0.906
DFIR4	DFIR	0.885
DFIR5	DFIR	0.828
DFIR6	DFIR	0.875
CA1	CA	0.870
CA2	CA	0.838
CA3	CA	0.815

Indicator	Construct	Outer loading
CA4	CA	0.843
CA5	CA	0.840
CA6	CA	0.855
SDAB1	SDAB	0.894
SDAB2	SDAB	0.829
SDAB3	SDAB	0.748
SDAB4	SDAB	0.821
SDAB5	SDAB	0.795
SDAB6	SDAB	0.870

Source: Authors' SmartPLS 4 measurement-model output.

Internal-consistency and convergent-validity statistics are strong across the three constructs. Cronbach's alpha ranges from .907 to .941, rho_A from .913 to .942 and composite reliability from .929 to .953. AVE values range from .685 to .772, all above .50. The high composite reliability for DFIR (.953) should be read as evidence of consistency while also inviting attention to possible item redundancy in future scale refinement.

Table 5. Reliability and convergent validity

Construct	Cronbach's α	rho_A	Composite reliability	AVE
SDAB	.907	.913	.929	.685
CA	.919	.921	.937	.712
DFIR	.941	.942	.953	.772

Source: Authors' SmartPLS 4 analysis. Reliability and AVE interpretation follows Hair et al. (2022).

4.2 Discriminant validity and construct-boundary assessment

HTMT indicates acceptable separation for DFIR–SDAB (.799) and CA–DFIR (.852) under the .90 criterion. CA–SDAB is .910, however, and therefore does not establish discriminant validity under the stricter threshold. This result is substantively consistent with the item wording: CA captures cybersecurity knowledge and protective practices, while multiple SDAB items refer to security, data protection, safety and trusted infrastructure. The CA–SDAB association may consequently be strengthened by shared content as well as by a genuine substantive relationship. Results involving these two constructs are therefore treated as exploratory and interpreted cautiously (Henseler et al., 2015).

Table 6. HTMT discriminant-validity assessment

Construct pair	HTMT	Assessment
CA – DFIR	.852	Below .90; acceptable with conventional criterion
CA – SDAB	.910	Borderline/high; explicit construct-boundary caution required
DFIR – SDAB	.799	Below .90; acceptable

Future confirmatory research should remove security, privacy and trust wording from the continuance outcome and report bootstrapped HTMT confidence intervals.

4.3 Structural model

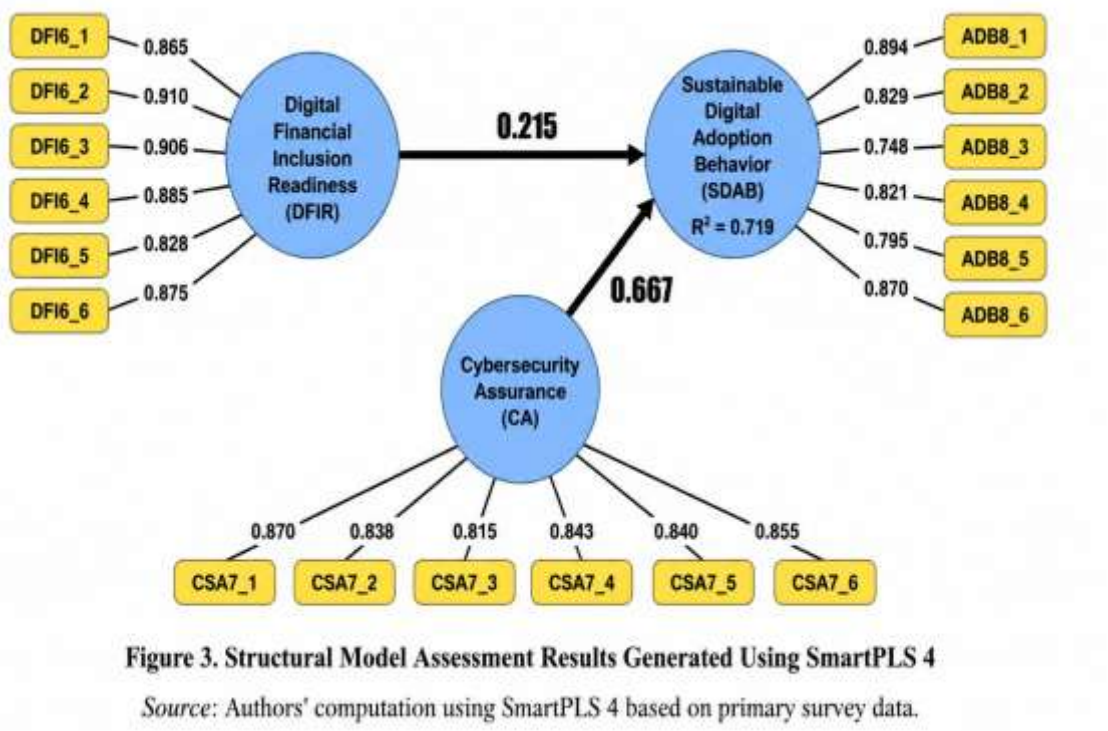


Figure 3. Structural Model Assessment Results Generated Using SmartPLS 4

Source: Authors' computation using SmartPLS 4 based on primary survey data.

Figure 3. SmartPLS 4 structural model and indicator loadings.

Source: Authors' SmartPLS 4 output. The model reports R^2=.719 for SDAB.

The fitted model explains 71.9% of SDAB variance (R^2=.719). CA has a positive and statistically supported association with SDAB (β=.667, t=5.143, p<.001). DFIR has a smaller positive estimate, but its bootstrap result is not statistically significant (β=.215, t=1.569, p=.117). H2 is therefore supported, whereas H1 is not supported by the primary PLS-SEM inference.

The bootstrap standard deviation for DFIR (.137) is large relative to its coefficient, which explains why the positive estimate is not statistically distinguishable from zero. CA has a smaller relative bootstrap uncertainty (SD=.130) and remains strongly supported. The difference between the PLS decision for H1 and the later composite-score regression is treated as method sensitivity rather than resolved in favour of the significant result.

Table 7. Bootstrapped structural paths

Hypothesis / relationship	Original β	Bootstrap M (SD); t; p	Decision
H1: DFIR → SDAB	.215	.238 (.137); 1.569; .117	Not supported
H2: CA → SDAB	.667	.646 (.130); 5.143; <.001	Supported

Note: Hypothesis decisions follow the SmartPLS bootstrap output; the composite-score regression is supplementary.

4.4 Robustness and response-quality sensitivity

A supplementary multiple regression entered the three construct means for the same 123 respondents. Predictor VIFs were 2.701. The model was significant, $F(2,120)=144.6$, $p<.001$, with $R^2=.707$ and adjusted $R^2=.702$. Standardized coefficients reproduced the ordering: DFIR $\beta=.212$ ($t=2.613$, $p=.010$) and CA $\beta=.662$ ($t=8.150$, $p<.001$). Excluding the 13 invariant responders reduced R^2 to .613; CA remained substantial ($\beta=.632$, $p<.001$), while DFIR was smaller ($\beta=.190$, $p=.035$). In a 5,000-resample bootstrap of this reduced composite-score model, the DFIR percentile interval crossed zero, whereas the CA interval remained positive. Thus, the assurance result is robust to this screening choice, but the readiness result is not. A Harman single-factor diagnostic found that the first unrotated factor explained 62.1% of item variance. Because this diagnostic is limited, it is interpreted only as a warning that common-method variance may be present, not as a correction for it (Podsakoff et al., 2003).

Table 8. Composite-score robustness and sensitivity checks

Analysis	DFIR result	CA result	Model fit / interpretation	Purpose
All cases (n=123)	β=.212; p=.010	β=.662; p<.001	$R^2=.707$; Adj. $R^2=.702$	Composite-score comparison
Invariant responses excluded (n=110)	β=.190; p=.035	β=.632; p<.001	$R^2=.613$	Response-quality sensitivity
Reduced-sample bootstrap (5,000)	95% percentile CI [−.024, .562]	95% percentile CI [.283, .811]	Ordering retained	Uncertainty sensitivity
Common-method diagnostic	First unrotated factor	62.1% of variance	Potential common-method influence	Diagnostic, not a correction

Note: The robustness model uses construct means and conventional OLS inference. It corroborates the ordering of effects but does not replace the original SmartPLS bootstrap output.

5. Discussion

The findings suggest that access readiness and cybersecurity assurance play different roles in post-access digital participation. DFIR is positively related to SDAB at the bivariate level, but it does not make a statistically reliable unique contribution in the bootstrapped PLS model once CA is included. CA shows the larger and more consistent path estimate. Because CA and SDAB share security-related content, that magnitude should not be interpreted as

a pure causal effect of cybersecurity assurance.

A cautious two-stage interpretation is nevertheless useful. Readiness concerns whether users can participate with reasonable convenience, affordability and confidence. Assurance concerns whether they feel sufficiently protected to rely on the channel. This interpretation complements UTAUT and continuance theory, but the present cross-sectional evidence cannot establish temporal ordering (Venkatesh et al., 2003; Venkatesh et al., 2012; Bhattacherjee, 2001).

The results also encourage a broader policy treatment of cybersecurity. Authentication, privacy controls, fraud warnings and redress processes are experienced by users as part of the service environment, not merely as backend technical controls. Indian evidence linking structural assurance with mobile-banking adoption (Priya et al., 2018) and perceived risk with sustained mobile-payment use (Yadav et al., 2024) supports this interpretation.

This reading is closely aligned with the policy direction of RBI's NSFI 2025–30, which places usage and quality alongside access and links customer protection and grievance redress with trust in formal financial services (RBI, 2026). It is also consistent with the Global Findex 2025 decision to collect globally comparable digital-safety measures alongside financial-inclusion indicators (World Bank, 2025). The empirical model therefore sits within a broader shift in the definition of inclusion—from counting entry points toward assessing whether users can transact safely, repeatedly and with confidence.

The HTMT=.910 result remains the central qualification. It indicates that the measured forms of CA and SDAB are not cleanly separated under the strict .90 criterion. The study therefore contributes an exploratory comparative pattern and a measurement agenda; it does not establish that cybersecurity assurance is universally or causally dominant over access readiness.

6. Theoretical Contributions

First, the study places access readiness and cybersecurity assurance within one post-access model. This integration moves beyond treating financial inclusion and cybersecurity as separate policy domains while remaining parsimonious.

Second, the Access–Assurance Asymmetry perspective focuses attention on comparative explanatory relevance rather than the binary question of whether cybersecurity matters. In this sample, the bootstrapped structural paths rank CA above DFIR, and only the CA path is statistically supported. The construct-overlap caveat remains central.

Third, the study extends post-adoption discussion by treating continued digital participation as distinct from initial access. Its evidence suggests that protective assurance deserves explicit consideration in continuance-oriented models of digital finance.

Fourth, the analysis shows why statistical significance, coefficient magnitude and construct validity must be considered together. A large R^2 does not substitute for discriminant validity, response-quality evidence or a representative sampling design.

7. Policy and Managerial Implications

7.1 From access-first to secure-by-design inclusion

For regulators and financial-inclusion programmes, access expansion should continue, but it should no longer be evaluated independently of safe use. Inclusion dashboards can incorporate active usage, transaction confidence, fraud exposure, complaint resolution and knowledge of recovery channels alongside account ownership and access points. This direction is consistent with RBI's emphasis on usage, quality, customer protection and grievance redress (RBI, 2026).

7.2 Cybersecurity as customer experience

Banks and fintech platforms should treat authentication, transaction alerts, privacy controls, fraud reporting and reversal processes as visible customer-experience features. A security control that is technically strong but confusing, inaccessible or poorly communicated may not create behavioural assurance. Conversely, clear risk

communication and reliable recovery can strengthen confidence without weakening usability.

7.3 A practical priority rule

For comparable digitally active user groups, the results support a conditional management rule: continue improving readiness where access or capability is weak, while giving explicit attention to visible safeguards, fraud response and redress. This sample-specific pattern does not justify reducing financial-literacy or access programmes.

7.4 Digital financial literacy should include recovery literacy

Digital-financial-literacy programmes often focus on how to transact. The cybersecurity items show why users also need to know how to recognise phishing, protect credentials, avoid insecure connections, use multi-factor authentication and report fraud. OECD guidance increasingly frames digital financial literacy as a combination of knowledge, skills, attitudes and behaviours required for safe digital-finance use (OECD, 2025). A secure-inclusion agenda should therefore teach both transaction capability and recovery capability.

8. Robustness, Reporting Boundaries and Research Integrity

Four reporting boundaries guide interpretation. First, all empirical results refer to the same 123 observed respondent records. Second, hypothesis decisions follow the 5,000-subsample SmartPLS bootstrap output. Third, the CA–SDAB HTMT result prevents an unqualified claim of discriminant validity. Fourth, invariant response patterns and the same-source design require caution even though the assurance association survives the reported sensitivity analysis.

The close correspondence between PLS and OLS coefficients strengthens confidence in the relative ordering, but the different inferential decision for DFIR shows that small effects are specification-sensitive. Neither method eliminates same-source measurement effects or security-related item overlap. The clean empirical dataset, questionnaire, consent documentation and complete SmartPLS project should accompany the reproducibility archive.

We make no out-of-sample predictive claim because that assessment was not part of the documented analysis.

9. Limitations and Future Research

The cross-sectional, same-source design limits temporal and causal interpretation and may inflate associations through common-method processes. Future research should use temporally separated measurement or behavioural records and prespecified procedural and statistical controls for common-method bias.

The measurement boundary between CA and SDAB requires redesign. CA should distinguish user cybersecurity knowledge and practices from perceived institutional safeguards; a continuance outcome should contain no security, privacy, trust or reliability wording. Trust can then be modelled separately as a mechanism connecting assurance with continuance. The 123-case sample is adequate for the parsimonious model under the stated planning assumptions but is less sensitive to small unique effects. It is also concentrated in Lucknow, urban respondents, younger users and graduates. Generalisation beyond similarly digitally active users is therefore inappropriate. A confirmatory replication should use probability-based or carefully stratified recruitment where feasible and determine its target sample from a preregistered smallest effect of substantive interest.

Future studies should test whether digital trust mediates the relationship between assurance and continuance and whether perceived cyber risk conditions that relationship. These extensions should be prespecified and estimated only after establishing measurement separation and adequate power.

Out-of-sample assessment should report repeated k-fold PLSpredict settings and indicator-level PLS-versus-LM RMSE and MAE. Multi-group comparisons should follow measurement-invariance testing and adequate subgroup sizes.

10. Conclusion

Digital financial inclusion is more durable when users can participate conveniently and perceive the service

environment as dependable. In this sample, CA has the larger and statistically supported PLS path to the post-access outcome; DFIR is positive but not significant in the primary bootstrap analysis. The model explains 71.9% of SDAB variance, and supplementary analyses preserve the relative ordering. These results support an access–assurance interpretation, but the CA–SDAB HTMT=.910, invariant response patterns and cross-sectional same-source design require restraint. The evidence identifies a robust sample association; it does not establish causal gatekeeping or universal dominance. The policy implication is that access expansion and secure participation should be developed together. Authentication, privacy protection, fraud prevention, customer communication and effective redress can be treated as components of inclusive service design. A stronger confirmatory study should use a larger and more diverse probability-based or stratified sample, cleaner construct boundaries, prespecified response-quality rules and longitudinal or behavioural outcomes.

References

[1] Aldasoro, I., Frost, J., Gambacorta, L., Leach, T., & Whyte, D. (2020). Cyber risk in the financial sector. SUERF Policy Note No. 206. https://www.suerf.org/publications/suerf-policy-notes-and-briefs/cyber-risk-in-the-financial-sector/

[2] Alalwan, A. A., Dwivedi, Y. K., Rana, N. P. P., & Williams, M. D. (2016). Consumer adoption of mobile banking in Jordan: Examining the role of usefulness, ease of use, perceived risk and self-efficacy. Journal of Enterprise Information Management, 29(1), 118–139. https://doi.org/10.1108/JEIM-04-2015-0035

[3] Bhattacherjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. MIS Quarterly, 25(3), 351–370. https://doi.org/10.2307/3250921

[4] Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. IMF Working Paper 18/143. International Monetary Fund. https://doi.org/10.5089/9781484360750.001

[5] Cohen, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.). Lawrence Erlbaum Associates. https://doi.org/10.4324/9780203771587

[6] Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). A primer on partial least squares structural equation modeling (PLS-SEM) (3rd ed.). Sage. https://us.sagepub.com/en-us/nam/a-primer-on-partial-least-squares-structural-equation-modeling-pls-sem/book270548

[7] 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

[8] Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. Information Systems Journal, 28(1), 227–261. https://doi.org/10.1111/isj.12131

[9] Koskelainen, T., Kalmi, P., Scornavacca, E., & Vartiainen, T. (2023). Financial literacy in the digital age—A research agenda. Journal of Consumer Affairs, 57(1), 507–528. https://doi.org/10.1111/joca.12510

[10] Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. Business Horizons, 61(1), 35–46. https://doi.org/10.1016/j.bushor.2017.09.003

[11] Lyons, A. C., & Kass-Hanna, J. (2021). A methodological overview to defining and measuring 'digital' financial literacy. Financial Planning Review, 4(2), e1113. https://doi.org/10.1002/cfp2.1113

[12] 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

[13] National Payments Corporation of India. (2026). Unified Payments Interface (UPI) product statistics. https://www.npci.org.in/product/upi/product-statistics

[14] OECD. (2025). Supporting informed and safe use of digital payments through digital financial literacy.

OECD Publishing. https://www.oecd.org/en/publications/supporting-informed-and-safe-use-of-digital-payments-through-digital-financial-literacy_21de47d1-en/full-report.html

[15] Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. Borsa Istanbul Review, 18(4), 329–340. https://doi.org/10.1016/j.bir.2017.12.003

[16] Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. Journal of Applied Psychology, 88(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

[17] Priya, R., Gandhi, A. V., & Shaikh, A. (2018). Mobile banking adoption in an emerging economy: An empirical analysis of young Indian consumers. Benchmarking: An International Journal, 25(2), 743–762. https://doi.org/10.1108/BIJ-01-2016-0009

[18] Reserve Bank of India. (2026). National Strategy for Financial Inclusion 2025–30. https://www.rbi.org.in/commonman/Upload/English/Content/PDFs/English12052026.pdf

[19] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478. https://doi.org/10.2307/30036540

[20] 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

[21] Widyanto, H. A., Kusumawardani, K. A., & Yohanes, H. (2022). Safety first: Extending UTAUT to better predict mobile payment adoption by incorporating perceived security, perceived risk and trust. Journal of Science and Technology Policy Management, 13(4), 952–973. https://doi.org/10.1108/JSTPM-03-2020-0058

[22] World Bank. (2025). The Global Findex Database 2025: Connectivity and financial inclusion in the digital economy. https://www.worldbank.org/en/publication/globalfindex/report

[23] Yadav, P., Kumar, A., Mishra, S. K., & Kochhar, K. (2024). Financial equality through technology: Do perceived risks deter Indian women from sustained use of mobile payment services? International Journal of Information Management Data Insights, 4(2), 100266. https://doi.org/10.1016/j.jjimei.2024.100266

Declarations

Conflict of interest: The authors declare that they have no conflict of interest.

Funding: No external funding was received for this study.

Ethics statement: Participation was voluntary and confidentiality was maintained.

Appendix A. Full Focal Measurement Instrument

The complete measurement instrument is reported to support transparency. It also makes the principal measurement limitation visible: several SDAB items contain security- and trust-related language that is conceptually close to CA. Results involving these constructs should therefore be interpreted as exploratory until the measures are redesigned and validated in an independent sample.

Table A1. Six-item construct specification aligned with the SmartPLS model

Construct	Code	Measurement statement
DFIR	DFI 6.1	I have convenient access to digital financial services such as UPI apps, mobile banking, or internet banking.

Construct	Code	Measurement statement
DFIR	DFI 6.2	I regularly use digital financial services for transactions like payments, transfers, and bill payments.
DFIR	DFI 6.3	I find digital banking services affordable and economical to use.
DFIR	DFI 6.4	I feel confident in using digital financial services without any external help.
DFIR	DFI 6.5	Digital financial services have improved my access to formal banking and government benefit schemes.
DFIR	DFI 6.6	I am aware of various digital financial tools and services available to me (e.g., UPI, AEPS, mobile wallets).
CA	CSA 7.1	I understand what phishing is and can recognize suspicious messages or emails.
CA	CSA 7.2	I know not to share my OTP, PIN, or CVV with anyone, even if requested by someone claiming to be from my bank.
CA	CSA 7.3	I regularly update my financial apps and operating system on my smartphone or computer.
CA	CSA 7.4	I avoid using public Wi-Fi networks when conducting digital banking or financial transactions.
CA	CSA 7.5	I use multi-factor authentication (such as OTP plus PIN or biometric login) on my banking or UPI apps.
CA	CSA 7.6	I am aware of and know how to report cyber fraud (e.g., phishing, transaction failure) to banks or cybercrime helplines.
SDAB	ADB 8.1	I feel confident using digital banking services because they are secure and easy to use.
SDAB	ADB 8.2	I believe digital banking platforms protect my personal and financial data effectively.

Construct	Code	Measurement statement
SDAB	ADB 8.3	Digital banking services are accessible and reliable even in rural or semi-urban areas.
SDAB	ADB 8.4	I prefer digital banking over physical banking due to its convenience and perceived safety.
SDAB	ADB 8.5	Government initiatives (e.g., UPI, Jan Dhan, Aadhaar) have made digital banking safer and more widely adopted.
SDAB	ADB 8.6	I would recommend digital banking to others because of its secure and trusted infrastructure.