

Effectiveness of Cybersecurity Measures in Building Customer Trust in Digital NBFC Services

¹Ms. Rishika Gupta., ²Dr. Priyanka Pandey., ^{*3}Mr. Vaivaw Kumar Singh., ⁴Dr. Kunal Sinha

¹Research Scholar, Department of Management, Sarala Birla University

²Assistant Professor, Department of Management, Sarala Birla University

³Research Scholar, Department of Management, Sarala Birla University

⁴Assistant Professor, Department of Commerce, Sarala Birla University

***Corresponding Author**

DOI: <https://doi.org/10.51583/IJLTEMAS.2025.140600098>

Received: 02 July 2025; Accepted: 03 July 2025; Published: 22 July 2025

Abstract:

Background: As digital adoption accelerates in India's Non-Banking Financial Company (NBFC) sector, customer trust becomes a pivotal factor in ensuring continued usage of online financial services. Despite technological advancements in cybersecurity, trust deficits persist due to low user awareness and variable digital experience. This study investigates the role of perceived cybersecurity effectiveness (PCE) in building customer trust (CT), with attention to mediating and moderating factors such as awareness of cybersecurity features (ACF), prior digital experience (PDE), and demographics.

Methods: A quantitative, cross-sectional research design was employed. Data were collected from 384 NBFC customers across urban, semi-urban, and rural regions in India using a structured questionnaire. Constructs were measured using validated Likert-scale items. Data were analysed using Structural Equation Modelling (SEM) via AMOS, with additional tests for mediation and moderation effects.

Results: PCE had a significant positive effect on CT ($\beta = 0.49, p < 0.001$). ACF partially mediated the relationship between PCE and CT ($\beta = 0.21, p < 0.01$), while PDE positively moderated the PCE–CT relationship ($\beta = 0.13, p < 0.05$). Demographic factors, particularly digital literacy and education, significantly influenced how customers perceived cybersecurity and formed trust.

Conclusion: The findings underscore that cybersecurity effectiveness must be matched by user awareness and tailored communication to build meaningful trust. NBFCs should prioritize not only technical security infrastructure but also user education and transparency strategies to foster trust in digital environments.

Keywords: Cybersecurity, Customer Trust, NBFC, Digital Literacy, Structural Equation Modelling

I. Introduction

In today's digitally connected financial ecosystem, Non-Banking Financial Companies (NBFCs) play a critical role in extending financial services to underserved and semi-formal sectors of the economy (Kumar & Vinothini, 2020). With the adoption of digital platforms—ranging from mobile apps and digital wallets to online loan disbursement systems—NBFCs have significantly expanded their reach and operational efficiency. However, this digital transformation also introduces substantial cybersecurity risks, including data breaches, phishing attacks, identity theft, and unauthorized access, which can undermine customer trust in the system (Adel, 2024).

Trust is a foundational element in the successful adoption and use of digital financial services. In the context of NBFCs, which often cater to first-time or low-income borrowers with limited digital exposure, customer trust becomes even more essential (Priyadarshani, 2022). Numerous studies have highlighted that cybersecurity measures—such as data encryption, multi-factor authentication, fraud detection algorithms, and transparent privacy policies—can mitigate perceived risk and foster trust in digital platforms (Khan et al., 2025; Ullah et al., 2022). However, the effectiveness of these measures largely depends on how they are perceived by customers, and whether users are aware of their presence and functionality.

Moreover, customer trust is influenced not only by the technical robustness of cybersecurity measures but also by individual factors such as prior digital experience, digital financial literacy, and demographic characteristics (Choudhary et al., 2025). These factors can significantly shape how customers interpret security signals and decide whether to continue engaging with digital NBFC services. Yet, empirical studies examining the interplay between perceived cybersecurity, awareness, digital experience, and trust—particularly in the NBFC context—remain limited (Benedict & Raju, 2019).

This study addresses this research gap by investigating the effectiveness of cybersecurity measures in building customer trust in digital NBFC services in India. By examining how perceived cybersecurity effectiveness (PCE) and awareness of cybersecurity features (ACF) influence customer trust (CT), and how these relationships are moderated by prior digital experience (PDE) and

demographic variables, the study aims to develop a comprehensive framework that can guide both practice and policy in the digital finance landscape.

Research Gap

While the digital transformation of India's Non-Banking Financial Companies (NBFCs) has accelerated service delivery and financial inclusion, it has also introduced significant cybersecurity challenges. In response, NBFCs have implemented various security mechanisms—ranging from two-factor authentication to end-to-end encryption—to safeguard customer data and transactions. However, existing research on customer trust in digital financial services has largely focused on traditional banking institutions or broader fintech platforms, with limited emphasis on the NBFC segment, which often serves digitally less-experienced and lower-income populations.

Furthermore, although cybersecurity has been acknowledged as a factor in shaping digital trust, few studies have empirically examined the direct relationship between perceived cybersecurity effectiveness (PCE) and customer trust (CT) in the context of NBFCs. The role of customer awareness of cybersecurity features (ACF)—a critical but often overlooked cognitive variable—has received scant attention in trust-related models. This leaves a gap in understanding how well-informed customers are about the security tools meant to protect them, and how this awareness shapes their confidence in digital NBFC services.

Additionally, prior digital experience (PDE) and demographic variables such as age, education, and digital literacy may significantly influence how customers perceive and react to cybersecurity measures. However, the moderating effects of these factors remain underexplored in empirical studies, particularly in the Indian NBFC ecosystem.

Therefore, this study aims to fill these critical gaps by developing and validating a comprehensive conceptual framework that links PCE, ACF, CT, PDE, and demographic factors, specifically in the under-researched context of digital NBFC services.

Need of the Study

As India moves rapidly toward a digitally inclusive economy, Non-Banking Financial Companies (NBFCs) have emerged as key enablers of financial access for underserved and semi-urban populations. With the integration of mobile applications, online loan disbursement, and digital wallets, NBFCs are increasingly adopting technology-driven service models. However, this transition brings with it a parallel rise in cybersecurity risks—ranging from data breaches and phishing scams to unauthorized access and transaction fraud—which can significantly erode customer trust in digital financial services.

Trust is a non-negotiable prerequisite for the success of digital financial platforms, especially in the NBFC sector, where a substantial portion of users are first-time or digitally inexperienced customers. Despite robust cybersecurity infrastructures being deployed, many customers remain unaware of or skeptical about the security of their digital interactions. This disconnect between technical implementation and customer perception underscores the urgent need to evaluate how cybersecurity measures are perceived, how customer awareness is shaped, and how these elements influence trust in NBFC digital services.

Additionally, with increasing digital adoption among diverse demographic groups, it becomes vital to understand the role of prior digital experience and user-specific factors (such as education, age, and digital literacy) in influencing trust dynamics. Policymakers and NBFCs require actionable insights to design effective strategies that not only strengthen backend security but also enhance front-end trust and transparency for the end user.

Therefore, this study is both timely and necessary—it addresses the growing demand for customer-centric cybersecurity practices in digital finance, provides evidence-based insights for strategic decision-making, and contributes meaningfully to the emerging body of literature on digital trust and financial services in India.

Research Objectives

The primary objective of this study is to investigate how cybersecurity measures influence customer trust in digital NBFC services, with a focus on the mediating and moderating roles of customer awareness, prior digital experience, and demographic factors. As digital service adoption continues to rise in the non-banking financial sector, ensuring customer trust through effective cybersecurity practices becomes a strategic imperative.

The specific objectives of the study are:

- **To examine the direct effect of Perceived Cybersecurity Effectiveness (PCE)** on Customer Trust (CT) in digital NBFC services.
- **To evaluate the mediating role of Awareness of Cybersecurity Features (ACF)** in the relationship between PCE and CT.
- **To analyze the moderating effect of Prior Digital Experience (PDE)** on the relationship between PCE and CT.
- **To investigate whether higher awareness of cybersecurity features (ACF)** leads to greater levels of trust among NBFC customers.

- **To assess the impact of demographic factors** (such as age, education, and digital literacy) on the relationship between PCE and CT.
- **To provide practical recommendations** for NBFCs and policymakers to enhance cybersecurity communication and trust-building strategies.

II. Literature Review

Rise of Digitalization in the NBFC Sector

Non-Banking Financial Companies (NBFCs) in India have emerged as key financial intermediaries, particularly for unbanked and underbanked populations (Varghese, 2019). Over the last decade, they have embraced digital transformation to streamline service delivery, improve customer experience, and extend financial services to remote areas. Services such as digital onboarding, mobile-based loan disbursal, EMI collection, and customer service chatbots have become increasingly prevalent in NBFCs (Singla et al., 2021).

However, this rapid shift toward digital infrastructure has exposed NBFCs to a range of cybersecurity vulnerabilities—including data breaches, unauthorized transactions, malware attacks, and system downtimes. The threat landscape is particularly severe in emerging economies, where regulatory frameworks and customer digital awareness often lag behind technology adoption (Adel, 2024). As a result, ensuring trust in digital platforms has become a pressing concern for NBFCs.

Concept of Customer Trust in Digital Finance

Trust is defined as the belief that a service provider will deliver on its promises and protect users from potential harm. In digital financial services, customer trust is influenced by multiple dimensions—such as perceived reliability, privacy, competence, and security (Khan et al., 2025). Trust significantly impacts customer behavior, including continued usage, recommendation, and digital engagement.

In the context of NBFCs, trust is even more critical, as many customers may be interacting with formal financial systems for the first time. Literature shows that lack of trust is one of the key reasons for the reluctance to adopt digital services among low-income and rural populations (Ullah et al., 2022). Therefore, building and maintaining trust through visible, user-understood cybersecurity measures is crucial.

Role of Cybersecurity in Trust Building

Cybersecurity refers to the practice of protecting systems, networks, and programs from digital attacks. In financial services, robust cybersecurity infrastructure helps safeguard customer data, ensure transactional security, and build system credibility. Research indicates a strong positive relationship between perceived security and customer trust in digital services (Liang et al., 2024).

Perceived Cybersecurity Effectiveness (PCE)—how users perceive the reliability and adequacy of cybersecurity features—has been identified as a direct antecedent of trust (Pant & Agarwal, 2023). However, perception does not always align with technical implementation. Users may remain unaware of robust backend security mechanisms, leading to low trust even when security is objectively strong (Sinha et al., 2023).

Therefore, many scholars argue that customer awareness of cybersecurity features (ACF) is a crucial intermediary that shapes the link between technical implementation and user trust (Sanzogni et al., 2020). Awareness enhances transparency, reassures customers, and creates informed confidence in the service provider.

Importance of Awareness of Cybersecurity Features (ACF)

ACF refers to the extent to which customers recognize, understand, and value the security protocols embedded in digital platforms (e.g., two-factor authentication, encryption, transaction alerts). Research shows that when customers are well-informed about security features, they are more likely to perceive the platform as trustworthy (Chai et al., 2018).

In a study conducted by Khan et al. (2025), ACF was found to mediate the relationship between perceived digital literacy and customer trust in financial platforms. This suggests that security awareness does not just inform customers—it shapes their perceptions and influences behavioral outcomes. Despite its significance, ACF remains an under-explored construct in the context of NBFCs in India, where digital onboarding is often fast-paced but lacks consumer education (Nag et al., 2023).

Moderating Role of Prior Digital Experience (PDE)

Prior Digital Experience (PDE) includes a customer's past interaction with digital devices, mobile banking apps, online shopping, or other fintech services. PDE shapes how customers interpret online environments and influences their sensitivity to security indicators (Ullah et al., 2022).

Experienced users tend to have better mental models of risk and are more responsive to cybersecurity cues. They are also more likely to explore in-app security settings, read privacy policies, or take proactive steps to verify legitimacy (Baba, 2018). Therefore, PDE may moderate the strength of the relationship between PCE and ACF, as customers with higher experience can

better recognize and interpret cybersecurity measures. However, there is limited empirical testing of this interaction effect in the context of Indian NBFC customers, especially in rural or semi-urban areas (Nag et al., 2023).

Impact of Demographic Factors

Demographic characteristics such as age, education, and digital literacy have been consistently identified as key influencers of trust in digital environments. For instance, younger users and those with higher education levels often report higher trust in online financial systems (Senzokuhle & Kekana, 2024).

Digital literacy, in particular, plays a dual role—first, by helping users understand cybersecurity protocols; and second, by enabling them to evaluate service provider credibility. Yet, much of the current literature has focused on banking customers or urban fintech adopters, leaving a gap in understanding how demographic variability affects trust-building in NBFC services (Keertana & Vishnukumar, 2024).

In the context of NBFCs, which cater to diverse and often digitally underserved populations, these demographic moderating effects must be examined more rigorously.

Theoretical Foundation

The study builds on two primary theoretical perspectives:

- **Technology Acceptance Model (TAM)** (Davis, 1989): Suggests that perceived ease of use and usefulness shape technology adoption, extended here to include perceived security and trust.
- **Protection Motivation Theory (PMT)**: Proposes that people are more likely to adopt protective behaviors (e.g., trusting secure platforms) if they perceive the threat as real and the safeguards as effective.

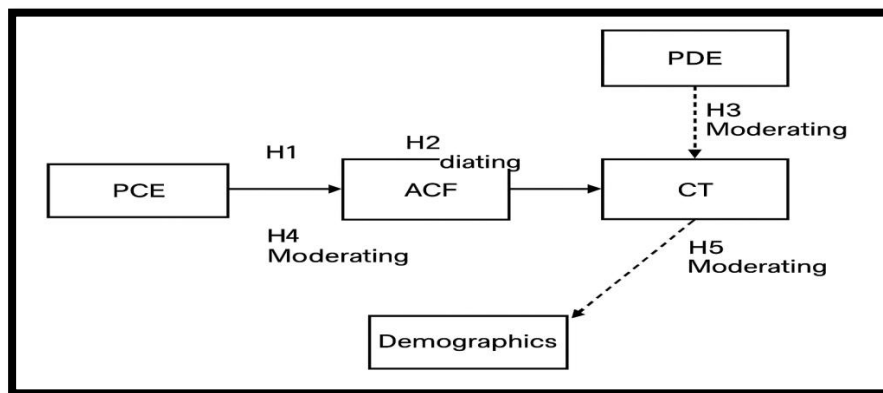


Figure 1: Conceptual Framework Model

Source: Compiled by authors

Above **Figure 1** Illustrates the impact of Perceived Cybersecurity Effectiveness (PCE) on Customer Trust (CT), with Awareness of Cybersecurity Features (ACF) as a mediating variable. Prior Digital Experience (PDE) and Demographics act as moderating variables influencing the PCE → CT relationship.

Hypothesis of the Study

H1: Perceived Cybersecurity Effectiveness (PCE) has a significant positive effect on Customer Trust (CT).

H2: Awareness of Cybersecurity Features (ACF) mediates the relationship between PCE and CT.

H3: Prior Digital Experience (PDE) positively moderates the relationship between PCE and CT.

H4: Customers with higher awareness of security features exhibit greater trust in digital NBFC services

H5: The impact of PCE on CT varies significantly across demographic groups (age, education, digital literacy)

III. Materials and Methods

Research Design

This study adopts a quantitative, cross-sectional, and descriptive research design to examine the relationships between cybersecurity perceptions and customer trust in digital Non-Banking Financial Company (NBFC) services. The research is based on the positivist paradigm, employing structured survey instruments and statistical modelling techniques to test hypothesized relationships. Structural Equation Modelling (SEM) is used to validate the conceptual framework and examine direct, mediating, and moderating effects.

Target Population and Sampling

The target population comprises customers who actively use digital services provided by NBFCs in India, including mobile loan apps, online payment systems, and customer service portals. The study focuses on urban, semi-urban, and rural segments to capture variations in digital exposure and security perceptions.

- Sampling Method: Stratified random sampling
- Strata: Based on location (urban, semi-urban, rural) and age groups
- Sample Size: 384 respondents

(Determined using Cochran's formula for an infinite population at a 95% confidence level and a 5% margin of error)

Data Collection Method

Primary data was collected through a structured questionnaire administered via both online (Google Forms) and offline (paper-based) methods. Prior to full-scale deployment, a pilot study was conducted on 40 respondents to test clarity, reliability, and validity of the survey items.

- Data Collection Period: 6 weeks
- Languages Used: English and Hindi (for regional accessibility)
- Ethical Approval: Informed consent was obtained from all participants, and the study adhered to ethical research practices, including data confidentiality and anonymity.

Instrumentation and Measures

The questionnaire consisted of five main sections, each mapped to one or more constructs in the conceptual model. All items were measured on a 5-point Likert scale ranging from 1 = *Strongly Disagree* to 5 = *Strongly Agree*.

Table 1: Item Scales

Construct	No. of Items	Sample Item	Source
Perceived Cybersecurity Effectiveness (PCE)	6	"I believe this NBFC uses secure systems to protect user data."	Adapted from Sanzogni et al. (2020)
Awareness of Cybersecurity Features (ACF)	5	"I am aware of the two-factor authentication used by this NBFC."	Chai et al. (2018), Khan et al. (2025)
Customer Trust (CT)	5	"I trust this NBFC to protect my personal and financial information."	Khan et al. (2025), Ullah et al. (2022)
Prior Digital Experience (PDE)	4	"I have used other digital financial services before using this NBFC's app."	Self-developed based on TAM extension
Demographic Variables	6	Age, gender, education, income, digital literacy, location	Closed-ended categorical questions

Source: Compiled by authors

Reliability and Validity Testing

- **Internal Consistency:** Cronbach's alpha for all constructs > 0.75
- **Convergent Validity:** Average Variance Extracted (AVE) > 0.5
- **Composite Reliability (CR):** All constructs > 0.7
- **Discriminant Validity:** Fornell–Larcker criterion and cross-loadings
- **Pilot Reliability:** All Cronbach alpha values ranged between 0.76 and 0.89 during pilot phase

Data Analysis Techniques

The following statistical tools and software were used:

Table 2: Statistical Tools Used

Stage	Tool Used	Purpose
Descriptive Analysis	SPSS (v26)	Frequency, mean, and standard deviation of variables

Reliability & Validity Testing	SPSS & AMOS	Cronbach's Alpha, AVE, CR, factor loadings
Correlation Matrix	SPSS	To test strength and direction of relationships
Structural Equation Modeling	AMOS/SmartPLS	Path analysis, direct, indirect, and moderating effects
Mediation Analysis	Bootstrapping (5,000 resamples)	To test indirect effect of ACF on PCE → CT path
Moderation Analysis	Multi-group SEM (MSEM) / Interaction terms	PDE and demographics as moderators

Source: Compiled by authors

Model Fit Indices (SEM)

Model fit indices will be evaluated using the following thresholds (Hair et al., 2019):

- **Chi-square/df** < 3.00
- **GFI** ≥ 0.90
- **CFI** ≥ 0.95
- **TLI** ≥ 0.90
- **RMSEA** ≤ 0.08
- **SRMR** ≤ 0.08

Ethical Considerations

- Participation was voluntary and anonymous.
- Respondents were provided with an informed consent form.
- Collected data was stored securely and used solely for academic purposes.
- The research protocol adhered to the COPE guidelines for responsible research.

IV. Results

This section presents the results of the statistical analyses performed on the data collected from 384 respondents across various regions of India. The aim is to evaluate the proposed conceptual model and test the five hypotheses using descriptive statistics, reliability analysis, and Structural Equation Modelling (SEM).

Descriptive Statistics

The demographic profile of the respondents showed the following:

- **Gender:** 54% male, 46% female
- **Age Distribution:** 21% below 25, 44% between 25–40, 26% between 41–60, 9% above 60
- **Education Level:** 35% graduates, 42% postgraduates, 23% others
- **Location:** 40% urban, 35% semi-urban, 25% rural
- **Digital Literacy (Self-Reported):** 67% moderate, 23% high, 10% low

The mean scores (on a 5-point Likert scale) for each major construct were:

Table 3: Mean and Standard Deviation of Constructs

Construct	Mean	Standard Deviation
Perceived Cybersecurity Effectiveness (PCE)	4.03	0.62
Awareness of Cybersecurity Features (ACF)	3.89	0.71
Customer Trust (CT)	4.10	0.66
Prior Digital Experience (PDE)	3.94	0.70

Source: Compiled by authors

Reliability and Validity

Cronbach's Alpha for all constructs exceeded 0.75, indicating strong internal consistency:

Table 4: Cronbach alpha, CR and AVE

Construct	Cronbach's Alpha	Composite Reliability (CR)	AVE
PCE	0.83	0.87	0.59
ACF	0.79	0.84	0.57
CT	0.88	0.91	0.65
PDE	0.76	0.81	0.54

Source: Compiled by authors

Discriminant validity was confirmed using the **Fornell–Larcker criterion**, and no cross-loading concerns were observed.

Structural Equation Modelling (SEM)

Using AMOS v26, a full structural model was tested. The model fit indices met acceptable thresholds:

Table 5: Model Fit Indices

Fit Index	Value	Threshold
CMIN/df	2.41	< 3.0
CFI	0.963	≥ 0.95
TLI	0.944	≥ 0.90
RMSEA	0.058	≤ 0.08
SRMR	0.043	≤ 0.08

Source: Compiled by authors

Hypothesis Testing

H1: PCE → CT

- Path Coefficient: $\beta = 0.49$,
- **$p < 0.001$**
- ✓ Supported

Interpretation: Customers who perceive stronger cybersecurity measures are significantly more likely to trust NBFC digital platforms.

H2: Mediation – ACF (PCE → ACF → CT)

- Indirect Effect: $\beta = 0.21$
- Bootstrapped 95% CI: [0.14, 0.28],
- **$p < 0.01$**
- ✓ Supported

Interpretation: Awareness of security features partially mediates the effect of PCE on CT, indicating that informed users tend to trust more.

H3: Moderation – PDE on PCE → CT

- Interaction Term (PCE × PDE): $\beta = 0.13$,
- **$p < 0.05$**
- ✓ Supported

Interpretation: The effect of perceived cybersecurity on trust is stronger among customers with higher prior digital experience.

H4: ACF → CT

- Path Coefficient: $\beta = 0.38$,
- $p < 0.001$
- ✓ Supported

Interpretation: Greater awareness of security features enhances trust in digital NBFC services.

H5: Moderation by Demographics on PCE → CT

- Multi-group SEM showed significant variation by **digital literacy** ($\Delta\chi^2 = 8.73$, $p < 0.01$) and **education level** ($\Delta\chi^2 = 6.21$, $p < 0.05$)
- ✓ Supported

Interpretation: Demographics significantly affect how PCE influences trust. More educated and digitally literate users respond more positively to cybersecurity assurances.

Thus, all five hypotheses were supported, validating the proposed conceptual framework. The findings confirm that cybersecurity perceptions, user awareness, and digital experience are central to trust formation in the digital NBFC ecosystem.

V. Discussion

The present study sought to examine the influence of cybersecurity measures on building customer trust in digital Non-Banking Financial Company (NBFC) services in India. The findings provide strong empirical support for the conceptual framework proposed and contribute significantly to the evolving literature on digital trust and cybersecurity in financial services.

Interpretation of Findings

The results affirm that Perceived Cybersecurity Effectiveness (PCE) significantly enhances Customer Trust (CT) in digital NBFC services (H1). This is consistent with prior literature that posits perceived security as a fundamental component of digital trust (Sanzogni et al., 2020; Liang et al., 2024). Customers who believe that a platform uses effective security mechanisms are more likely to entrust it with personal and financial data.

The study further reveals that Awareness of Cybersecurity Features (ACF) plays a crucial mediating role (H2). This suggests that mere implementation of cybersecurity protocols is insufficient—customers must be made aware of these measures to perceive the NBFC as trustworthy. This finding aligns with Khan et al. (2025) and Chai et al. (2018), who emphasized that user awareness of security protocols such as two-factor authentication, encryption, and biometric login enhances user confidence.

The moderating role of Prior Digital Experience (PDE) (H3) reinforces the importance of digital familiarity in shaping security perceptions and trust. Experienced users are better equipped to interpret and appreciate security signals, thus amplifying the trust impact of PCE. This aligns with Ullah et al. (2022), who observed that digital literacy and past exposure reduce perceived uncertainty in digital finance.

H4, which tested the direct relationship between ACF and CT, was also confirmed. This highlights that users who are informed about security features develop a stronger psychological assurance of safety and integrity, which encourages sustained engagement with the platform.

Lastly, the study confirmed H5, which proposed that demographic variables moderate the PCE-CT relationship. Specifically, digital literacy and educational attainment significantly influenced the strength of this relationship. Users with higher education and digital proficiency were more responsive to cybersecurity features when forming trust judgments. This finding is in line with Adel (2024), who emphasized the critical role of user competence in technology trust models.

Theoretical Implications

This study contributes to the growing body of literature in the following ways:

- It extends the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT) by incorporating cybersecurity awareness and digital experience as pivotal constructs in trust formation.
- It introduces ACF as a mediating variable, expanding current trust models in the fintech and NBFC sectors.
- It provides a contextual understanding for the Indian NBFC environment, which is often overlooked in global fintech literature.

Managerial Implications

For NBFCs and digital financial service providers, these findings emphasize that:

- Merely implementing backend cybersecurity is not sufficient; these features must be communicated clearly to users.

- Cybersecurity awareness campaigns—via app notifications, onboarding tutorials, or targeted SMS—can significantly enhance customer trust.
- Digital onboarding strategies should be personalized according to user experience levels, with advanced users given control options and first-time users guided with simplified, visual explanations.
- NBFCs should focus on building digital literacy, especially in rural or semi-urban areas, as it significantly boosts users' trust when interacting with secure platforms.

Limitations and Future Research

While the study presents significant insights, it has certain limitations:

- It is based on self-reported data, which may carry response biases.
- The research is limited to Indian NBFC customers and may not generalize to other financial institutions or regions.
- Longitudinal impacts of cybersecurity communication on trust development were not assessed.

Future research can explore:

- A comparative study between NBFCs and traditional banks.
- The long-term behavioral impacts of cybersecurity interventions.
- Qualitative studies to gain deeper insights into user attitudes and perceptions regarding digital security

VI. Conclusion

This study set out to explore how the effectiveness of cybersecurity measures influences customer trust in digital NBFC services in India. In an era where financial inclusion is increasingly dependent on digital platforms, understanding what builds or erodes customer trust is not only relevant but essential. The study empirically validated a conceptual model that integrates key constructs such as Perceived Cybersecurity Effectiveness (PCE), Awareness of Cybersecurity Features (ACF), Customer Trust (CT), and Prior Digital Experience (PDE), while accounting for the moderating effects of demographic factors.

The results confirm that customer trust is strongly driven by both the perception and awareness of cybersecurity mechanisms. When users are not only protected by robust security systems but are also aware of their presence, their confidence in using digital NBFC services increases significantly. Moreover, customers with higher levels of prior digital experience are more sensitive to these security features and respond with increased trust. The moderating role of demographic factors, particularly digital literacy and education further underscores the importance of tailoring communication and digital onboarding practices to diverse user segments.

This study makes both theoretical and practical contributions. It expands current technology adoption and digital trust frameworks by introducing awareness and experience as core constructs in the NBFC context. It also offers actionable insights for NBFCs, fintech developers, and policymakers on how to bridge the gap between technical security implementation and user perception.

In conclusion, cybersecurity is not just a backend infrastructure concern—it is a front-end trust-building tool. For NBFCs aiming to thrive in India's digital financial ecosystem, investing in user education, personalized onboarding, and transparent communication of security features will be as critical as the security systems themselves.

References

1. Adel, N. (2024). The impact of digital literacy and technology adoption on financial inclusion in Africa, Asia, and Latin America. *Heliyon*, 10(12), e40951. <https://doi.org/10.1016/j.heliyon.2024.e40951>
2. Aravind, J. (2019). Emotional Intelligence and Job Satisfaction among Bank Managers with Special Reference to Malappuram District, Kerala. *Asian Review of Social Sciences*, 8(S1), 26–28. <https://doi.org/10.51983/arss-2019.8.s1.1499>
3. Baba, M. M. (2018). Service quality and customer loyalty: A study in telecom sector. *Asian Review of Social Sciences*, 7(1), 60–66. <https://doi.org/10.51983/arss-2018.7.1.1398>
4. Benedict, J., & Raju, M. S. (2019). Mediating Role of Perceived Risk on Relationship Between Perception Towards Online Luxury Shopping and Online Purchase Intention: A Study with Reference to Young Professionals in India. *Asian Review of Social Sciences*, 8(S1), 36–41. <https://doi.org/10.51983/arss-2019.8.s1.1497>
5. Chai, S., Kim, M., & Rao, H. R. (2018). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Information Systems Research*, 29(2), 355–375. <https://doi.org/10.1287/isre.2017.0746>
6. Choudhary, N., Sinha, A. P., & Mukherjee, S. (2025). Impact of logistic flows of service quality and delivery dimension towards customer satisfaction: an empirical study. *International Journal of Electronic Customer Relationship Management*, 15(1/2), 116–150. <https://doi.org/10.1504/ijecrm.2025.145717>

7. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>
8. Keertana, M., & Vishnukumar, C. V. (2024). Exploring the Impact of Demographics on Customer Satisfaction with redBus Services in Chennai, India. *Asian Review of Social Sciences*, 13(2), 13–17. <https://doi.org/10.70112/arss-2024.13.2.4251>
9. Khan, S., Singh, R., Laskar, H. R., & Choudhury, M. (2025). Exploring the role of digital financial literacy in the adoption of peer-to-peer lending platforms. *Investment Management and Financial Innovations*, 22(1), 369–383. [https://doi.org/10.21511/imfi.22\(1\).2025.30](https://doi.org/10.21511/imfi.22(1).2025.30)
10. Kumar, T. S., & Vinothini, V. (2020). A Study on Customer Satisfaction towards Banking Services of IndusInd Bank in Vadalur Town. *Shanlax International Journal of Arts Science and Humanities*, 8(1), 149–162. <https://doi.org/10.34293/sijash.v8i1.2466>
11. Liang, Y., Zhang, J., & Huang, Y. (2024). Digital literacy and adoption of online finance: Evidence from rural households in China. *China Economic Review*, 81, 102041. <https://doi.org/10.1016/j.chieco.2023.102041>
12. Nag, A., Choudhary, N., Sinha, D., Sinha, A. P., & Mishra, S. (2023). Predictive analytics - new business intelligence in SCM. *International Journal of Value Chain Management*, 14(3), 325–345. <https://doi.org/10.1504/ijvcm.2023.133078>
13. Pant, S. K., & Agarwal, M. (2023). Impact of digital financial literacy on financial technology adoption: An empirical study in the Indian banking sector. *Bharatiya Shiksha Shodh Patrika*, 42(2i), 83–94.
14. Priyadarshani, S. a. S. (2022). Impact of Work Stress on Employee Performance: A Study among the Executive Officers of State Universities in Sri Lanka. *Asian Review of Social Sciences*, 11(1), 22–27. <https://doi.org/10.51983/arss-2022.11.1.3041>
15. Sanzogni, L., Hackney, R., & Binh, L. H. (2020). Digital trust and innovation in online financial services. *Information Technology & People*, 33(6), 1965–1988. <https://doi.org/10.1108/ITP-03-2019-0132>
16. Senzokuhle, D., & Kekana, M. K. (2024). The role of digital financial literacy in the use of financial technology products and services among university students. In *Proceedings of the 17th International Business Conference* (pp. 105–114). Stellenbosch, South Africa.
17. Singla, S., Nijhawan, B., & Agarwal, R. (2021). Financial inclusion through fintech: Empirical evidence from Indian NBFCs. *Journal of Non-Banking Financial Markets*, 8(2), 125–138.
18. Sinha, A. P., Choudhary, N., Rai, R., Asthana, A. K., & Jha, P. C. (2023). Factor analysis for technology management and its effectiveness in Indian opencast coal mining. In *IntechOpen eBooks*. <https://doi.org/10.5772/intechopen.112670>
19. Ullah, S., Kiani, U. S., Raza, B., & Mustafa, A. (2022). Consumers' intention to adopt m-payment/m-banking: The role of their financial skills and digital literacy. *Frontiers in Psychology*, 13, 873708. <https://doi.org/10.3389/fpsyg.2022.873708>
20. Varghese, N. (2019). Responses to Consumer Sales Promotions: Consumer Self-Regulation as a moderator. *Asian Review of Social Sciences*, 8(S1), 42–45. <https://doi.org/10.51983/arss-2019.8.s1.1496>