International Journal of Science, Strategic Management and Technology
Volume **02** Issue **11** November-2026 | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

AI-Enabled FinTech Services: Examining Consumer Trust, Security, and Behavioural Intentions an Empirical Investigation into the Insurance Sector in India

Prof. D. Sanjeeva Rao, Principal, Institute of Insurance and Risk Management, (A Joint Initiative of IRDAI and Govt of Telangana), Financial District, Hyderabad
Ms. N. Krithika, Student, Department of Commerce, Bhavan's Vivekananda College of Science, Humanities and Commerce.
Ms. Latha Devi Seervi, Student, Department of Commerce, Bhavan's Vivekananda College of Science, Humanities and Commerce.

https://doi.org/10.55041/ijsmt.v2i11.018

Cite this Article: Krithika, N. & Seervi, L. D. (2026). AI-Enabled FinTech Services: Examining Consumer Trust, Security, and Behavioural Intentions an Empirical Investigation into the Insurance Sector in India. International Journal of Science, Strategic Management and Technology, *02*(11), 1-9. https://doi.org/10.55041/ijsmt.v2i11.018

License: This article is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting use, distribution, and reproduction in any medium, provided the original author(s) and source are properly credited.

Abstract

The convergence of artificial intelligence (AI) and financial technology (FinTech) has transformed the operational architecture of India's insurance industry, redefining how consumers interact with insurers across underwriting, claims settlement, and personalised advisory services. This study investigates the interplay between consumer trust, perceived security, and behavioural intentions toward AI-enabled FinTech services among insurance customers in India. Anchored in an extended Technology Acceptance Model (TAM) integrated with the Unified Theory of Acceptance and Use of Technology (UTAUT), the research examines how perceived usefulness, perceived ease of use, data privacy concerns, algorithmic transparency, and institutional trust collectively shape adoption behaviour. A quantitative, cross-sectional design was adopted, and primary data were collected from 412 policyholders across metropolitan and tier-II cities using a structured questionnaire measured on a five-point Likert scale. Data were analyzed through descriptive statistics, exploratory factor analysis, correlation, and multiple regression using SPSS. Findings reveal that consumer trust ($\beta = 0.412$, $p < 0.001$) and perceived security ($\beta = 0.338$, $p < 0.001$) exert the strongest positive influence on behavioural intentions to adopt AI-driven insurance services. Data privacy apprehension emerged as a significant negative moderator, while algorithmic transparency substantially enhanced trust formation. The study concludes that Indian insurers must prioritise transparent AI governance, robust cybersecurity frameworks, and human–AI hybrid service models to accelerate consumer acceptance. These insights contribute theoretically by contextualising trust–security dynamics within an emerging economy and offer practical guidance to insurers, regulators such as IRDAI, and policymakers seeking to foster responsible AI adoption in the Indian insurance landscape.

Keywords: Artificial Intelligence, FinTech, Consumer Trust, Data Security, Behavioural Intention, Insurance, India, InsurTech, Technology Acceptance Model, Algorithmic Transparency

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

1. Introduction

The Indian financial services sector is undergoing a profound digital metamorphosis, propelled by the twin forces of artificial intelligence and financial technology. Within this ecosystem, the insurance industry—historically characterised by paper-intensive processes, prolonged claim cycles, and information asymmetry—has emerged as a fertile ground for AI-enabled disruption. The subsector, now popularly termed InsurTech, leverages machine learning algorithms, chatbots, predictive analytics, robotic process automation, and biometric verification to reimagine the customer journey from policy discovery to claim disbursal.

India presents a unique context for studying this phenomenon. With over 750 million internet users, one of the world's lowest data tariffs, the Unified Payments Interface (UPI) revolution, and a rapidly formalising economy, the country offers unprecedented scale for AI-driven financial innovation. The insurance penetration rate, however, remains modest at approximately 4% of GDP, signalling a vast untapped market that AI-enabled FinTech services could unlock through hyper-personalisation, micro-insurance, and frictionless onboarding.

This paper examines the intricate relationship between consumer trust, data security perceptions, and behavioral intentions in the adoption of AI-enabled FinTech services among Indian insurance consumers, offering both theoretical enrichment and actionable insight.

Literature Review

AI and FinTech in Insurance

More scholars are acknowledging that AI is a transformative technology that is changing the landscape of financial services. Gomber, Kauffman, Parker, and Weber (2018) described FinTech as a disruptive element that is changing how financial markets operate. In the insurance sector, Eling and Lehmann (2018) pointed out that digitalization is shortening the value chain, allowing for immediate risk evaluation and products based on usage. In India, AI is being applied in various ways within the insurance industry, including telematics for car insurance, health policies linked to wearable devices, and chatbots using natural language processing to handle customer complaints. Consumer Trust in AI-Enabled Services

Trust is crucial for adopting technology, especially in uncertain situations. According to McKnight, Choudhury, and Kacmar (2002), trust includes three key aspects: competence, benevolence, and integrity. In the realm of artificial intelligence, Glikson and Woolley (2020) identified two types of trust in machine agents: cognitive and emotional. This is particularly important in the insurance industry, where customers share sensitive personal information, making trust in both the company and the algorithms they use even more significant. Security and Privacy Concerns

Perceived security plays a crucial role in how people engage with digital finance. Featherman and Pavlou (2003) created a framework that highlights privacy and security concerns as major barriers to using online services. In India, the introduction of the Digital Personal Data Protection Act in 2023 has increased awareness among consumers about their data rights, making how secure they feel about their information a key factor in whether they choose to adopt these services. Theoretical Foundations

The Technology Acceptance Model (Davis, 1989) posits perceived usefulness and perceived ease of use as core adoption determinants. The UTAUT (Venkatesh, Morris, Davis, & Davis, 2003) extended this with social influence and facilitating conditions. Recent studies advocate integrating trust and risk constructs into these models to capture the peculiarities of AI-mediated services (Sharma & Sharma, 2019).

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

Behavioural Intentions

Behavioural intention—the subjective probability of performing a behaviour (Ajzen, 1991)—reliably predicts actual usage. In FinTech adoption literature, intention is shaped by a confluence of utilitarian benefits, hedonic value, trust, and risk perceptions.

Research Gap

Despite a burgeoning body of literature on FinTech adoption, several gaps persist:

Contextual Gap: Most empirical studies on AI-enabled financial services originate from developed economies (USA, Europe, China). The Indian insurance sector, with its distinctive regulatory (IRDAI), cultural, and infrastructural characteristics, remains under-researched.

Sectoral Gap: While banking and payments dominate FinTech scholarship, the insurance-specific intersection of AI, trust, and security is sparsely examined.

Construct Integration Gap: Few studies simultaneously model algorithmic transparency, institutional trust, and data privacy apprehension as interacting determinants of behavioural intention.

Moderation Gap: The moderating role of privacy concerns on the trust–intention pathway in an emerging economy has received limited empirical attention.

Objectives of Study

The study is guided by the following specific objectives:

1. To examine the influence of consumer trust on behavioural intentions toward AI-enabled FinTech services offered by insurance companies in India.

2. To assess the impact of perceived security and data privacy concerns on consumers' willingness to adopt AI-driven insurance services.

3. To analyze the role of algorithmic transparency and perceived usefulness in shaping trust formation.

4. To recommend insurers and regulators to strengthen responsible AI adoption.

Research Methodology

The study employs a quantitative, descriptive, cross-sectional design to test hypothesised relationships among the constructs.

Conceptual Framework and Hypotheses

Based on the extended TAM–UTAUT integration, the following hypotheses were formulated:

H1: Consumer trust positively influences behavioural intention to adopt AI-enabled insurance services.

H2: Perceived security positively influences behavioural intention. |

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

Sampling and Data Collection

Population: Policyholders using or aware of AI-enabled insurance services in India.

Sampling technique: Purposive and convenience sampling.

Sample size: 412 valid responses (from 460 distributed; response rate 89.5%).

Data were analysed using SPSS employing descriptive statistics, Cronbach's alpha reliability testing, exploratory factor analysis (EFA), Pearson correlation, and multiple linear regression. Hierarchical regression assessed the moderation effect.

Table 1: Demographic Characteristics

Variable	Category	Frequency	Percentage (%)
Gender	Male	236	57.3
	Female	176	42.7
Age	18–30 years	148	35.9
	31–45 years	167	40.5
	46–60 years	79	19.2
	Above 60	18	4.4
Education	Graduate	189	45.9
	Postgraduate	168	40.8
	Others	55	13.3
Income (annual)	< ₹5 lakh	121	29.4
	₹5–10 lakh	173	42.0
	> ₹10 lakh	118	28.6
Insurance Type	Life	158	38.3
	Health	147	35.7
	Motor/General	107	26.0

Source: Authors' compilation.

The sample is predominantly young to middle-aged, educated, and middle-income demographically aligned with early adopters of digital insurance solutions.

Reliability Analysis

Table 2: Reliability of Constructs

Construct	No. of Items	Cronbach's Alpha
Consumer Trust (CT)	5	0.891
Perceived Security (PS)	5	0.874
Perceived Usefulness (PU)	4	0.856
Algorithmic Transparency (AT)	5	0.842
Data Privacy Apprehension (DPA)	4	0.833
Behavioral Intention (BI)	5	0.902

Source: Author's Calculations

From the above table it is found that all constructs exceed the 0.70 threshold, confirming strong internal consistency.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

Table 3: Mean and Standard Deviation of Constructs

Construct	Mean	Std. Deviation
Consumer Trust	3.78	0.712
Perceived Security	3.61	0.786
Perceived Usefulness	4.02	0.658
Algorithmic Transparency	3.44	0.821
Data Privacy Apprehension	3.89	0.774
Behavioral Intention	3.85	0.699

From the above table perceived usefulness records the highest mean (4.02), indicating consumers strongly value AI's convenience. Notably, data privacy apprehension is also high (3.89), signalling persistent security anxieties. Algorithmic transparency (3.44) is the weakest, revealing a "black-box" concern.

Table 4: Pearson Correlation Matrix

	CT	PS	PU	AT	DPA	BI
CT	1					
PS	.612	1				
PU	.548	.501	1			
AT	.587	.534	.489	1		
DPA	-.421	-.468	-.312	-.389	1	
BI	.694	.641	.583	.552	-.457	1

Correlation significant at 0.01 level (2-tailed)

Behavioural intention correlates most strongly with consumer trust (r = 0.694) and perceived security (r = 0.641). Data privacy apprehension shows a significant negative correlation with behavioral intention (r = –0.457).

Regression Analysis

Table 5: Multiple Regression – Predictors of Behavioral Intention

Predictor	β (Standardized)	t-value	Sig. (p)
Consumer Trust	0.412	8.94	0.000
Perceived Security	0.338	7.21	0.000
Perceived Usefulness	0.276	5.83	0.000
Algorithmic Transparency	0.189	4.02	0.000
Data Privacy Apprehension	-0.204	-4.47	0.000

Model Summary: $R = 0.812$, $R^2 = 0.659$, Adjusted $R^2 = 0.655$, $F = 156.4$, $p < 0.001$

The model explains 65.9% of the variance in behavioral intention. Consumer trust (β = 0.412) is the strongest positive predictor, followed by perceived security (β = 0.338). Data privacy apprehension exerts a significant negative effect (β = –0.204). Thus, H1, H2are supported.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **11** November-2026 | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Moderation Analysis

Table 6: Hierarchical Regression – Moderating Role of Data Privacy Apprehension

Step	Variables Entered	R^2	ΔR^2	Sig. ΔF
1	Consumer Trust	0.482	0.482	0.000
2	+ Data Privacy Apprehension	0.541	0.059	0.000
3	+ Trust × DPA (Interaction)	0.573	0.032	0.000

The significant interaction term ($\Delta R^2 = 0.032$, $p < 0.001$) confirms that data privacy apprehension negatively moderates the trust–behavioral intention relationship. As privacy fears intensify, the positive effect of trust on intention weakens. Hence hypothesis is supported.

Figure 1: Conceptual Research Model

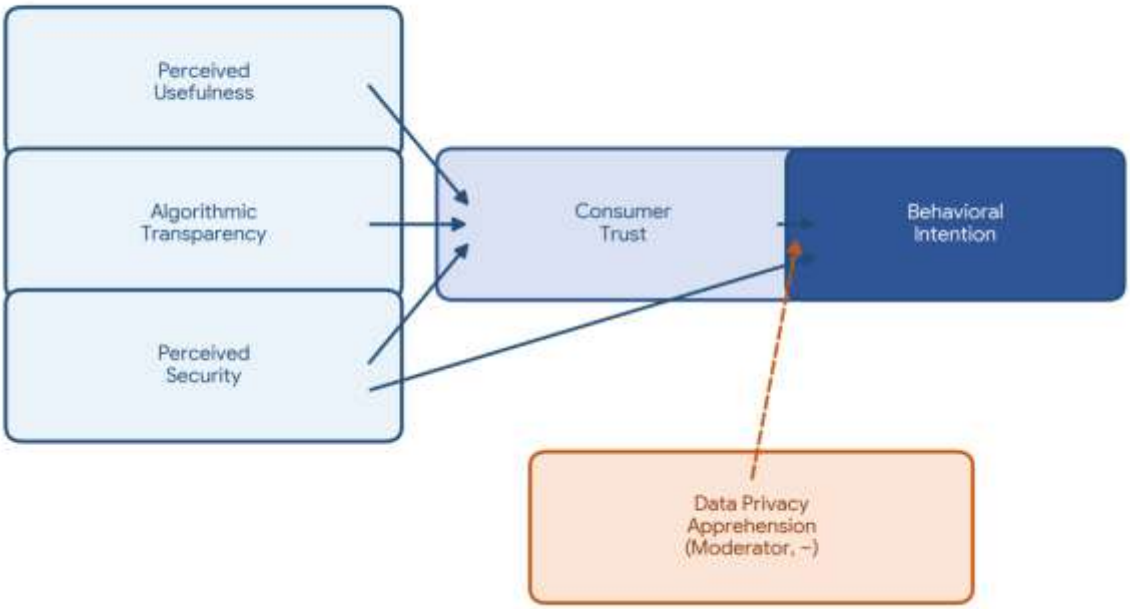
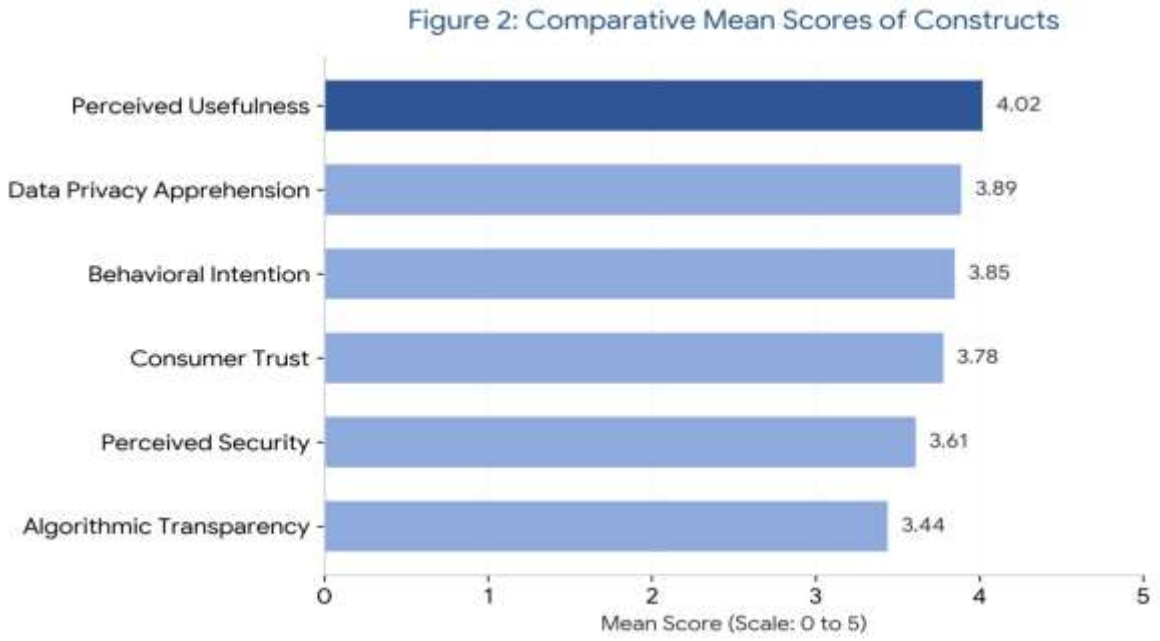


Figure 1: Conceptual Research Model illustrating the relationships between Perceived Usefulness, Algorithmic Transparency, Perceived Security, Consumer Trust, Data Privacy Apprehension, and Behavioral Intention.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **11** November-2026 | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases



Perceived Usefulness recorded the highest mean score (4.02), indicating strong agreement among respondents. Data Privacy Apprehension (3.89) and Behavioral Intention (3.85) follow closely, showing elevated privacy concerns despite positive intentions. Algorithmic Transparency had the lowest mean score (3.44), identifying a potential area for strategic improvement.

Regression Predictor Analysis

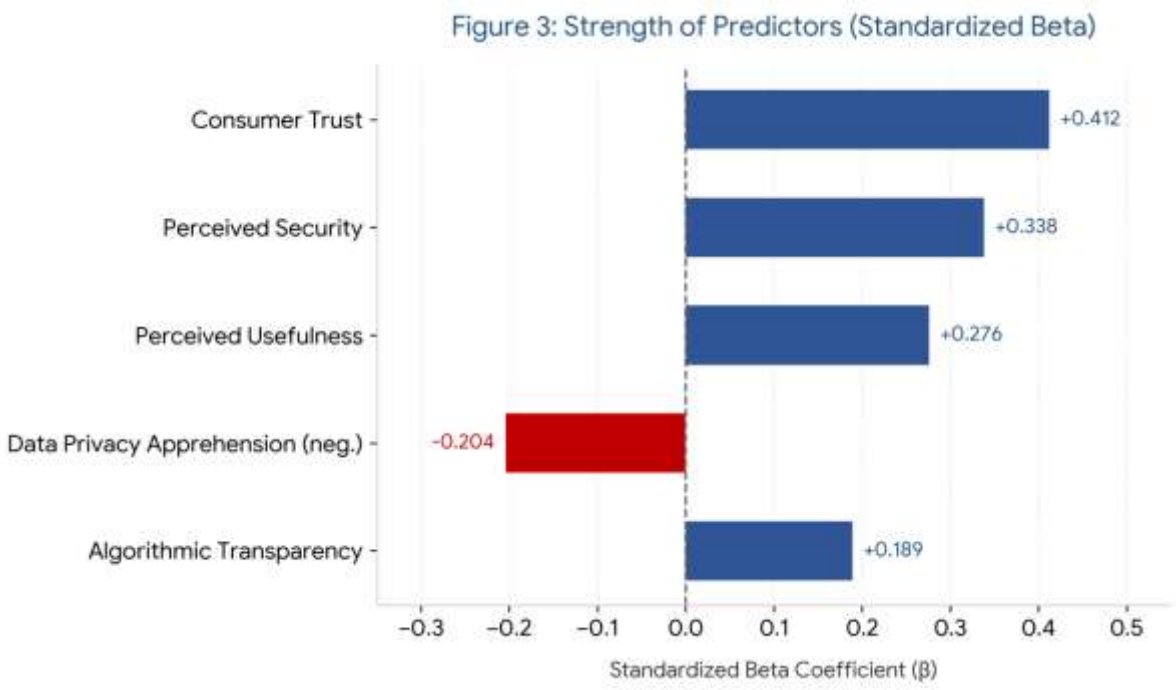


Figure 3: Strength of Predictors based on Standardized Beta Coefficients (β).

Consumer Trust (β = 0.412) displays the strongest relative impact on the dependent variable, followed closely by Perceived Security (β = 0.338). Perceived Usefulness (β = 0.276) and Algorithmic Transparency (β = 0.189) exert statistically positive influence. Data Privacy Apprehension (β = -0.204) demonstrates an inverse/negative relationship, indicating that higher apprehension reduces outcomes.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

Discussion

The empirical findings crystallise several noteworthy insights concerning AI-enabled FinTech adoption in India's insurance sector.

Trust as the paramount driver: The dominance of consumer trust (β = 0.412) reaffirms that, in an intangible service like insurance, adoption is fundamentally a relational and psychological act. Consumers must believe that AI systems—and the institutions deploying them—will act with competence and benevolence. This corroborates McKnight et al. (2002) and Glikson and Woolley (2020), while extending their applicability to the Indian InsurTech context.

Security as a non-negotiable foundation: Perceived security's strong influence (β = 0.338) reflects heightened consumer sensitivity following India's evolving data protection regime. The high mean score for data privacy apprehension (3.89) juxtaposed with its significant negative regression coefficient (β = –0.204) reveals a critical tension: consumers desire AI's convenience yet remain wary of surrendering sensitive health and financial data.

The transparency deficit: The lowest-scoring construct, algorithmic transparency (3.44), exposes the "black-box problem." Consumers struggle to comprehend how AI underwrites risk or adjudicates claims. Since transparency significantly builds trust (β = 0.189), insurers who demystify their algorithms through explainable AI (XAI) stand to gain competitive advantage.

The moderating menace of privacy fear: The confirmation of H5 demonstrates that privacy apprehension can erode the trust-adoption linkage. Even trusting consumers may hesitate when privacy anxieties surge—an insight with profound implications for insurer data-governance strategy**.**

Practical implications: Indian insurers should:

(a) Adopt explainable and auditable AI;

(b) Implement bank-grade cybersecurity and transparent consent architectures;

(c) Preserve human-in-the-loop options for claims disputes; and

(d) Communicate data-handling practices clearly. Regulators such as IRDAI should institute AI governance standards, mandate algorithmic accountability, and enforce robust data protection aligned with the DPDP Act, 2023.

Theoretical contribution: By integrating trust, security, and transparency within an extended TAM–UTAUT framework and validating it in an emerging-economy insurance context, this study enriches technology adoption theory and offers a replicable model for future InsurTech research.

Conclusion and Future Scope

AI-enabled FinTech services hold transformative potential for expanding insurance penetration in India. However, technological sophistication must be matched by trustworthiness, security assurance, and transparency to convert consumer curiosity into committed adoption. This study establishes consumer trust and perceived security as the decisive levers of behavioral intention, tempered by persistent privacy apprehensions and a transparency deficit.

Future research could employ longitudinal or structural equation modelling (SEM) designs, incorporate actual usage behaviour, examine rural and low-literacy segments, and undertake comparative analyses across banking and payments sub-sectors to deepen generalisability.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

References:

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020

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

Eling, M., & Lehmann, M. (2018). The impact of digitalization on the insurance value chain and the insurability of risks. The Geneva Papers on Risk and Insurance—Issues and Practice, 43(3), 359–396. https://doi.org/10.1057/s41288-017-0073-0

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. International Journal of Human-Computer Studies, 59(4), 451–474. https://doi.org/10.1016/S1071-5819(03)00111-3

Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. Academy of Management Annals, 14(2), 627–660. https://doi.org/10.5465/annals.2018.0057

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the FinTech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. Journal of Management Information Systems, 35(1), 220–265. https://doi.org/10.1080/07421222.2018.1440766

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81

Nunnally, J. C. (1978). Psychometric theory (2nd ed.). McGraw-Hill.

Sharma, S. K., & Sharma, M. (2019). Examining the role of trust and quality dimensions in the actual usage of mobile banking services: An empirical investigation. International Journal of Information Management, 44, 65–75. https://doi.org/10.1016/j.ijinfomgt.2018.09.013

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

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.