

Article

Coping with Digital Risk in Urban Bangladesh: Fintech Adoption Across Different Levels of Usage Experience

M. Sirajul Islam ^{1,2,*} , Tawsif Shafayet Ali ³ , Suntu Kumar Ghosh ³  and Md. Mahfuz Ashraf ⁴

¹ Informatics Department, Örebro University School of Business, 70182 Örebro, Sweden

² Operations and Project Management Department, College of Business, Alfaisal University, Riyadh 11533, Saudi Arabia

³ Department of Business Administration, Northern University Bangladesh, Dhaka 1230, Bangladesh; ali.tawsif@gmail.com (T.S.A.); suntu_ghosh@yahoo.com (S.K.G.)

⁴ Higher Degree Research Coordinator, Barton Business School, Melbourne, VIC 3066, Australia; ashraf.mahfuz@gmail.com

* Correspondence: sirajul.islam@oru.se or sislam@alfaisal.edu

Abstract

Fintech adoption increasingly takes place in digital environments where users must balance the convenience of financial technologies against persistent risks of fraud, scams, account misuse, and unauthorized access. This study examines the associations of cybersecurity literacy, perceived fintech security, and institutional trust with fintech adoption among urban users in Bangladesh, with particular attention to secure user behaviour and differences across levels of fintech usage experience. Data from 357 respondents were analysed using Partial Least Squares Structural Equation Modeling (PLS-SEM), including indirect effects and multi-group analysis. Cybersecurity literacy, perceived fintech security, and secure user behaviour have significant positive associations with adoption, although their individual effect sizes are small. Institutional trust has no significant direct association with adoption. The indirect association through secure user behaviour is significant for cybersecurity literacy but not for perceived fintech security or institutional trust. Measurement invariance checks support standardized path comparisons across the three tenure groups, but none of the nine focal comparisons is significant using two-sided bootstrap MGA at the 5% level. A four-band sensitivity analysis does not establish robust differences after adjustment for multiple comparisons. The model accounts for 61.0% of the in-sample variance in adoption; out-of-sample predictive performance was not assessed. The findings therefore support a cautious, association-based account of security-related fintech use among existing users, without establishing causal effects or developmental changes with experience.

Keywords: cybersecurity; fintech adoption; digital risk; secure user behaviour; fintech use tenure; multi-group analysis; Bangladesh



Academic Editor: Shyan-Ming Yuan

Received: 8 September 2026

Revised: 8 October 2026

Accepted: 21 October 2026

Published: 26 October 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

JEL Classification: G23; G41; O33; D91

1. Introduction

The use of fintech services such as mobile payments and digital wallets has become increasingly common among urban populations in Bangladesh. However, access to a mobile connection, ownership of a financial account, and active use of digital financial services represent different forms of participation and should not be treated as equivalent indicators of adoption. Hossain et al. [1] highlighted cyber threats and scam-related incidents affecting fintech organizations in Bangladesh. Similarly, Transparency International

Bangladesh [2] raised concerns regarding customer rights and structural weaknesses within the mobile financial services industry. As a result, fintech users are not merely considering the convenience of these technologies; they are also operating in a digital environment in which fraud, account misuse, and suspicious transaction attempts require attention.

Bangladesh in a Comparative International Context

A comparison with selected Asian and European economies helps clarify the setting in which the present study was conducted. Table 1 presents population, urbanization, income, connectivity, and digital payment indicators for Bangladesh, Indonesia, South Korea, the United Kingdom, France, and Germany. The countries are used as contextual reference points, rather than as matched comparison samples. Population, urbanization, and income figures refer to 2024, while the connectivity and digital-payment series use common reference years selected for comparability [3,4].

Table 1. Bangladesh and selected Asian and European economies.

Indicator	Bangladesh	Indonesia	S. Korea	UK	France	Germany
Population, millions	173.6	283.5	51.8	69.3	68.6	83.5
Urban population, %	32.7	58.8	81.2	83.2	78.8	82.0
GDP per capita, USD	2593	4925	36,239	53,341	46,103	56,104
Internet use, %	53.4	72.8	97.9	95.5	88.7	93.5
Mobile subscriptions per 100 people ¹	111.3	125.2	162.1	122.8	116.7	124.7
Digital payments, % of adults ²	45.3	37.2	97.9	99.2	98.4	99.5

Source: Authors’ compilation from World Development Indicators [3] and the Global Index Database [4], accessed 6 October 2026. Values are for 2024 except ¹ mobile subscriptions (2023, common available year) and ² made or received digital payments in the past year (2021, adults aged 15+). Subscriptions count connections, not unique owners. National definitions of urban areas may differ.

Bangladesh had a population of approximately 173.6 million in 2024, compared with 283.5 million in Indonesia and 51.8 million in South Korea. Its GDP per capita, approximately USD 2593, was below Indonesia’s USD 4925 and substantially below the levels in South Korea and the three European economies. These differences are relevant because the resources available for devices, connectivity, and financial participation vary across settings. However, national income does not directly determine an individual user’s cybersecurity knowledge or behaviour. The comparison therefore helps situate the survey without supplying an explanation for its structural coefficients.

The urban share of Bangladesh’s population was 32.7% in the retrieved World Development Indicators series, compared with 58.8% in Indonesia and approximately 79–83% in the other reference economies. National definitions and revisions affect urbanization statistics, so these values should be interpreted with their source definitions in mind. More importantly for the present study, the national figures differ from the composition of a survey concentrated in Dhaka. Findings from digitally active urban respondents cannot be extended directly to the much broader national population.

The connectivity indicators also show why access and use should be distinguished. Internet use in 2024 was reported for 53.4% of Bangladesh’s population, compared with 72.8% in Indonesia, 97.9% in South Korea, and 88.7–95.5% in the European reference economies. Mobile cellular subscriptions exceeded 100 per 100 people in all six countries in the common 2023 comparison. This indicator counts subscriptions, rather than unique phone owners; multiple subscriptions can therefore coexist with unequal individual access. A high subscription rate does not establish universal smartphone ownership, internet use, or competence in secure digital transactions.

Digital financial participation presents a related distinction. The Global Findex measure of adults who made or received a digital payment in the preceding year was 45.3% in Bangladesh and 37.2% in Indonesia in 2021, compared with approximately 98–99% in the other reference economies. The 2021 wave is retained for this particular comparison because the 2024 financial-use questions were not collected in the high-income reference economies. Digital payments include several account-based payment channels and should not be interpreted as a narrowly defined e-banking adoption rate. Taken together, the comparisons indicate that Bangladesh combines a large potential user base with substantial differences in connectivity, income, and financial participation. This provides a reason to examine security-related perceptions among existing urban users while retaining clear limits on national and international generalization.

Given this growing risk environment, it is important to understand how users interpret these threats and what protective routines they adopt while continuing to use fintech applications. Existing technology adoption research typically explains user acceptance through factors such as usefulness, ease of use, and facilitating conditions [5]. However, such studies often assume relatively stable and secure usage environments. In Bangladesh, where users may experience uncertainty arising from growing security concerns, such conventional adoption factors may not fully explain their continued use of fintech services. This suggests that fintech adoption is influenced not only by utility considerations but also by how users perceive and cope with digital risks.

Prior research has highlighted the importance of cybersecurity literacy in supporting safer digital participation. Cybersecurity literacy encompasses security-related knowledge, awareness, and confidence in taking protective action [6,7]. Within this context, two additional dimensions become relevant at the system and institutional levels. Perceived fintech security refers to users' evaluations of the reliability and protection offered by fintech applications, including transaction processing, privacy, and security features [8]. Institutional trust reflects confidence in providers, regulatory protection, and available mechanisms for support and dispute resolution [9]. Together, these dimensions provide a basis for examining how personal capability, perceived platform assurance, and institutional confidence are associated with continued fintech participation [10–12].

This issue is particularly relevant in Bangladesh because the expansion of digital financial services occurs alongside uneven access to income, connectivity, and financial participation. The national comparisons above provide context for this setting, whereas the present survey focuses on adults who already use fintech services and live primarily in urban areas. Consequently, the study examines security-related perceptions and reported practices among existing users; it does not estimate the national prevalence of fintech adoption or directly measure the technical security of service providers.

Previous research conducted in Bangladesh has considered user perceptions and the development of fintech services [13]. However, there remains scope to examine cybersecurity literacy, perceived security, institutional trust, and secure user behaviour together, while assessing whether selected associations differ across tenure groups. Therefore, this study focuses on adult fintech users living primarily in urban areas of Bangladesh and examines these constructs within a unified research model. The use of a cross-sectional design means that any group differences concern different respondents observed at one point in time.

Fintech usage experience may be relevant because respondents with different periods of use can differ in their familiarity with security features, transaction routines, and institutional support. However, tenure can also be associated with age, education, service choice, and other characteristics. It is therefore appropriate to examine tenure-related heterogeneity without assuming that longer use necessarily produces greater capability

or stronger security-related associations. In this study, tenure serves as an exploratory grouping condition whose interpretation depends on measurement comparability and the stability of the results across the available categories.

The aim of this study is therefore to investigate how cybersecurity literacy, perceived fintech security, and institutional trust are associated with fintech adoption among urban users in Bangladesh. In doing so, the study examines direct associations and specific indirect associations through secure user behaviour. It further examines whether selected structural coefficients differ across fintech tenure groups after assessing measurement invariance. By considering these relationships within a single model, the study seeks to provide a more qualified understanding of security-related fintech participation in the surveyed population.

The paper is organized into five sections. Following the introduction, Section 2 reviews relevant literature and develops the theoretical and conceptual framework. Section 3 describes the research methodology and analytical procedures, while Section 4 presents the measurement and structural results, indirect effects, invariance checks, and tenure comparisons. Section 5 discusses the findings and their theoretical, managerial, and policy implications. Appendix A reports the additional invariance and robustness results.

2. Literature Review: Towards a Conceptual Framework

Fintech adoption in this study refers to respondents' reported engagement with technology-enabled financial services. Because the sample consists of existing users, the outcome includes current use and intentions to continue using services. It is therefore distinct from an initial adoption decision by someone who has never used fintech. Cybersecurity, in turn, concerns protection against threats to digital systems, information, and transactions; cybersecurity literacy describes a user capability, while perceived security describes an evaluation of the platform. These distinctions prevent personal knowledge, technical protection, and perceptions of protection from being treated as the same phenomenon.

A broader economic perspective can help explain why users consider both the benefits and possible costs of financial participation. Becker's economic approach provides a framework for considering choices under constraints [14]. Applied here as conceptual reasoning, convenience and access may be considered alongside perceived financial loss, time, and the effort involved in protective action. However, the present survey does not estimate a formal utility model. Similarly, Smith, Walter, and DeLong's account of global banking places financial services within a wider system of intermediation, competition, and institutional organization [15]. This helps distinguish a provider's visible interface from the broader institutions within which financial transactions occur. These perspectives complement the behavioural model without supplying unmeasured variables or additional causal claims.

Research on technology adoption has traditionally been dominated by the Technology Acceptance Model (TAM). This model proposes that perceived usefulness and perceived ease of use are the primary determinants of users' behavioural intentions toward technology adoption [16]. TAM has been widely applied across various digital service contexts. Building on TAM, the Unified Theory of Acceptance and Use of Technology (UTAUT) further incorporates performance expectancy, effort expectancy, social influence, and facilitating conditions as determinants of behavioural intention and usage behaviour [17]. Both theories have been extensively used to explain how consumers adopt digital technologies in stable and evolving environments. However, these models do not fully explain adoption behaviour when technology use occurs under conditions of uncertainty, perceived risk, and institutional vulnerability, particularly in digital finance environments. To address these limitations, researchers have increasingly incorporated perceived risk and trust-based ex-

tensions into adoption models [10]. These extensions place greater emphasis on issues such as data protection, transaction integrity, and institutional credibility, which are particularly relevant within fintech and digital finance settings.

Another important theoretical lens relevant to this study is Protection Motivation Theory (PMT). PMT distinguishes threat appraisal, concerning the perceived severity of and vulnerability to a threat, from coping appraisal, concerning the perceived effectiveness and feasibility of a protective response [18]. Cybersecurity literacy is relevant to users' perceived ability to recognize and respond to digital threats, while secure user behaviour concerns reported protective action. However, the present instrument does not separately measure perceived threat severity, vulnerability, response efficacy, and response cost. Perceived fintech security and institutional trust also cannot be treated as direct substitutes for these PMT dimensions. Consequently, this study uses PMT to inform its behavioural reasoning, rather than presenting the model as a complete test or extension of PMT.

The Diffusion of Innovations framework provides a complementary perspective on how individuals interpret the attributes of a technology, including its relative advantage, compatibility, and observability [19]. Within fintech services, visible authentication and transaction-confirmation features may contribute to users' evaluations of the platform. However, duration of use is distinct from an adopter category in diffusion theory. The tenure groups used here are therefore survey-based categories for comparing respondents, rather than theoretically established stages through which all users progress.

Recent FinTech research also indicates that explanatory structural coefficients and predictive patterns address different questions. Bhuiyan et al. examine retention intention using explainable machine learning and identify potentially nonlinear and interaction-based patterns within their fitted models [20]. Such results motivate caution when interpreting a small linear coefficient, but they do not establish corresponding nonlinear effects in the present sample. The current PLS-SEM analysis concerns the specified linear associations; no out-of-sample or nonlinear analysis is claimed.

2.1. Cybersecurity Literacy and Fintech Adoption

Cybersecurity literacy refers to an individual's capability to remain protected in digital environments. It generally encompasses security-related knowledge, awareness, and confidence in acting safely online [6]. Knowledge involves understanding how cyberattacks occur and recognizing the precautions necessary to prevent them [21]. Awareness refers to the ability to identify suspicious activities in real time [7]. Confidence, or self-efficacy, relates to an individual's belief in their own ability to protect themselves online.

Cybersecurity literacy may be associated with fintech participation because respondents who understand common security risks can be better placed to evaluate digital transactions and select protective practices. Research on digital literacy, security behaviour, and e-payment intention provides a basis for examining these related dimensions [22], while research in a developing-country context highlights the relevance of cybersecurity and risky behaviour [23]. However, knowledge and reported behaviour remain conceptually distinct. The present model therefore examines both the direct association between literacy and adoption and the indirect association through secure user behaviour, without assuming that knowledge necessarily leads to protective action.

H1a. *Cybersecurity literacy is positively associated with fintech adoption.*

2.2. Perceived Fintech Security and Fintech Adoption

Perceived fintech security refers to consumers' perceptions regarding the safety of financial applications and digital transactions. Research on digital finance risk suggests that consumers who perceive fintech services as secure tend to experience greater confidence

and lower levels of perceived risk [10]. In threat-intensive environments, perceptions of security become particularly important because they shape users' evaluations of whether fintech systems can adequately protect them and whether continued usage is worth the associated risks. Previous studies on fintech and trust have demonstrated that when consumers perceive fintech services to be secure, they are more likely to trust and engage with financial applications, banking platforms, and mobile payment systems [12,24–26]. These findings suggest that stronger perceptions of security encourage greater adoption and continued use of fintech services.

At the same time, perceived security should be distinguished from independently verified technical protection. Respondents can evaluate reliability, privacy, and visible safeguards without being able to assess the underlying security architecture. Therefore, the construct concerns users' perceptions of platform assurance. Whether this association differs across periods of use remains an empirical question, rather than an assumed consequence of experience.

H1b. *Perceived fintech security is positively associated with fintech adoption.*

2.3. Institutional Trust and Fintech Adoption

Institutional trust reflects consumers' confidence in service providers, regulatory authorities, and institutional mechanisms operating within the digital financial ecosystem. Trust can reduce perceptions of risk and vulnerability, thereby increasing users' willingness to rely on online systems and engage in potentially risky digital transactions. Recent studies indicate that consumers evaluate regulatory protection, platform legitimacy, and institutional responsiveness when making fintech adoption decisions [12]. Furthermore, several studies have found positive relationships between institutional trust and the adoption and continued use of digital payment services [27,28].

Trust can also be understood at different levels. Fukuyama's account concerns the broader social foundations of cooperation and economic organization [29]. The present construct has a narrower scope: it concerns confidence in fintech providers, regulatory protection, and support when problems arise. It should therefore not be interpreted as a direct measure of societal trust or the actual effectiveness of regulation. This distinction is relevant because the absence of a conditional association in one statistical model would not establish that institutions or social trust are unimportant.

In the present model, institutional trust is examined alongside perceived fintech security and cybersecurity literacy. These constructs can share variance, so the direct path to adoption represents the association remaining after the other modelled predictors have been considered. This provides a more specific test than the general proposition that trust matters for economic participation.

H1c. *Institutional trust is positively associated with fintech adoption.*

2.4. Secure User Behaviour and Mediation Logic

Secure user behaviour refers to the protective practices respondents report using during digital financial activities. In this study, these practices include using a strong and non-reused PIN or password, enabling two-factor authentication, avoiding unfamiliar payment links, and avoiding public Wi-Fi for money transfers. Prior work distinguishes security intentions from reported behaviour and examines the motivations underlying cybersecurity practices [30,31]. The present survey measures reported practices, rather than directly observing protective actions or subsequent fraud outcomes.

Secure user behaviour may therefore provide an indirect statistical connection between security-related perceptions and fintech participation. Cybersecurity literacy can be associ-

ated with respondents' ability to recognize risks, while perceived platform protection and institutional confidence can be associated with their willingness to undertake protective practices. However, the order of these processes cannot be established from responses collected at one time. Accordingly, the mediation analysis is interpreted as an assessment of specific indirect associations within the proposed model.

H2. *Secure user behaviour is positively associated with fintech adoption.*

H3a. *Cybersecurity literacy has a positive indirect association with fintech adoption through secure user behaviour.*

H3b. *Perceived fintech security has a positive indirect association with fintech adoption through secure user behaviour.*

H3c. *Institutional trust has a positive indirect association with fintech adoption through secure user behaviour.*

2.5. Fintech Use Tenure and Exploratory Group Comparisons

Fintech use tenure refers to the period for which respondents report having used fintech services. It is not treated as a latent construct measured through multiple indicators. Instead, it provides a grouping condition for examining whether the same model yields different coefficients among respondents with different periods of use. Such differences could be consistent with variation in familiarity, but they could also reflect selection into longer use or other differences between respondents. Consequently, tenure comparisons cannot by themselves establish learning or within-person development.

The survey recorded four tenure bands, which allow the sensitivity of a broader three-group specification to be assessed. The analysis focuses on three relationships identified in the original framework: cybersecurity literacy with secure user behaviour, perceived fintech security with adoption, and institutional trust with adoption. To simplify the theoretical presentation, these comparisons are consolidated into one exploratory research question, while the direct and indirect propositions are organized into three hypothesis families.

RQ1. *Do the $CL \rightarrow SUB$, $PFS \rightarrow FA$, and $IT \rightarrow FA$ associations differ across fintech use tenure groups?*

2.6. The Conceptual Framework

Building on the preceding literature, this study develops a conceptual framework (Figure 1) that integrates user capability, perceived platform assurance, institutional confidence, and reported protective behaviour. Fintech adoption (FA) is the outcome, while cybersecurity literacy (CL), perceived fintech security (PFS), and institutional trust (IT) are antecedent constructs. Secure user behaviour (SUB) is included as an intermediate construct. The same seven-path structural model is estimated for the full sample and for the tenure groups; tenure is examined through group comparisons rather than an additional latent-variable path.

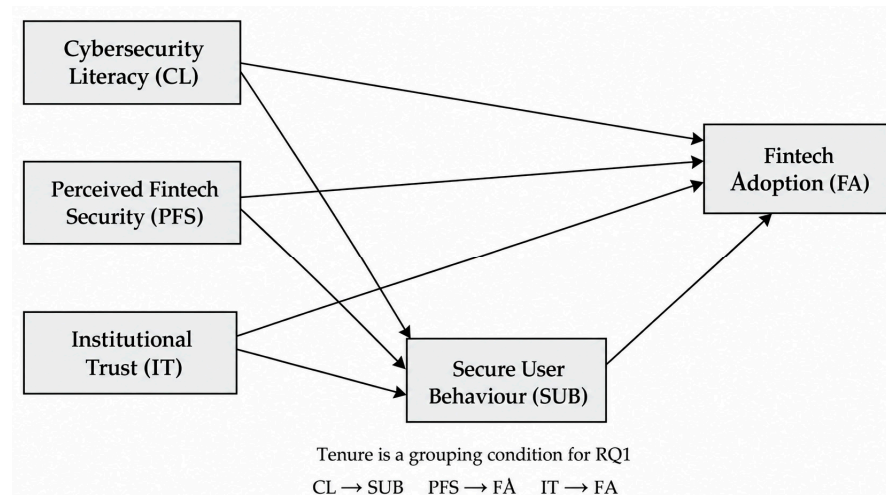


Figure 1. Conceptual framework and exploratory tenure comparisons. Source: Authors' conceptualization. Arrows show the specified associations; tenure comparisons address RQ1 and do not establish causal change.

3. Research Methodology

This study adopts a quantitative, cross-sectional design to examine the relationships among cybersecurity literacy, perceived fintech security, institutional trust, secure user behaviour, and fintech adoption. All five constructs were specified with first-order reflective indicators on a seven-point Likert scale. The target population comprised adult fintech users aged 18 years or older residing primarily in urban areas such as Dhaka and Chattogram. Respondents were required to have used at least one fintech service, such as bKash, Nagad, or another mobile financial service, within the previous three months. Table 2 summarizes the data and analytical procedures.

Table 2. Summary of the study data and analytical procedures.

Element	Specification
Design and recruitment	Cross-sectional online convenience survey; existing adult fintech users
Analytical sample	357 complete observations; 26 indicators; no missing indicator or tenure values
Sample concentration	Dhaka 77.3%; age 18–27 76.2%; students 68.1%
Measurement	Seven-point Likert scales; reflective CL (6), PFS (6), IT (4), SUB (4), FA (6)
Primary tenure groups	<1 year: 125; 1–3 years: 102; >3 years: 130
Four-band check	<6 months: 69; 6–12 months: 56; 1–3 years: 102; >3 years: 130
Structural specification	CL, PFS, IT → SUB; CL, PFS, IT, SUB → FA
Original inference	SmartPLS 4; 5000 bootstrap resamples; two-sided 5% tests
Additional checks	MICOM and two-sided permutation contrasts, 5000 permutations per pair; Holm adjustment for 18 our-band tests
Interpretive scope	Associations within the achieved sample; no causal or out-of-sample predictive claim

Source: Authors' questionnaire, analytical dataset, and archived SmartPLS 4 outputs. Additional checks were performed for this revision using the same 357 responses.

Due to the absence of a publicly available sampling frame for fintech users in Bangladesh, the study employed non-probability convenience sampling. Participants self-recruited through online distribution channels, including social media platforms and urban digital communities. The final analytical sample comprised 357 responses, with complete values for all 26 measurement indicators and the tenure variable. The sample was concentrated among younger, digitally active respondents and should not be considered representative of all fintech users in Bangladesh. Because selection probabilities are unknown, a probability-sampling margin of error cannot be assigned to this convenience sample. The achieved sample is therefore reported without a claim of 5% population precision.

The primary instrument was a self-administered questionnaire covering security knowledge and practices, platform perceptions, institutional confidence, and fintech participation. Cybersecurity literacy was measured using six indicators (CL1–CL6), perceived fintech security using six (PFS1–PFS6), institutional trust using four (IT1–IT4), secure user behaviour using four (SUB1–SUB4), and fintech adoption using six (FA1–FA6). The adoption items include intended future use, self-reported recent use, and continuance preferences. Therefore, FA represents a broad measure of engagement among existing users, rather than the initial decision of a non-user to adopt. The combined treatment of these dimensions is retained from the submitted model and acknowledged as a measurement limitation.

The original analysis was conducted using SmartPLS 4 [32], with standardized indicators, reflective Mode A estimation, and the path weighting scheme. The measurement model was assessed using outer loadings, internal consistency reliability, convergent validity, and discriminant validity. Structural assessment covered collinearity, R^2 , f^2 , direct coefficients, and specific indirect effects. Bootstrap inference used 5000 resamples and two-sided tests at the 5% level. The revision additionally uses a reproducible Python (version 3.12) implementation of the same PLS algorithm for permutation checks. Its full-sample and three-group path estimates reproduce the archived SmartPLS coefficients to their reported three-decimal precision. The supplementary procedure uses initial weights of one, a 10^{-7} convergence tolerance, and a maximum of 3000 iterations.

The original questionnaire recorded less than six months ($n = 69$), six to twelve months ($n = 56$), one to three years ($n = 102$), and more than three years ($n = 130$). The primary specification combines the two first-year bands into G1 (<1 year, $n = 125$), retains G2 (1–3 years, $n = 102$), and retains G3 (>3 years, $n = 130$). This grouping follows the available response categories and provides more balanced group sizes; the cut-offs are not claimed to identify validated developmental stages. Exact continuous tenure was not collected. Consequently, the sensitivity analysis retains all four original bands, avoiding assumptions about exact durations or a midpoint for the open-ended final category.

The structural model consists of two equations for the endogenous constructs. The first represents associations with secure user behaviour, while the second represents associations with fintech adoption. The path notation expresses the proposed statistical model and does not establish temporal or causal ordering from the cross-sectional data.

Equation (1): Determinants of Secure User Behaviour

$$\text{SUB} = \beta_1 \text{CL} + \beta_2 \text{IT} + \beta_3 \text{PFS} + \zeta_1 \quad (1)$$

Equation (2): Determinants of Fintech Adoption

$$\text{FA} = \beta_4 \text{CL} + \beta_5 \text{IT} + \beta_6 \text{PFS} + \beta_7 \text{SUB} + \zeta_2 \quad (2)$$

where:

SUB = Secure User Behaviour

FA = Fintech Adoption

CL = Cybersecurity Literacy

IT = Institutional Trust

PFS = Perceived Fintech Security

β_1 – β_7 = Path coefficients estimated through the PLS algorithm

ζ_1 and ζ_2 = Structural error terms or residuals

Specific indirect associations were calculated as products of the relevant path coefficients. Their significance was assessed using the bootstrap results, while recognizing that the cross-sectional design does not identify a causal mediation process.

Mediation Path of CL

$$\beta_{indirect} = \beta_1 \times \beta_7$$

Mediation Path of IT

$$\beta_{indirect} = \beta_2 \times \beta_7$$

Mediation Path of PFS

$$\beta_{indirect} = \beta_3 \times \beta_7$$

Before interpreting group comparisons, measurement invariance was assessed using MICOM [33]. Configural comparability follows from identical indicators, coding, data treatment, reflective specification, and estimation settings across groups. For each group pair, 5000 fixed-size label permutations were used to compare the observed correlation between pooled-data composites formed with group-specific weights against its 5th-percentile reference value. Pooled-fit scores were then used to examine mean differences and log variance ratios against 95% permutation intervals. Partial invariance permits standardized path comparisons; equal means and variances are additionally required for full invariance. All nine focal three-group contrasts are reported using the archived two-sided bootstrap MGA results and supplementary two-sided permutation tests. The four-band check covers all six pairs for each of the three focal paths; Holm adjustment controls the family of 18 exploratory tests [34]. Random seeds and computational details are provided in Appendix A.

4. Results

This section presents the descriptive statistics and respondent profile, followed by the measurement and structural results. Indirect associations are then examined, before measurement invariance and complete tenure comparisons are reported. The additional checks distinguish exploratory group patterns from supported differences.

4.1. Descriptive Statistics

As shown in Table 3, the mean scores for the individual indicators range from 5.00 to 6.16. For example, the cybersecurity literacy indicators range from 5.00 for CL5 to 6.16 for CL2, while the fintech adoption indicators reach 5.90 for FA2. These values indicate relatively high self-reported agreement on the seven-point scales, with standard deviations of approximately 1.54–2.09. They describe indicator responses rather than objective levels of cybersecurity capability or population-wide adoption.

Table 3. Descriptive statistics of indicators.

Indicator	Mean	SD	Min	Max
CL1	5.501	1.994	1.000	7.000
CL2	6.160	1.733	1.000	7.000
CL3	5.810	1.758	1.000	7.000
CL4	5.594	1.755	1.000	7.000
CL5	5.000	2.085	1.000	7.000

Table 3. *Cont.*

Indicator	Mean	SD	Min	Max
CL6	5.179	2.014	1.000	7.000
FA1	5.804	1.623	1.000	7.000
FA2	5.902	1.670	1.000	7.000
FA3	5.297	1.998	1.000	7.000
FA4	5.462	1.955	1.000	7.000
FA5	5.280	1.827	1.000	7.000
FA6	5.454	1.697	1.000	7.000
IT1	5.529	1.610	1.000	7.000
IT2	5.289	1.766	1.000	7.000
IT3	5.303	1.788	1.000	7.000
IT4	5.132	1.849	1.000	7.000
PFS1	5.462	1.674	1.000	7.000
PFS2	5.796	1.650	1.000	7.000
PFS3	5.462	1.716	1.000	7.000
PFS4	5.541	1.627	1.000	7.000
PFS5	5.599	1.780	1.000	7.000
PFS6	5.902	1.544	1.000	7.000
SUB1	5.641	1.776	1.000	7.000
SUB2	5.375	1.904	1.000	7.000
SUB3	5.849	1.793	1.000	7.000
SUB4	5.216	2.043	1.000	7.000

Source: Authors' survey data ($N = 357$).

4.2. Demographic Profile

The demographic characteristics of the respondents ($N = 357$, Tables 4 and 5) show that the sample is concentrated in Dhaka and among younger users. Dhaka accounts for 77.3% of respondents, 76.2% are aged 18–27, and 68.1% are students. This concentration is consistent with online convenience recruitment, but it also limits coverage of older users, rural populations, and less digitally connected groups. The findings should therefore be interpreted in relation to the achieved sample.

Table 4. Demographic profile of respondents.

Demographic Variable	Category	Frequency	Percentage (%)
City of Residence	Dhaka	276	77.3
City of Residence	Other	43	12.0
City of Residence	Chattogram	20	5.6
City of Residence	Khulna	16	4.5
City of Residence	Sylhet	2	0.6
Age	18–27	272	76.2
Age	28–37	59	16.5
Age	38–47	22	6.2
Age	48–57	4	1.1
Gender	Male	239	66.9
Gender	Female	117	32.8
Gender	Prefer not to say	1	0.3
Highest Education	Bachelor's	149	41.7
Highest Education	HSC	137	38.4
Highest Education	Master's	63	17.6
Highest Education	Diploma	6	1.7
Highest Education	Other	2	0.6
Employment Status	Student	243	68.1
Employment Status	Employed	88	24.6

Table 4. Cont.

Demographic Variable	Category	Frequency	Percentage (%)
Employment Status	Student, Employed	12	3.4
Employment Status	Self-employed	3	0.8
Employment Status	Employed, Self-employed	3	0.8
Employment Status	Other	3	0.8
Employment Status	Others (Mixed/Unemployed)	5	1.4
Monthly Household Income	<25,000 BDT	110	30.8
Monthly Household Income	25,000–49,999 BDT	106	29.7
Monthly Household Income	50,000–99,999 BDT	101	28.3
Monthly Household Income	100,000–199,999 BDT	24	6.7
Monthly Household Income	≥200,000 BDT	16	4.5

Source: Authors' survey data ($N = 357$).

Table 5. Fintech use tenure and MGA grouping.

Fintech Use Tenure Category	Frequency	Percentage (%)
<6 months	69	19.3
6–12 months	56	15.7
1–3 years	102	28.6
>3 years	130	36.4
Group 1: New users (<1 year)	125	35.0
Group 2: Moderate users (1–3 years)	102	28.6
Group 3: Experienced users (>3 years)	130	36.4

Source: Authors' survey data ($N = 357$).

4.3. Measurement Model Analysis

The measurement model (Figure 2) was assessed to establish the reliability and validity of all constructs before examining the structural relationships. The evaluation included indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. As all constructs were modelled as first-order reflective constructs, the measurement model was evaluated using outer loadings, Cronbach's alpha, rho_A, composite reliability (CR), average variance extracted (AVE), and the heterotrait–monotrait ratio (HTMT).

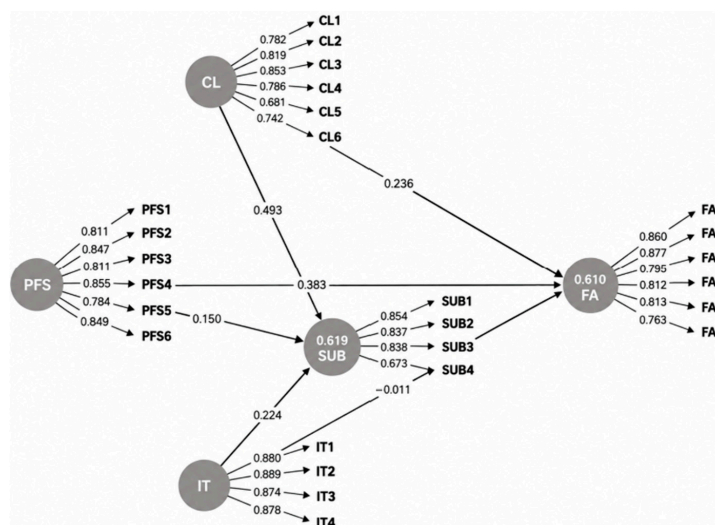


Figure 2. Measurement Model Analysis with Outer Loadings and Path Coefficients. Source: Authors' SmartPLS 4 analysis of the 357 survey responses. Numbers on paths are standardized coefficients; numbers within endogenous constructs are R^2 .

4.4. Indicator Reliability

Outer loadings were used as the primary criterion for assessing the reliability of the reflective indicators. According to Hair et al. [35], outer loadings should exceed 0.708 to ensure that a construct explains more than 50% of the variance in its indicators. However, indicators with loadings between 0.40 and 0.708 may still be retained if their removal does not substantially improve the average variance extracted (AVE).

The results show (Table 6) that the outer loadings range from 0.673 (SUB4) to 0.889 (IT2), with the majority of indicators exceeding the recommended threshold of 0.708. Two indicators, CL5 and SUB4, fall slightly below this threshold. Nevertheless, they were retained because they remain theoretically meaningful and the overall AVE values for their respective constructs exceed the accepted threshold. Furthermore, all indicator loadings were statistically significant at $p < 0.001$, supporting the indicator reliability of the measurement model.

Table 6. Summary of outer loadings for reflective constructs.

Indicator Relationship	Loading	t-Statistic	p-Value
CL1 <- CL	0.782	23.195	<0.001
CL2 <- CL	0.819	28.079	<0.001
CL3 <- CL	0.853	42.080	<0.001
CL4 <- CL	0.786	24.399	<0.001
CL5 <- CL	0.681	20.715	<0.001
CL6 <- CL	0.742	26.644	<0.001
FA1 <- FA	0.860	48.319	<0.001
FA2 <- FA	0.877	53.787	<0.001
FA3 <- FA	0.795	29.171	<0.001
FA4 <- FA	0.812	29.584	<0.001
FA5 <- FA	0.813	31.175	<0.001
FA6 <- FA	0.763	19.251	<0.001
IT1 <- IT	0.880	58.902	<0.001
IT2 <- IT	0.889	46.218	<0.001
IT3 <- IT	0.874	45.392	<0.001
IT4 <- IT	0.878	48.984	<0.001
PFS1 <- PFS	0.811	34.693	<0.001
PFS2 <- PFS	0.847	33.140	<0.001
PFS3 <- PFS	0.811	28.027	<0.001
PFS4 <- PFS	0.855	35.729	<0.001
PFS5 <- PFS	0.784	25.399	<0.001
PFS6 <- PFS	0.849	34.983	<0.001
SUB1 <- SUB	0.854	41.346	<0.001
SUB2 <- SUB	0.837	39.697	<0.001
SUB3 <- SUB	0.838	33.749	<0.001
SUB4 <- SUB	0.673	16.449	<0.001

Source: Authors' SmartPLS 4 analysis of the survey data ($N = 357$).

4.5. Internal Consistency Reliability and Convergent Validity

Internal consistency reliability (Table 7) assesses the extent to which items measuring the same construct produce consistent scores. According to Hair et al. [35], values between 0.70 and 0.95 are generally considered satisfactory for Cronbach's alpha, rho_A, and composite reliability. As presented in Table 7, all constructs demonstrate satisfactory internal consistency reliability. Cronbach's alpha values range from 0.815 for secure user behaviour (SUB) to 0.907 for perceived fintech security (PFS), while composite reliability values range from 0.879 to 0.932. The average variance extracted (AVE) values range from 0.607 to 0.775, confirming convergent validity, as all values exceed the recommended threshold of 0.50.

Table 7. Reliability and convergent validity.

Construct	Cronbach's Alpha	rho_A	Composite Reliability	AVE
CL	0.869	0.871	0.902	0.607
FA	0.903	0.915	0.925	0.674
IT	0.903	0.906	0.932	0.775
PFS	0.907	0.910	0.928	0.684
SUB	0.815	0.830	0.879	0.647

Source: Authors' SmartPLS 4 analysis of the survey data ($N = 357$).

4.6. Discriminant Validity

Discriminant validity assesses whether each construct is empirically distinct from the other constructs included in the model. In this study, discriminant validity was evaluated using both the Fornell–Larcker criterion and HTMT. According to the Fornell–Larcker criterion, the square root of the average variance extracted (AVE) for each construct should exceed its correlations with other constructs in the model. The correlation matrix presented in Table 8 indicates that this requirement was satisfied for all constructs.

In addition, HTMT was examined (Table 9) as a more robust assessment of discriminant validity, following the recommendations of Henseler et al. [36]. All HTMT values remained below the recommended threshold of 0.90. Although the value between perceived fintech security (PFS) and institutional trust (IT) approached the upper boundary, this remains within the accepted threshold and is reasonable in a risk-sensitive fintech context, where perceptions of platform security and trust in institutional structures may conceptually overlap to some extent.

Table 8. Fornell–Larcker matrix.

Construct	CL	FA	IT	PFS	SUB
CL	0.779	0.706	0.623	0.759	0.746
FA	0.706	0.821	0.608	0.729	0.688
IT	0.623	0.608	0.880	0.809	0.652
PFS	0.759	0.729	0.809	0.827	0.705
SUB	0.746	0.688	0.652	0.705	0.804

Source: Authors' SmartPLS 4 analysis of the survey data ($N = 357$).

Table 9. HTMT ratios.

Relationship	HTMT
FA <-> CL	0.786
IT <-> CL	0.697
IT <-> FA	0.658
PFS <-> CL	0.848
PFS <-> FA	0.785
PFS <-> IT	0.889
SUB <-> CL	0.881
SUB <-> FA	0.787
SUB <-> IT	0.751
SUB <-> PFS	0.807

Source: Authors' SmartPLS 4 analysis of the survey data ($N = 357$).

4.7. Collinearity Diagnostics

The inner-model VIF values (Table 10) range from 2.362 to 4.253. Although none exceeds five, the values around four for perceived fintech security indicate appreciable overlap with the other predictors. In particular, the correlation between perceived security

and institutional trust is 0.809. Therefore, the direct coefficients are interpreted as conditional associations, and the near-zero trust coefficient should not be taken to establish the absence of a broader relationship between trust and fintech use.

Table 10. Collinearity diagnostics (Inner VIF).

Path	VIF
CL -> FA	2.998
CL -> SUB	2.362
IT -> FA	3.032
IT -> SUB	2.901
PFS -> FA	4.253
PFS -> SUB	4.194
SUB -> FA	2.623

Source: Authors' SmartPLS 4 analysis of the survey data ($N = 357$).

4.8. Structural Model Analysis

The coefficients of determination summarize the proportion of variance accounted for within the estimation sample (Table 11). Fintech adoption has $R^2 = 0.610$ and adjusted $R^2 = 0.606$, while secure user behaviour has $R^2 = 0.619$ and adjusted $R^2 = 0.616$. These values concern in-sample explanatory performance. They do not establish causal explanation or performance for new respondents, because no holdout assessment, cross-validation, or PLSpredict analysis was conducted. Figure 3 presents the structural model with bootstrapped p -values.

Table 11. R-square values.

Endogenous Construct	R-Square	Adjusted R-Square
FA	0.610	0.606
SUB	0.619	0.616

Source: Authors' SmartPLS 4 analysis of the survey data ($N = 357$).

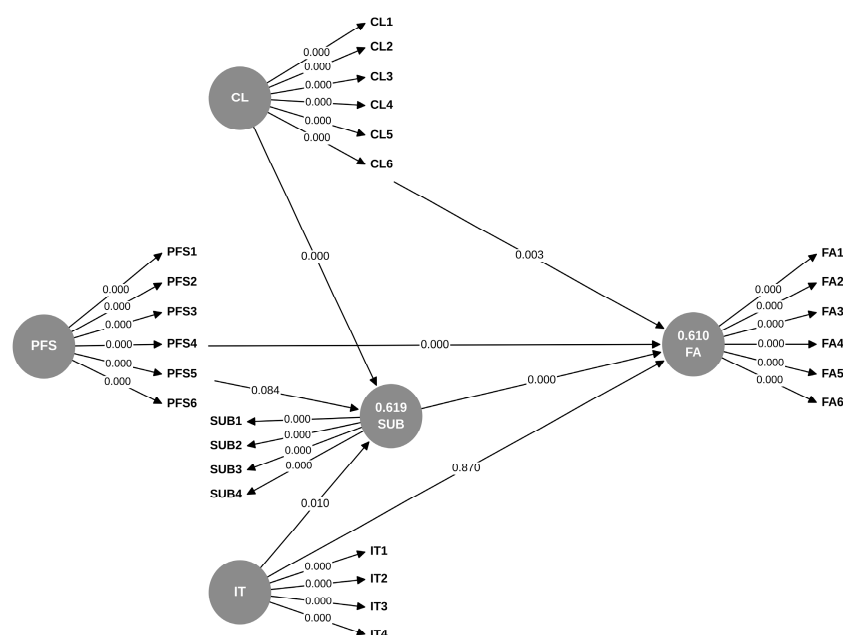


Figure 3. Structural Model Analysis with Bootstrapped p -values. Source: Authors' SmartPLS 4 bootstrap analysis using 5000 resamples. Values displayed as 0.000 denote $p < 0.001$, rather than an exact zero.

The f^2 statistics assess the incremental in-sample contribution of each predictor after the others are included (Table 12). Using the conventional reference values of 0.02, 0.15, and 0.35 [37], CL $\rightarrow$ SUB has a medium effect size (0.269). The contributions to FA from CL (0.048), PFS (0.088), and SUB (0.061) are small, as is IT $\rightarrow$ SUB (0.045). PFS $\rightarrow$ SUB (0.014) is below the small-effect reference value, while IT $\rightarrow$ FA is approximately zero. Thus, statistical significance for several paths coexists with modest incremental effect sizes.

Table 12. f-square effect sizes.

Path	f-Square	Rating
CL $\rightarrow$ FA	0.048	Small
CL $\rightarrow$ SUB	0.269	Medium
IT $\rightarrow$ FA	0.000	None
IT $\rightarrow$ SUB	0.045	Small
PFS $\rightarrow$ FA	0.088	Small
PFS $\rightarrow$ SUB	0.014	None
SUB $\rightarrow$ FA	0.061	Small

Source: Authors' SmartPLS 4 analysis of the survey data ($N = 357$).

4.9. Hypothesis Testing

Table 13 reports the original bootstrap estimates. Cybersecurity literacy ($\beta = 0.236$, $p = 0.003$), perceived fintech security ($\beta = 0.383$, $p < 0.001$), and secure user behaviour ($\beta = 0.250$, $p < 0.001$) have positive conditional associations with fintech adoption, supporting H1a, H1b, and H2. Institutional trust has a small negative estimate with substantial uncertainty ($\beta = -0.011$, $p = 0.870$), so H1c is not supported. These significance decisions should be considered alongside the small f^2 values for the supported adoption paths.

Table 13. Path coefficients and hypothesis testing.

Hypothesis	Structural Path	Coefficient	t-Statistic	p-Value	Result
H1a	CL $\rightarrow$ FA	0.236	3.004	0.003	Supported
Context	CL $\rightarrow$ SUB	0.493	7.098	<0.001	Context path
H1c	IT $\rightarrow$ FA	-0.011	0.164	0.870	Not Supported
Context	IT $\rightarrow$ SUB	0.224	2.590	0.010	Context path
H1b	PFS $\rightarrow$ FA	0.383	4.310	<0.001	Supported
Context	PFS $\rightarrow$ SUB	0.150	1.727	0.084	Context path
H2	SUB $\rightarrow$ FA	0.250	3.561	<0.001	Supported

Source: Authors' SmartPLS 4 analysis of the survey data ($N = 357$).

For secure user behaviour, the CL coefficient is positive and significant ($\beta = 0.493$, $p < 0.001$), as is the IT coefficient ($\beta = 0.224$, $p = 0.010$). The PFS coefficient is positive but does not reach the 5% threshold ($\beta = 0.150$, $p = 0.084$). These coefficients form the first part of the proposed indirect associations.

4.10. Mediation Effects Assessment

The specific indirect associations are reported in Table 14. The CL $\rightarrow$ SUB $\rightarrow$ FA estimate is 0.123 ($p = 0.001$), supporting H3a. The PFS $\rightarrow$ SUB $\rightarrow$ FA estimate is 0.037 ($p = 0.117$), and the IT $\rightarrow$ SUB $\rightarrow$ FA estimate is 0.056 ($p = 0.063$); H3b and H3c are therefore not supported at the 5% level. These results concern products of coefficients in the cross-sectional model.

Table 14. Specific indirect effects.

Hypothesis	Indirect Path	Coefficient	t-Statistic	p-Value	Result
H3a	CL → SUB → FA	0.123	3.196	0.001	Supported
H3c	IT → SUB → FA	0.056	1.862	0.063	Not Supported
H3b	PFS → SUB → FA	0.037	1.566	0.117	Not Supported

Source: Authors' SmartPLS 4 analysis of the survey data ($N = 357$).

The significant literacy pathway is consistent with an association connecting reported capability, protective practices, and fintech participation. However, the data do not establish that literacy precedes secure behaviour or that secure behaviour subsequently causes adoption. The non-significant indirect estimates also do not establish that the corresponding mechanisms are absent in other settings or samples.

Measurement Invariance and Tenure Comparisons

Configural comparability was established through a common instrument and identical model and data treatment. All 15 construct-by-pair comparisons satisfy compositional invariance: observed correlations range from 0.998006 to 0.999904 and exceed their permutation-based 5th-percentile values (Table A1). All variance-equality checks pass, but six mean-equality checks do not (Table A2). These concern FA for G1–G2; CL, PFS, SUB, and FA for G1–G3; and CL for G2–G3. Consequently, partial measurement invariance supports standardized path comparisons, while full invariance is not established across the three groups. The full-sample estimates are retained as aggregate associations in this convenience sample, rather than as evidence of an identical model distribution in each tenure group.

Table 15 reports all three pairwise contrasts for each focal path. The original one-tailed PLS-MGA probabilities are retained for transparency, together with the two-sided values in the archived exports. For CL → SUB, the G1–G3 difference is -0.331 , with one-tailed probability 0.969 but two-sided $p = 0.062$. For PFS → FA, the G1–G2 difference is -0.423 , with one-tailed probability 0.974 but two-sided $p = 0.053$. The original hypotheses stated that relationships differed without specifying the direction of each pairwise contrast. The revised interpretation therefore uses two-sided tests; none of the nine focal contrasts is significant at 0.05. The supplementary permutation tests lead to the same significance decisions.

Table 15. Complete comparisons of the three focal paths across tenure groups.

Path	Pair	β A	β B	Δ A – B	p_1	p_2	p Perm.
CL → SUB	G1–G2	0.262	0.594	-0.332	0.944	0.112	0.129
CL → SUB	G1–G3	0.262	0.594	-0.331	0.969	0.062	0.060
CL → SUB	G2–G3	0.594	0.594	0.000	0.498	0.997	0.998
PFS → FA	G1–G2	0.177	0.601	-0.423	0.974	0.053	0.077
PFS → FA	G1–G3	0.177	0.429	-0.252	0.872	0.255	0.238
PFS → FA	G2–G3	0.601	0.429	0.171	0.223	0.446	0.467
IT → FA	G1–G2	0.133	0.000	0.133	0.250	0.499	0.495
IT → FA	G1–G3	0.133	-0.115	0.249	0.075	0.149	0.125
IT → FA	G2–G3	0.000	-0.115	0.116	0.278	0.557	0.529

Source: Authors' archived SmartPLS bootstrap MGA results and supplementary permutation reanalysis. G1 < 1 year; G2 1–3 years; G3 > 3 years. p_1 is the original one-tailed PLS-MGA probability; p_2 is the exported two-sided value. Decisions use $p_2 < 0.05$; no contrast meets this threshold. Permutation tests are also two-sided. Differences use unrounded coefficients.

The four-band analysis further qualifies the apparent tenure patterns (Table A3). The CL → SUB coefficients are 0.315, 0.074, 0.594, and 0.594 for the <6-month, 6–12-month, 1–3-

year, and >3-year groups, respectively. The corresponding PFS $\rightarrow$ FA coefficients are 0.075, 0.596, 0.601, and 0.429. These point estimates do not form a simple increasing sequence. Two contrasts have unadjusted permutation p -values below 0.05, but neither survives Holm adjustment across the 18 focal comparisons. All four-band compositional checks pass (Table A4), although the smaller groups reduce precision. The sensitivity analysis therefore does not establish a stable tenure moderation pattern.

RQ1 remains exploratory. The results do not provide sufficient two-sided evidence of differences across the primary tenure groups, and they do not establish equivalence of the structural coefficients. The original classifications of the two selected tenure comparisons as simply supported have therefore been withdrawn. Table 16 summarizes the revised hypothesis families and the exploratory research question.

Table 16. Summary of hypotheses.

Hypothesis/Question	Relationship	Result
H1a	CL $\rightarrow$ FA	Supported; small f^2
H1b	PFS $\rightarrow$ FA	Supported; small f^2
H1c	IT $\rightarrow$ FA	Not supported
H2	SUB $\rightarrow$ FA	Supported; small f^2
H3a	CL $\rightarrow$ SUB $\rightarrow$ FA	Supported indirect association
H3b	PFS $\rightarrow$ SUB $\rightarrow$ FA	Not supported
H3c	IT $\rightarrow$ SUB $\rightarrow$ FA	Not supported
RQ1	Three focal tenure comparisons	No significant two-sided primary contrasts; exploratory

Source: Authors' analysis. Supported refers to statistical support for the specified association at the 5% level, not a causal effect. H1a–c correspond to former H1–H3; H2 to former H4; H3a–c to former H5–H7; RQ1 consolidates former H8–H10.

5. Discussion and Conclusions

This study examined security-related fintech participation among 357 respondents living primarily in urban Bangladesh. The findings identify positive conditional associations of cybersecurity literacy, perceived fintech security, and secure user behaviour with fintech adoption. The indirect association through secure user behaviour is also supported for cybersecurity literacy. At the same time, the individual adoption effect sizes are small, the direct institutional trust coefficient is not significant, and the complete two-sided tenure comparisons do not establish moderation. These qualifications are central to the interpretation of the study.

Cybersecurity literacy has both a direct association with adoption and an indirect association through reported protective behaviour. This suggests that users' knowledge, awareness, and confidence are relevant to how they report participating in fintech services. The medium f^2 value for the literacy–behaviour path provides more substantial incremental explanatory evidence than the small direct literacy–adoption contribution. However, the findings do not establish that a literacy intervention would produce a corresponding increase in adoption.

Secure user behaviour is positively associated with adoption after the other predictors are considered. Respondents who report stronger protective practices also tend to report greater fintech participation. This is consistent with the proposed behavioural reasoning, but both constructs were reported by the same respondents at the same time. Therefore, the association could also reflect shared response tendencies, reverse ordering, or characteristics not included in the model.

The significant CL $\rightarrow$ SUB $\rightarrow$ FA product identifies one supported indirect association within the model. It does not demonstrate that protective practices are the process through

which knowledge causes later use. In particular, continued use could itself be associated with greater familiarity with security practices. The distinction matters because the present study describes a pattern that a future longitudinal or intervention study would need to examine more directly.

Perceived fintech security has the largest estimated direct coefficient among the included adoption predictors, while its incremental f^2 value remains small. This combination indicates that platform assurance is relevant within the fitted model without implying an overwhelming or independently causal role. Providers may therefore find it useful to communicate the purpose of visible security features clearly, although the present survey cannot assess whether those features are technically effective or whether communication changes behaviour.

The indirect PFS $\rightarrow$ SUB $\rightarrow$ FA association is not statistically supported. Accordingly, the results do not establish that favourable perceptions of platform security are associated with adoption through respondents' own protective practices. They also do not demonstrate that users transfer responsibility for security to providers, because responsibility attribution was not measured. Perceived platform assurance and reported protective behaviour should therefore remain distinct dimensions in interpreting the findings.

Institutional trust has no significant direct association with adoption after cybersecurity literacy, perceived security, and secure behaviour are included. This result concerns the conditional coefficient in the specified model. It does not establish that trust is unimportant, that regulation is ineffective, or that respondents have experienced institutional failure. The overlap between trust and perceived security provides an additional reason to avoid broad conclusions from this single coefficient.

Institutional trust is positively associated with secure user behaviour, but its specific indirect association with adoption does not reach the 5% threshold. Consequently, the evidence for the trust pathway is mixed. A more detailed study could separate confidence in providers, confidence in regulators, and confidence in complaint handling, rather than treating these related evaluations as one construct.

The tenure analysis illustrates the importance of interpreting point estimates together with measurement checks and uncertainty. Although some coefficients appear different across groups, none of the nine primary comparisons is significant under two-sided bootstrap MGA. Measurement comparability supports making the comparisons, but it does not by itself establish that the structural coefficients differ.

The finer tenure categories also show why the broader labels require caution. The two first-year groups have different point estimates, and the four-band pattern is not a simple sequence from less to more experienced users. These differences remain exploratory after accounting for the number of comparisons. The results therefore do not justify assigning distinct security strategies to the three tenure categories as an empirically established consequence of this study.

The model accounts for a meaningful proportion of variance within the achieved sample, while several individual contributions are modest. These statements concern different aspects of the results and should not be treated as interchangeable. The study did not evaluate predictions for unseen respondents, nonlinear relationships, or interactions beyond the specified group comparisons. Such possibilities remain open even where a linear conditional coefficient is small or non-significant.

The cross-sectional design also prevents an interpretation of tenure as within-person development. Respondents with longer use were not observed when they were new users, and the analysis cannot determine whether differences reflect learning, selection, cohort composition, or unmeasured characteristics. The findings therefore provide evidence

about associations among existing users, rather than demonstrating that coping capability develops through repeated fintech use.

5.1. Theoretical Implications

The theoretical contribution of this study is to bring security-related capability, perceived platform assurance, institutional confidence, and reported protective behaviour into one account of fintech participation. The supported literacy indirect association is consistent with PMT-informed reasoning about capability and protective action. However, the instrument does not measure the full appraisal structure of PMT, and the tenure results do not establish an experiential extension of that theory. The findings also qualify the interpretation of trust by distinguishing a non-significant conditional adoption coefficient from the broader relevance of institutions. These contributions concern the scope and interpretation of the observed relationships, rather than the establishment of new causal mechanisms.

5.2. Managerial and Policy Implications

The findings suggest that fintech service providers may benefit from considering user guidance and platform assurance together. Clear explanations of authentication, suspicious links, and safe transaction practices are consistent with the security-related dimensions examined here. However, the small incremental adoption effects do not establish the size of any benefit from a particular intervention. Providers should evaluate proposed changes through user testing and behavioural outcomes, while avoiding the assumption that the present tenure categories identify distinct needs for every user.

From a policy perspective, accessible complaint handling, fraud reporting, and dispute resolution remain relevant areas for further investigation. The non-significant conditional trust coefficient should not be used to conclude that formal protection is unnecessary or ineffective. The study measures respondents' confidence in these arrangements, rather than their actual performance. Future evaluations could therefore connect perceptions with service records and user outcomes to assess which forms of protection are associated with safer participation.

5.3. Limitations and Future Research

This study has some limitations. First, cross-sectional associations cannot establish causal direction or within-person change. The indirect estimates should therefore not be treated as identified causal mediation effects. Second, tenure was recorded in categories, without exact duration, usage frequency, or a longitudinal record; the four-band check reveals sensitivity in point estimates and does not resolve potential confounding. Third, the convenience sample is concentrated in Dhaka, among younger respondents and students, which limits generalization to rural, older, or less connected users. Fourth, all constructs rely on self-report, creating possible recall, social desirability, and common-method influences. Fifth, FA combines recent use, future intention, and continuance preferences among existing users; future work should separate these outcomes and examine non-users. Sixth, institutional trust and perceived security overlap empirically, and a more differentiated instrument could improve their interpretation. Seventh, personal fraud exposure and the actual performance of institutional protection were not measured. Finally, incomplete equality of composite means limits claims about a common distribution across tenure groups, and the analysis provides no out-of-sample predictive assessment. Future research should combine broader sampling with longitudinal, behavioural, and predictive validation, including careful examination of possible nonlinear and interaction patterns.

Author Contributions: Conceptualization, T.S.A. and M.S.I.; methodology, T.S.A. and S.K.G.; software, T.S.A.; validation, T.S.A., M.S.I. and S.K.G.; formal analysis, T.S.A.; investigation, T.S.A. and

S.K.G.; resources, T.S.A. and S.K.G.; data curation, T.S.A.; writing—original draft preparation, T.S.A. and M.S.I.; writing—review and editing, M.S.I., T.S.A., S.K.G. and M.M.A.; visualization, T.S.A.; supervision, M.S.I. and M.M.A.; project administration, S.K.G. and M.S.I. All authors have read and agreed to the published version of the manuscript.

Funding: The Open access publication funding was supported by Örebro University, Sweden.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Ethics Committee of Research Cell, Northern University Bangladesh (protocol code NUB/RC/EA/2026/025 and date of 20 June 2025).

Informed Consent Statement: Informed consent was waived due to the fact that the survey was anonymous. Prior to completing the questionnaire, participants were informed about the purpose of the research, the voluntary nature of their participation, and the confidentiality and anonymity of their responses. Participants were informed that they could decline to participate or discontinue the survey at any time. Only individuals aged 18 years or older who voluntarily agreed to participate proceeded with and completed the questionnaire. No personally identifiable information was collected, and the data were used solely for academic research purposes.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Measurement Invariance and Robustness Results

All additional estimates use the unchanged 357-response dataset and the seven-path model. The Python Mode A implementation uses standardized indicators and path weighting and reproduces all seven full-sample and all 21 primary group coefficients to the reported SmartPLS precision. For MICOM Step 2, the group-specific weight vectors are applied to a common pooled indicator matrix, following the X_w correlation formulation [33] and the cSEM implementation [38]. Step 3 uses standardized pooled-fit composite scores. Each pair uses 5000 permutations with group sizes fixed. Primary pair seeds are 20261006–20261008; four-band pair seeds are 20261016–20261021, following the pair order in Tables A3 and A4. Monte Carlo probabilities use the correction $(1 + \text{count})/(5001)$. No estimates failed to converge. Step 3 results are interpreted against their permutation reference intervals, rather than by whether those intervals include zero.

Table A1. Compositional invariance for the primary tenure groups.

Pair	Construct	c	5% Quantile	p	Step 2
G1–G2	CL	0.999333	0.995179	0.740	Yes
G1–G2	PFS	0.999367	0.998131	0.414	Yes
G1–G2	IT	0.999904	0.999165	0.817	Yes
G1–G2	SUB	0.999234	0.997347	0.448	Yes
G1–G2	FA	0.999725	0.997934	0.815	Yes
G1–G3	CL	0.998547	0.996716	0.319	Yes
G1–G3	PFS	0.999600	0.997564	0.756	Yes
G1–G3	IT	0.998661	0.998307	0.101	Yes
G1–G3	SUB	0.999776	0.996137	0.908	Yes
G1–G3	FA	0.999504	0.997944	0.525	Yes
G2–G3	CL	0.998006	0.996725	0.158	Yes
G2–G3	PFS	0.999414	0.997999	0.514	Yes
G2–G3	IT	0.999316	0.998836	0.189	Yes
G2–G3	SUB	0.999781	0.997046	0.883	Yes
G2–G3	FA	0.998986	0.997906	0.263	Yes

Source: Authors’ supplementary reanalysis. Step 2 passes when c is at least the 5% permutation quantile. Configural comparability was maintained for every pair.

Table A2. Equality of composite means and variances for the primary groups.

Pair	Construct	Δ Mean	95% Interval	Log Variance Ratio	95% Interval	Equal Mean/Variance
G1–G2	CL	−0.207	[−0.259, 0.261]	0.050	[−0.472, 0.489]	Yes/Yes
G1–G2	PFS	−0.226	[−0.257, 0.259]	0.114	[−0.513, 0.561]	Yes/Yes
G1–G2	IT	−0.107	[−0.250, 0.257]	0.090	[−0.430, 0.458]	Yes/Yes
G1–G2	SUB	−0.079	[−0.267, 0.262]	−0.087	[−0.447, 0.468]	Yes/Yes
G1–G2	FA	−0.344	[−0.265, 0.262]	0.184	[−0.429, 0.452]	No/Yes
G1–G3	CL	−0.491	[−0.238, 0.242]	0.372	[−0.527, 0.492]	No/Yes
G1–G3	PFS	−0.352	[−0.243, 0.252]	0.369	[−0.541, 0.512]	No/Yes
G1–G3	IT	−0.066	[−0.237, 0.246]	0.103	[−0.390, 0.376]	Yes/Yes
G1–G3	SUB	−0.276	[−0.244, 0.244]	0.255	[−0.470, 0.451]	No/Yes
G1–G3	FA	−0.517	[−0.241, 0.246]	0.423	[−0.470, 0.446]	No/Yes
G2–G3	CL	−0.287	[−0.258, 0.256]	0.323	[−0.635, 0.578]	No/Yes
G2–G3	PFS	−0.119	[−0.251, 0.257]	0.253	[−0.594, 0.554]	Yes/Yes
G2–G3	IT	0.040	[−0.259, 0.264]	0.007	[−0.429, 0.420]	Yes/Yes
G2–G3	SUB	−0.191	[−0.253, 0.258]	0.354	[−0.539, 0.500]	Yes/Yes
G2–G3	FA	−0.178	[−0.256, 0.262]	0.240	[−0.639, 0.575]	Yes/Yes

Source: Authors' supplementary reanalysis. Differences are first group minus second; the variance statistic is $\log(\text{var A}/\text{var B})$. Equality is supported when the observed statistic falls inside its permutation reference interval. Failure of six mean checks prevents full invariance; partial invariance supports standardized path comparisons.

Table A3. Four-band sensitivity analysis for all focal path comparisons.

Bands A/B	Path	β A	β B	p Perm.	p Holm
>3 years/1–3 years	CL → SUB	0.594	0.594	0.998	1.000
>3 years/1–3 years	PFS → FA	0.429	0.601	0.451	1.000
>3 years/1–3 years	IT → FA	−0.115	0.000	0.538	1.000
>3 years/6–12 months	CL → SUB	0.594	0.074	0.007	0.119
>3 years/6–12 months	PFS → FA	0.429	0.596	0.612	1.000
>3 years/6–12 months	IT → FA	−0.115	0.121	0.325	1.000
>3 years/<6 months	CL → SUB	0.594	0.315	0.168	1.000
>3 years/<6 months	PFS → FA	0.429	0.075	0.138	1.000
>3 years/<6 months	IT → FA	−0.115	0.103	0.227	1.000
1–3 years/6–12 months	CL → SUB	0.594	0.074	0.053	0.845
1–3 years/6–12 months	PFS → FA	0.601	0.596	0.990	1.000
1–3 years/6–12 months	IT → FA	0.000	0.121	0.668	1.000
1–3 years/<6 months	CL → SUB	0.594	0.315	0.258	1.000
1–3 years/<6 months	PFS → FA	0.601	0.075	0.037	0.632
1–3 years/<6 months	IT → FA	0.000	0.103	0.662	1.000
6–12 months/<6 months	CL → SUB	0.074	0.315	0.545	1.000
6–12 months/<6 months	PFS → FA	0.596	0.075	0.090	1.000
6–12 months/<6 months	IT → FA	0.121	0.103	0.943	1.000

Source: Authors' supplementary reanalysis. Group sizes: <6 months, 69; 6–12 months, 56; 1–3 years, 102; >3 years, 130. All tests are two-sided; Holm adjustment covers the full family of 18 comparisons. Unadjusted results are exploratory.

Table A4. Compositional checks for all four-band comparisons.

Bands A/B	Construct	c	5% Quantile	p	Step 2
>3 years/1–3 years	CL	0.998006	0.996830	0.153	Yes
>3 years/1–3 years	PFS	0.999414	0.997992	0.511	Yes
>3 years/1–3 years	IT	0.999316	0.998884	0.186	Yes
>3 years/1–3 years	SUB	0.999781	0.997009	0.868	Yes
>3 years/1–3 years	FA	0.998986	0.997893	0.258	Yes

Table A4. Cont.

Bands A/B	Construct	c	5% Quantile	p	Step 2
>3 years/6–12 months	CL	0.999588	0.995907	0.851	Yes
>3 years/6–12 months	PFS	0.998630	0.996732	0.278	Yes
>3 years/6–12 months	IT	0.998883	0.997440	0.253	Yes
>3 years/6–12 months	SUB	0.999925	0.992603	0.991	Yes
>3 years/6–12 months	FA	0.999680	0.997323	0.768	Yes
>3 years/<6 months	CL	0.996867	0.993116	0.242	Yes
>3 years/<6 months	PFS	0.998364	0.994210	0.432	Yes
>3 years/<6 months	IT	0.998364	0.995734	0.380	Yes
>3 years/<6 months	SUB	0.998916	0.992766	0.697	Yes
>3 years/<6 months	FA	0.999232	0.995701	0.602	Yes
1–3 years/6–12 months	CL	0.998729	0.994593	0.520	Yes
1–3 years/6–12 months	PFS	0.999215	0.998078	0.311	Yes
1–3 years/6–12 months	IT	0.999756	0.999431	0.288	Yes
1–3 years/6–12 months	SUB	0.999882	0.996920	0.938	Yes
1–3 years/6–12 months	FA	0.998984	0.997656	0.271	Yes
1–3 years/<6 months	CL	0.999385	0.991412	0.885	Yes
1–3 years/<6 months	PFS	0.997304	0.996565	0.090	Yes
1–3 years/<6 months	IT	0.999907	0.998629	0.926	Yes
1–3 years/<6 months	SUB	0.998123	0.996079	0.230	Yes
1–3 years/<6 months	FA	0.999752	0.996205	0.932	Yes
6–12 months/<6 months	CL	0.998344	0.988463	0.767	Yes
6–12 months/<6 months	PFS	0.995266	0.994717	0.069	Yes
6–12 months/<6 months	IT	0.999594	0.997429	0.762	Yes
6–12 months/<6 months	SUB	0.998504	0.992832	0.576	Yes
6–12 months/<6 months	FA	0.998723	0.995122	0.485	Yes

Source: Authors' supplementary reanalysis. The identical indicator specification and data treatment were maintained. All compositional checks pass; this supports comparing standardized paths without implying equal group means or identical coefficients.

References

- Hossain, M.J.; Rifat, R.H.; Mugdho, M.H.; Jahan, M.; Rasel, A.A.; Rahman, M.A. Cyber Threats and Scams in FinTech Organizations: A brief overview of financial fraud cases, future challenges, and recommended solutions in Bangladesh. In Proceedings of the 2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Jakarta, Indonesia, 16–17 November 2022. [CrossRef]
- Transparency International Bangladesh. Service Charges in a Policy-Weakened Sector 15 Times Higher than Banks; The Sector Needs Complete Overhaul to Protect Customer Rights. 2025. Available online: <https://www.ti-bangladesh.org/index.php/en/articles/press-release/7262> (accessed on 27 August 2026).
- World Bank. World Development Indicators. Population, Urban Population Share, GDP per Capita, Individuals Using the Internet, and Mobile Cellular Subscriptions; Series SP.POP.TOTL, SP.URB.TOTL.IN.ZS, NY.GDP.PCAP.CD, IT.NET.USER.ZS, and IT.CEL.SETS.P2. Available online: <https://data.worldbank.org/indicator> (accessed on 6 October 2026).
- World Bank. The Global Findex Database 2025: Connectivity and Financial Inclusion in the Digital Economy. Country-Level Data, 2021 and 2024 Waves. Available online: <https://www.worldbank.org/en/publication/globalfindex/download-data> (accessed on 6 October 2026).
- Hanif, Y.; Lallie, H.S. Security factors on the intention to use mobile banking applications in the UK older generation (55+). *Technol. Soc.* **2021**, *67*, 101693. [CrossRef]
- Xenakis, A.; Vlachos, V.; Roig, P.J.; Alcaraz, S. Addressing the necessity of cybersecurity literacy: The case of ETTCS CyberTeach project. *Inf. Comput. Secur.* **2025**, *33*, 427–451. [CrossRef]
- Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behavior: A comparative study. *J. Comput. Inf. Syst.* **2020**, *62*, 82–97. [CrossRef]
- Shafik, W. Security, privacy, and trust in fintech. In *FinTech and Financial Inclusion*; Routledge: Abingdon, UK, 2025; pp. 216–233. [CrossRef]
- Devlin, J.F.; Roy, S.K.; Sekhon, H.; Moin, S.M.A.; Sahiner, M. Trust and FinTech: A review and research agenda. *Electron. Mark.* **2025**, *35*, 62. [CrossRef]

10. Featherman, M.S.; Pavlou, P.A. Predicting e-services adoption: A perceived risk facets perspective. *Int. J. Hum.-Comput. Stud.* **2003**, *59*, 451–474. [\[CrossRef\]](#)
11. Pavlou, P.A. Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *Int. J. Electron. Commer.* **2003**, *7*, 101–134. [\[CrossRef\]](#)
12. Zhao, S.; Zhao, D. FinTech, Household Finance and Financial Consumer Protection: Opportunities, Challenges and Countermeasures. In *The Household Finance Issues in China*; Springer: Singapore, 2024; pp. 35–50. [\[CrossRef\]](#)
13. Huda, S.S.; Hossain, M.F.; Rahman, S.M.; Nazmul, S.B.; Hasan, R. An evaluation of FinTech in Bangladesh. *J. Inf. Technol. Teach. Cases* **2024**, *16*, 40–45. [\[CrossRef\]](#)
14. Becker, G.S. *The Economic Approach to Human Behavior*; University of Chicago Press: Chicago, IL, USA, 1976.
15. Smith, R.C.; Walter, I.; DeLong, G. *Global Banking*, 3rd ed.; Oxford University Press: New York, NY, USA, 2012. [\[CrossRef\]](#)
16. Davis, F.D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* **1989**, *13*, 319–340. [\[CrossRef\]](#) [\[PubMed\]](#)
17. Venkatesh, V.; Morris, M.G.; Davis, G.B.; Davis, F.D. User acceptance of information technology: Toward a unified view. *MIS Q.* **2003**, *27*, 425–478. [\[CrossRef\]](#)
18. Rogers, R.W. A protection motivation theory of fear appeals and attitude change. *J. Psychol.* **1975**, *91*, 93–114. [\[CrossRef\]](#) [\[PubMed\]](#)
19. Rogers, E.M. *Diffusion of Innovations*, 3rd ed.; Free Press: New York, NY, USA, 1983.
20. Bhuiyan, I.; Ahmed, H.; Hoque, A.; Bhuiyan, T. Trust, Security, and Nonlinear Retention Dynamics in FinTech Neobanking: An Explainable Machine Learning (XAI) Approach. *FinTech* **2026**, *5*, 53. [\[CrossRef\]](#)
21. Maqsood, S.; Chiasson, S. Design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens. *ACM Trans. Priv. Secur.* **2021**, *24*, 28. [\[CrossRef\]](#)
22. Nguyen, T.T.; Thi, T.; Huyen, T.; Khanh, T.; Uyen, T.; Minh, T. Digital literacy, online security behaviors and e-payment intention. *J. Open Innov.* **2024**, *10*, 100292. [\[CrossRef\]](#)
23. Khan, N.F.; Ikram, N.; Saleem, S.; Zafar, S. Cyber-security and risky behaviors in a developing country context: A Pakistani perspective. *Secur. J.* **2022**, *36*, 373–405. [\[CrossRef\]](#) [\[PubMed\]](#)
24. Liu, Q.; Chan, K.-C.; Chimhundu, R. Fintech research: Systematic mapping, classification, and future directions. *Financ. Innov.* **2024**, *10*, 24. [\[CrossRef\]](#)
25. Rahardja, U.; Miftah, M.; Rakhmansyah, M.; Zanubiya, J. Revolutionizing financial services with big data and fintech: A scalable approach to innovation. *ADI J. Recent Innov.* **2025**, *6*, 118–129. [\[CrossRef\]](#)
26. Savitha, B.; Hawaldar, I.T.; Kumar, K., N. Continuance intentions to use FinTech peer-to-peer payments apps in India. *Heliyon* **2022**, *8*, e11654. [\[CrossRef\]](#) [\[PubMed\]](#)
27. Alrashedi, A.; Iskandar, P. Key factors influencing fintech adoption among Saudi banks: A conceptual framework. *Humanit. Soc. Sci. Commun.* **2025**, *12*, 1194. [\[CrossRef\]](#)
28. Jafri, J.A.; Amin, S.I.M.; Rahman, A.A.; Nor, S.M. A systematic literature review of the role of trust and security on FinTech adoption in banking. *Heliyon* **2024**, *10*, e22980. [\[CrossRef\]](#) [\[PubMed\]](#)
29. Fukuyama, F. *Trust: The Social Virtues and the Creation of Prosperity*; Free Press: New York, NY, USA, 1995.
30. Egelman, S.; Harbach, M.; Peer, E. Behavior ever follows intention? In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, 7–12 May 2016. [\[CrossRef\]](#)
31. Dodge, C.; Fisk, N.; Burruss, G.W.; Moule, R.K.; Jaynes, C.M. What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminol. Public Policy* **2023**, *22*, 849–868. [\[CrossRef\]](#)
32. Ringle, C.M.; Wende, S.; Becker, J.-M. *SmartPLS 4*; SmartPLS: Bönningstedt, Germany, 2024. Available online: <https://www.smartpls.com> (accessed on 10 January 2026).
33. Henseler, J.; Ringle, C.M.; Sarstedt, M. Testing measurement invariance of composites using partial least squares. *Int. Mark. Rev.* **2016**, *33*, 405–431. [\[CrossRef\]](#)
34. Holm, S. A simple sequentially rejective multiple test procedure. *Scand. J. Stat.* **1979**, *6*, 65–70.
35. Hair, J.F.; Risher, J.J.; Sarstedt, M.; Ringle, C.M. When to use and how to report the results of PLS-SEM. *Eur. Bus. Rev.* **2019**, *31*, 2–24. [\[CrossRef\]](#)
36. Henseler, J.; Ringle, C.M.; Sarstedt, M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J. Acad. Mark. Sci.* **2015**, *43*, 115–135. [\[CrossRef\]](#)
37. Cohen, J. *Statistical Power Analysis for the Behavioral Sciences*, 2nd ed.; Lawrence Erlbaum Associates: Mahwah, NJ, USA, 1988.
38. cSEM Development Team. testMICOM Source Implementation, postestimate_test_MICOM.R. Available online: https://github.com/FloSchuberth/cSEM/blob/master/R/postestimate_test_MICOM.R (accessed on 6 October 2026).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.