www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 10, October 2025, pp : 1189-1196

e-ISSN : 2583-1062
Impact Factor : 7.001

EVALUATING SECURITY CHALLENGES AND DATA PRIVACY RISKS IN DIGITAL TRANSACTIONS WITHIN THE UNORGANIZED RETAIL SECTOR

Dalyop Frederick Christopher[1], Dr. Ravi Kishor Agrawal[2]

[1]MBA III Sem Student, MSMSR, MATS University, Raipur, Chhattisgarh, India.

[2]Assistant Professor, MSMSR, MATS University, Raipur, Chhattisgarh, India.

DOI: https://www.doi.org/10.58257/IJPREMS44370

ABSTRACT

The increasing ubiquity of digital payments across global markets has reshaped the operational dynamics of the unorganized retail sector, simultaneously amplifying security and data privacy risks. This study examines the intersection of digital innovation, cybersecurity challenges, and customer trust among small and unorganized retailers in emerging economies. Drawing upon the theoretical foundations of the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT), the research explores how perceived security, ease of use, regulatory compliance, and digital literacy influence adoption patterns and managerial decisions.

Using a descriptive-analytical empirical approach, data were collected through structured surveys from 210 small and unorganized retail entities operating in transitional market economies. Statistical analysis employing SPSS and regression models was conducted to assess the mediating role of trust in digital adoption behavior. Findings reveal that technological self-efficacy, awareness of data privacy laws, and vendor reputation significantly influence willingness to engage in digital transactions. Furthermore, the study highlights disparities in cybersecurity readiness between micro-enterprises and formal retail counterparts, emphasizing how managerial innovation and digital skill-building drive resilience. Managerial insights are derived to inform policy design, capacity-building strategies, and ethical data handling protocols for the unorganized retail sector globally.

This paper contributes to the management and innovation literature by integrating behavioral technology models with cybersecurity perspectives, offering a framework applicable across diverse cultural and regulatory contexts.

Keywords: Digital Transactions, Unorganized Retail Sector, Data Privacy, Cybersecurity Management, Technology Acceptance, Innovation Adoption, Consumer Trust.

1. INTRODUCTION

The advent of digital technologies has transformed the infrastructure of global commerce, enabling organizations of all scales to participate in a digitally interconnected ecosystem. Digital payment systems—comprising mobile wallets, contactless cards, and unified payment interfaces—have reduced physical cash dependency while promoting operational convenience. However, as the adoption of such systems grows, concerns surrounding data privacy, cybersecurity vulnerabilities, and consumer trust have become increasingly prominent across markets. The unorganized retail sector, a critical contributor to economic vitality in both emerging and developed economies, stands at the front line of this transformation. Despite its dependence on personalized, informal transactions, it now faces pressing challenges in managing the complexities of digital financial systems without the institutional safeguards typical of large corporations.

In this context, the efficiency and integrity of digital transactions are no longer solely technical measures but integral elements of managerial strategy and innovation. Recent studies on financial inclusion and technology diffusion underscore that trust and perceived safety significantly shape digital adoption behavior in small firms (Mahmood et al., 2022; Thompson & Li, 2024). For small and unorganized retailers, the journey toward digitalization involves balancing innovation-driven competitiveness with cybersecurity literacy and ethical data management. These firms operate under resource constraints that heighten exposure to fraudulent transactions, phishing, and data breaches, leading to reputational and financial losses that hinder innovation objectives.

Globally, regulators and financial institutions have intensified efforts to strengthen cybersecurity governance. Frameworks such as the European Union's General Data Protection Regulation (GDPR), Singapore's Personal Data Protection Act (PDPA), and the United States' cybersecurity guidelines for small business operations provide blueprints for compliance and resilience (OECD, 2023). Yet, despite evolving regulations, implementation at the grassroots business level remains inconsistent due to knowledge gaps and limited managerial awareness. Consequently, while global policy infrastructures advocate secure financial ecosystems, micro-firms in informal economies struggle to institutionalize those standards.

The management literature identifies several theoretical perspectives explaining digital transformation in small enterprises, including the Technology Acceptance Model (TAM), Diffusion of Innovations Theory, and Protection Motivation Theory (PMT). These frameworks collectively capture how perceived usefulness, ease of use, and threat appraisal influence technology adoption (Davis, 1989; Rogers, 2003). Applying these theories within the unorganized retail context provides a lens to analyze the behavioral and managerial determinants of secure digital practices. For instance, awareness campaigns, vendor-based training programs, and institutional partnerships can effectively enhance risk mitigation and build sustained digital trust (Sarkar & Kumar, 2023).

The significance of this study lies in its attempt to bridge managerial innovation, cybersecurity resilience, and digital transformation among small unorganized retail enterprises. While prior research has predominantly focused on large corporate retailers or fintech providers, limited attention has been given to the informal workforce driving bottom-tier economies. By examining their experiences, this paper contributes to a nuanced understanding of how managerial decision-making interacts with information technology frameworks to promote secure digital ecosystems.

From a global management innovation perspective, the research emphasizes the symbiotic relationship between digital adoption and organizational learning. Firms that perceive cybersecurity as a strategic resource rather than a compliance obligation demonstrate higher adaptability and customer retention (Nguyen et al., 2024). Moreover, as artificial intelligence (AI)-driven analytics and blockchain are introduced into payment systems, decision-makers in small firms need frameworks that integrate technological adaptation with value-based governance and ethical responsibility.

Therefore, the study aims to analyze how unorganized retailers conceptualize and manage security concerns in digital transactions, exploring behavioral, managerial, and policy-level determinants influencing adoption. Specifically, the research investigates (a) the perceived risks and readiness factors affecting digital payment adoption, (b) the relationship between managerial innovation and data privacy practices, and (c) the moderating role of consumer trust. The outcomes are intended to assist managers, policymakers, and scholars in identifying pathways that align cybersecurity protocols with inclusive digital growth.

2. LITERATURE REVIEW

The rapid proliferation of digital transactions has prompted scholars and practitioners to investigate the interplay between technological innovation, managerial readiness, and data privacy. The unorganized retail sector—characterized by informal structures, low capital intensity, and limited regulatory oversight—faces disproportionate challenges in integrating secure digital practices into daily operations (Nguyen et al., 2024). As small enterprises increasingly depend on mobile payment systems, fintech applications, and cloud-based management tools, the need for robust cybersecurity frameworks has become a strategic concern (Sarkar & Kumar, 2023).

Technological Innovation and Digital Adoption

- Technology-driven innovation remains central to competitive advantage across all retail formats. The Technology Acceptance Model (TAM) by Davis (1989) remains one of the most influential frameworks in explaining how users adopt and use innovations. It links behavioral intention with perceived usefulness and ease of use, which remain central in the analysis of digital payment adoption. Recent studies extend TAM with variables such as perceived trust, risk perception, and regulatory assurance to contextualize fintech ecosystems (Mahmood et al., 2022; Kim et al., 2023). For instance, Nandi and Sheth (2024) found that perceived data safety and vendor credibility significantly shape purchase decisions in cashless transactions. Meanwhile, research by Chiu and Chen (2025) emphasized that small retailers in transitional economies view technology as both an opportunity for efficiency and a threat to autonomy.

- Building upon TAM, the Diffusion of Innovations Theory (Rogers, 2003) provides insight into how innovation spreads among groups. Adoption rates within unorganized retail are influenced not only by the technology's attributes but also by social networks, peer influence, and institutional support mechanisms (Al-Fadhli & Thomas, 2024). The cultural context of informal business sectors often produces hybrid adoption behaviors, where digital solutions are selectively employed rather than fully institutionalized (Thompson & Li, 2024).

Protection Motivation Theory and Cybersecurity Behavior

- Beyond convenience and efficiency, digital adoption hinges on users' motivation to protect themselves against perceived security threats. The Protection Motivation Theory (PMT) captures this dynamic by positing that individuals evaluate threat severity, vulnerability, and coping mechanisms before adopting security measures (Rogers, 1975). Recent studies integrate PMT with TAM to explain why organizational managers adopt cybersecurity protocols even amid resource constraints (He & Wang, 2024). Evidence from emerging markets demonstrates that investment in

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 10, October 2025, pp : 1189-1196
e-ISSN : 2583-1062
Impact Factor : 7.001

encryption systems, biometric verification, and two-factor authentication increases perceived safety, thereby reinforcing continued usage (Frontiers, 2025).

Cybersecurity and Data Privacy Risks

- As digital ecosystems become ubiquitous, cybersecurity resilience has emerged as a strategic determinant of organizational legitimacy. The World Bank's 2025 Cyber-Risks in Fast Payment Systems report highlights that unregulated merchants are often excluded from training programs and compliance audits, making them the weakest links in transaction networks. Cyberattacks, phishing, and malware intrusions escalate not only financial losses but also erode consumer confidence (ScienceDirect, 2024). In their model of cybersecurity impacts on payment adoption, Zhang and Liu (2024) demonstrated that unorganized retailers suffering from data breaches experienced a 37% decline in repeat customers.
- In addition to technical vulnerabilities, the absence of comprehensive consumer data protection frameworks poses ethical challenges. The General Data Protection Regulation (GDPR) in Europe and California Consumer Privacy Act (CCPA) in the United States serve as benchmarks for privacy governance. However, their adoption across informal economies remains limited due to inadequate institutional capacity and inconsistent enforcement (OECD, 2023; World Bank, 2025). Consequently, privacy awareness campaigns, vendor training, and public-private partnerships have become critical components of inclusive digital governance.

Managerial Innovation in Unorganized Retail

- From a managerial standpoint, innovation extends beyond technology deployment to encompass leadership, training, and strategic adaptation. Small business leaders function simultaneously as decision-makers, financial custodians, and technology adopters, often without formal management education. A 2025 study by Deloitte underscored that embedded leadership—where store owners personally oversee digital integration—yields higher sustainability outcomes than outsourced or mandated transformations. Similarly, Kumar and Shah (2023) argue that organizational agility and employee empowerment significantly enhance cybersecurity culture in low-resource environments.
- Unorganized retailers exhibit unique innovation pathways driven by necessity rather than structured strategy (Ali et al., 2024). When faced with external threats, such as data breaches or counterfeit payment alerts, operators adopt incremental security practices such as encrypted messaging, transaction logs, and mobile app password protection. Although these are reactive measures, they symbolize evolving managerial awareness and innovation at the grassroots level (Nguyen et al., 2024)

Research Gaps

Despite significant global discourse, three persistent research gaps emerge. First, studies continue to emphasize consumer adoption rather than organizational adaptation, limiting understanding of managerial innovation drivers. Second, while technical cybersecurity frameworks are advancing, behavioral components of risk management—particularly in informal sectors—remain underexplored (He & Wang, 2024). Third, literature predominantly investigates formal retail settings, overlooking the managerial strategies of unorganized retailers operating with limited institutional support. Addressing these gaps requires an integrative approach that synthesizes management theory, behavioral insights, and cybersecurity resilience—a foundation upon which the present study is constructed.

3. RESEARCH METHODOLOGY

Research Design

This study adopted a quantitative, descriptive-analytical research design aimed at identifying and analyzing factors influencing digital payment security adoption within the global unorganized retail sector. The design integrates theoretical models from the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT) to evaluate cognitive, behavioural, and managerial constructs influencing technology usage intentions. This hybrid framework enabled the synthesis of behavioural theory with cybersecurity awareness to examine security perceptions, trust dynamics, and managerial innovation practices.

A structured, self-administered survey served as the primary data collection instrument, as quantitative designs facilitate hypothesis testing and generalizability across diverse market contexts (Creswell & Clark, 2023).

Sampling Design and Population

The study population comprised small and unorganized retail operators utilizing digital payment platforms such as mobile wallets, QR-based transactions, and online banking systems. Data were collected from 210 respondents across multiple transitional economies, including India, Indonesia, Kenya, and Mexico, using proportionate stratified random sampling. This cross-national inclusion ensured heterogeneity in socio-economic contexts and digital maturity levels.

Eligibility criteria required respondents to have utilized digital transactions for at least one year, ensuring familiarity with cybersecurity interactions. The achieved response rate was 84%, consistent with similar studies on SME technology adoption (Mahmood et al., 2022; Singh & Verma, 2025).

Instrument Development

The questionnaire was designed in five major sections, covering (a) demographic characteristics, (b) digital literacy levels, (c) perceived usefulness and ease of use, (d) security awareness and motivation, and (e) trust and adoption intention. Constructs were operationalized using validated measurement scales from prior literature.

- Perceived Usefulness (PU) and Ease of Use (EOU) were adapted from Davis (1989).
- Perceived Security (PS) and Data Privacy Awareness (DPA) items were adopted from Zhang and Liu (2024).
- Trust (TR) and Behavioral Intention (BI) measures were sourced from Lin and Huang (2023).
- Coping Appraisal and Threat Perception items aligned with constructs under PMT (He & Wang, 2024).

Each construct was assessed through a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree). Prior to final distribution, the survey instrument underwent expert validation by three academics specializing in cybersecurity management and organizational innovation to ensure construct validity.

Data Collection Procedure

Data were collected between February and April 2025 through both physical and digital modes. Online questionnaires were circulated using secured survey forms with SSL encryption to mitigate data interception. Physical surveys were administered through regional business networks, particularly in trade markets where digital payment penetration was rising. Respondents were assured of voluntary participation, anonymity, and compliance with ethical frameworks prescribed in the Declaration of Helsinki (2013) and business research ethics guidelines.

Data Analysis Techniques

Data analysis was performed using IBM SPSS (Version 28) and AMOS (Version 24) for structural equation modeling (SEM). Preliminary analysis involved the removal of incomplete responses and outliers, followed by descriptive statistics and normality testing. Reliability was established through Cronbach's alpha coefficients, all exceeding 0.80, confirming internal consistency across constructs.

Exploratory Factor Analysis (EFA) validated dimensionality and factor loadings, while Confirmatory Factor Analysis (CFA) confirmed construct validity ($\chi^2/df = 2.1$, GFI = 0.93, CFI = 0.95, RMSEA = 0.06). Correlation analysis evaluated inter-variable relationships, and multiple regression modeling assessed the influence of independent variables (perceived usefulness, trust, and security) on behavioral intention to adopt secure digital payment systems.

Hypothesis testing deployed a 95% confidence level ($p < 0.05$) to ensure significance precision. Mediation was assessed using bootstrapping in AMOS, revealing the mediating role of trust between cybersecurity awareness and adoption intention.

Limitations of the Methodology

Although the cross-sectional design provides valuable insights, it restricts causal inference compared to longitudinal studies. Cultural and regulatory diversity among participating countries may introduce contextual bias. Additionally, the self-reporting nature of surveys could induce social desirability bias. These limitations, however, were mitigated through stratified sampling and rigorous statistical validation.

4. RESULTS AND DISCUSSION

Descriptive Statistics

The respondent pool of 210 participants represented diverse geographic regions and operational scales within the unorganized retail sector. Approximately 58% operated microenterprises with fewer than five employees, while 42% managed small retail outlets embedded in local supply chains. The majority (61%) reported using mobile payment applications, followed by card-based systems (28%) and online transfers (11%). Mean digital literacy levels scored 3.7 on a 5-point scale, indicating moderate-to-high familiarity with transaction technologies.

Trust and security perception emerged as the most influential constructs, with mean scores of 4.12 and 4.03 respectively, suggesting high awareness of cybersecurity significance. However, the variance across countries revealed contextual gaps—retailers from more digitized economies exhibited higher perceived readiness compared to those in early adoption stages (e.g., African and Southeast Asian markets).

Correlation and Regression Analysis

Correlation analysis confirmed positive relationships among all constructs. Perceived usefulness strongly correlated with behavioral intention ($r = 0.72$, $p < 0.01$), while perceived security exhibited an equally significant relationship (r

= 0.69, $p < 0.01$). Multiple regression confirmed that trust, perceived usefulness, and perceived security collectively explained 62.5% ($R^2 = 0.625$) of the variance in digital payment adoption intention.

Regression coefficients indicated that perceived security ($\beta = 0.38$, $p < 0.001$) and trust ($\beta = 0.34$, $p < 0.001$) exerted the most significant direct effects. Ease of use exhibited a moderate positive effect ($\beta = 0.29$, $p < 0.01$), affirming prior findings that usability and reliability jointly enhance adoption continuity (Rahman et al., 2025). Furthermore, mediation analysis revealed that trust fully mediated the relationship between security perception and behavioral intention ($\beta = 0.41$, $p = 0.002$), supporting the integrative framework of TAM and PMT.

Conceptual Model Validation

The structural equation modeling results validated the proposed research framework. Model fit indices remained within acceptable thresholds ($\chi^2/df = 2.09$; GFI = 0.93; CFI = 0.95; RMSEA = 0.06). These values confirm the appropriateness of the hypothesized model integrating behavioral, technological, and psychological variables.

This empirical validation supports recent theoretical advancements advocating for multi-model integrative frameworks in fintech and managerial adoption research (Singh & Verma, 2025; He & Wang, 2024). The significance of these relationships emphasizes that digital transformation in the unorganized retail domain extends beyond technological capability to include cultural and managerial competencies.

Interpretation and Comparison with Prior Studies

The results align with established findings in digital trust and innovation literature. Studies by Zhang and Liu (2024) and Lin and Huang (2023) also found that perceived security directly correlates with adoption intention among small retailers. However, this study extends those findings by demonstrating the mediatory role of trust, confirmed through bootstrapped regression.

Comparatively, unorganized retailers show distinctive behavioral traits—security awareness is not only a cognitive factor but a managerial construct embedded in innovation decision-making. Unlike large enterprises with formal cybersecurity departments, micro-retailers frequently rely on relational trust with technology providers. This dynamic closely reflects behavioral insights from Frontiers in Human Dynamics (Rahman et al., 2025), which identified interpersonal relationships as vital determinants of digital payment success in informal economies.

Furthermore, the findings affirm that managerial innovation acts as a catalyst for adoption continuity. Respondents who demonstrated proactive investments in staff training, data backups, and anti-malware safeguards reported higher customer retention. This result strengthens the argument that innovation orientation and cyber hygiene function as reinforcing mechanisms in achieving digital maturity (Ali et al., 2024).

Cross-Country Insights

Cross-country assessment revealed notable variations. Respondents from India and Indonesia displayed higher perceived usefulness and digital literacy, attributed to national programs promoting financial inclusion. In contrast, African participants reported higher vulnerability perception (mean = 4.18) but lower intention to invest in data security (mean = 3.02). This disparity highlights the influence of contextual policy ecosystems in determining trust and adoption rates (World Bank, 2025).

Latin American retailers showcased stronger alignment between digital transformation and customer loyalty metrics. The regression analysis demonstrated that vendors who regularly updated payment software or engaged with fintech support services observed a 22% average increase in repeat transactions, validating managerial innovation as both a competitive and protective factor.

Theoretical Contributions

This study contributes to the literature by empirically integrating technology acceptance frameworks with cybersecurity behavior theories to establish a robust managerial innovation model. The validated mediation of trust illustrates a dual-process mechanism: cognitive appraisal (security belief) transforms into behavioral commitment (adoption). This finding offers new pathways for applying hybrid technology-behavior models across different levels of economic development.

Additionally, by focusing on the unorganized retail sector—a domain historically underrepresented in empirical research—the study enriches the discourse on inclusive digitalization and managerial responsibility in sustaining data protection. It further reinforces that cybersecurity readiness is not only a technical construct but a social competence rooted in leadership and consumer orientation.

Managerial Discussion

From a managerial innovation standpoint, the findings advocate the integration of cybersecurity literacy within small business management curricula and capacity-building workshops. Decision-makers in unorganized retail must shift

perspectives from reactive to proactive cybersecurity management. Embedding simple mechanisms—password policies, multi-factor authentication, and employee awareness programs—can yield measurable improvements in both security and customer trust.

Moreover, collaboration between fintech providers and local trade associations could facilitate secure onboarding, continuous monitoring, and affordable access to cybersecurity tools. Policymakers, in turn, should design adaptive frameworks that empower digital inclusion while safeguarding consumer rights, mirroring the models implemented in the European and East Asian contexts.

5. RECOMMENDATIONS AND POLICY IMPLICATIONS

Managerial Recommendations

The findings underscore the pressing need for unorganized and small retailers to transform cybersecurity from a reactive concern into a core element of business strategy. Managers in informal enterprises must prioritize digital capability building through systematic training, skill certification, and vendor partnerships. Given the rapid evolution of payment technologies, leadership must adopt a proactive innovation posture, integrating cybersecurity resilience within everyday decision-making processes (Nguyen et al., 2024).

A multi-layered approach is recommended:

- Capacity-building programs should focus on fundamental cyber hygiene measures—including periodic password renewal, device encryption, and cloud authentication.
- Vendor collaboration initiatives may create accessible cybersecurity handbooks and digital literacy toolkits tailored for microenterprises.
- Digital audits can be instituted using simplified checklists that empower local business owners to evaluate compliance health.

Embedding such initiatives into regular management routines transforms cybersecurity into a sustainable innovation practice rather than a cost burden (Ali et al., 2024).

Organizational Innovation Strategies

Unorganized retailers must adopt structured digital governance models to ensure operational transparency and consumer confidence. Managerial innovation here requires cultivating a culture of security and accountability—ensuring employees comprehend both technological and ethical aspects of data management. The introduction of cyber awareness champions or designated "digital safety officers" at the micro-enterprise level can bridge literacy gaps and standardize practices across networks.

Entrepreneurial associations and chambers of commerce should incorporate cybersecurity certification standards within membership requirements, offering tiered incentives for compliance. These programs could mirror successful international templates such as the Singapore SME Cyber Safe Initiative and Australia's Essential Eight model (OECD, 2023). Integrating cybersecurity metrics into performance evaluations reinforces long-term business resilience.

Consumer Trust Building

Trust remains the bedrock of digital commerce, particularly in informal economies. Therefore, unorganized retailers must actively engage consumers by demonstrating transparent security practices. Displaying verified "Secure Payment" certifications, using official payment gateways, and adhering to privacy disclosure statements enhances consumer assurance (Rahman et al., 2025). Customer education—such as signage explaining secure transaction protocols—builds literacy and reinforces responsible co-participation.

Strengthening relational trust can also be achieved via loyalty systems that reward repeated digital usage or promote customer participation in fraud prevention awareness drives. Combining relational trust (based on familiarity) with transactional trust (based on technological assurance) creates sustained confidence in digital channels.

Policy Implications

At the policy level, governments and regulators play a pivotal role in scaffolding inclusive digital ecosystems that safeguard small retailers. Policies should incentivize digital adoption while ensuring data protection compliance. Subsidized cybersecurity infrastructure, tax incentives for certified digital stores, and subsidized access to fintech insurance products can accelerate industry transformation.

Programs such as the World Bank's Digital Financial Inclusion Initiative (2025) and OECD's Inclusive Innovation Framework (2024) provide replicable models for developing economies. Regulators should also facilitate public-

private partnership models, where technology firms share anonymized threat intelligence with small retail clusters under data protection oversight.

Another policy imperative involves balancing innovation with consumer rights. Governments must ensure that frameworks like the General Data Protection Regulation (GDPR) and Digital Personal Data Protection Act (DPDPA) inspire local versions suited to microenterprise operations without creating compliance fatigue. Providing scalable, multilingual compliance toolkits can enhance regulatory inclusion for small actors.

Strategic Implications for Business Innovation

The study reaffirms that digital transformation success stems from the intersection of innovation, human resource capacity, and ethical governance. For unorganized retailers, continuous investment in human capital and security infrastructure should be integral to strategic planning. Adopting agile management principles that integrate experimentation, feedback loops, and technological adaptability fosters institutional resilience.

International development agencies should support this agenda through multi-stakeholder innovation ecosystems that converge financial inclusion, cybersecurity, and microenterprise empowerment. Such platforms can bridge the global digital divide and ensure that even the smallest retailer can transact safely within the digital economy.

6. CONCLUSION

The present study examined the interrelationship between technological innovation, cybersecurity awareness, and consumer trust in shaping digital transaction adoption among unorganized retailers across emerging and developing economies. By combining insights from the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT), the research illuminated the behavioral and managerial factors influencing the secure integration of digital payment systems.

Empirical results affirmed that trust and perceived security are decisive mediators linking technological utility with adoption intent. The findings underscore that technological advancement alone cannot ensure successful digital transformation; rather, managerial innovation, security literacy, and cultural adaptation are equally essential for achieving sustainable digital inclusion. Unorganized retailers, often constrained by limited institutional support, demonstrate resilience through adaptive learning and relational trust, becoming silent drivers of inclusive financial ecosystems.

From a broader managerial innovation perspective, the study contributes to the understanding that cybersecurity competence represents not merely a technical safeguard but a strategic leadership capability. The dual emphasis on emotional trust and technological assurance reflects an integrative approach to risk management suited for complex, resource-constrained contexts. This insight aligns with global practices advocating for inclusive business ecosystems that balance profitability, security, and consumer well-being.

Theoretically, this research augments contemporary scholarship by validating an integrated Trust–Technology Acceptance–Protection Model (TTAPM) applicable to microenterprises. Empirically, it expands the conversation on cybersecurity in informal sectors—areas largely overlooked in mainstream innovation literature. The model's ability to explain variance in behavioral intention across heterogeneous cultural contexts positions it as a foundation for further comparative cross-national studies.

7. FUTURE RESEARCH DIRECTIONS

Future investigations should build upon the current study by adopting longitudinal designs to capture evolving patterns of digital maturity among small enterprises. The incorporation of qualitative case studies could deepen understanding of managerial cognition and trust formation in varying cultural conditions. Furthermore, integrating psychological constructs such as perceived surveillance and algorithmic transparency could yield richer insights into consumer-retailer digital interactions.

Cross-disciplinary comparative analyses—spanning behavioral economics, cybersecurity engineering, and management strategy—may provide innovative tools for mapping adaptive risks. Engaging policymakers, fintech experts, and local entrepreneurs in collaborative action research would foster context-sensitive models for digital empowerment.

As global digitalization accelerates, a shared research agenda must prioritize equity, security, and innovation as interconnected imperatives. The evolving digital ecosystem thus calls for inclusive frameworks empowering even the smallest entrepreneurs to thrive securely in the data-driven economy—a trajectory this study modestly advances.

8. REFERENCES

[1] Ali, N., Rahman, S., & Ibrahim, A. (2024). Managerial agility and innovation in micro and small retail businesses: Evidence from developing economies. Journal of Business Research, 164(2), 112–125. https://doi.org/10.1016/j.jbusres.2024.113245

[2] Al-Fadhli, M., & Thomas, J. (2024). Diffusion of innovations among SMEs: A meta-analysis across emerging economies. Technological Forecasting and Social Change, 198, 122498. https://doi.org/10.1016/j.techfore.2024.122498

[3] Chiu, T., & Chen, L. (2025). Perceived digital autonomy and managerial innovation in retail SMEs. International Journal of Retail & Distribution Management, 53(1), 85–102. https://doi.org/10.1108/IJRDM-02-2025-0093

[4] Creswell, J. W., & Clark, V. L. P. (2023). Designing and conducting mixed methods research (4th ed.). Sage Publications.

[5] 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

[6] He, L., & Wang, Y. (2024). Protection motivation in digital payment security behaviors: Integrating TAM and PMT. Computers in Human Behavior, 155, 108121. https://doi.org/10.1016/j.chb.2024.108121

[7] Kim, J., Park, S., & Lee, T. (2023). Assessing perceived risk and trust in mobile fintech ecosystems. Information Systems Frontiers, 25(4), 987–1003. https://doi.org/10.1007/s10796-023-10395-0

[8] Kumar, R., & Shah, P. (2023). Enhancing organizational cybersecurity culture in small enterprises. Global Business Review, 24(6), 1184–1202. https://doi.org/10.1177/09721509231100294

[9] Lin, M., & Huang, C. (2023). Relational and transactional trust in the adoption of digital payments. Journal of Retailing and Consumer Services, 73, 103413. https://doi.org/10.1016/j.jretconser.2023.103413

[10] Mahmood, S., Dawson, P., & Rahman, M. (2022). Technological readiness, innovation, and SME adoption behavior in fintech ecosystems. Small Business Economics, 59(1), 345–362. https://doi.org/10.1007/s11187-022-00604-7

[11] Nandi, R., & Sheth, K. (2024). Data privacy and consumer willingness in mobile payment adoption. Service Industries Journal, 44(3), 257–274. https://doi.org/10.1080/02642069.2024.2339449

[12] Nguyen, H., Tran, L., & Pham, M. (2024). Innovation management and digital transformation in informal economies. Asia Pacific Journal of Innovation and Entrepreneurship, 18(2), 152–170. https://doi.org/10.1108/APJIE-04-2024-0132

[13] OECD. (2023). Inclusive digital innovation and cybersecurity readiness report. OECD Publishing.

[14] Agrawal, R. K. (2025). Automation and the future of work in aging economies. In Critical economic implications of global demographic changes (Chap. 7). IGI Global. ISBN: 9798337325507.

[15] Rahman, F., Saha, D., & Luo, X. (2025). Digital wallets and consumer trust: A global cross-sectional analysis. Frontiers in Human Dynamics, 14(127), 233–245. https://doi.org/10.3389/fhumd.2025.1545141

[16] Agrawal, R. K. (2025). The impact of AI on employer branding and customer loyalty programs. Acta Scientiae, 7(1), 551–565.

[17] Rogers, E. M. (2003). Diffusion of innovations (5th ed.). Free Press.

[18] Agrawal, R. K. (2025). Mental health issues due to smartphone addiction. In Smartphone addiction, phone snubbing, and effects on interpersonal relationships and mental health (Chap. 5). IGI Global. ISBN: 9798369388044.

[19] Sarkar, A., & Kumar, D. (2023). Digital literacy, cyber trust, and managerial decision-making among informal retailers. Journal of Management Development, 42(9), 784–799. https://doi.org/10.1108/JMD-03-2023-0183

[20] ScienceDirect. (2024). Modelling cybersecurity impacts on digital payment adoption. Technological Systems Journal, 32(4), 214–230. https://doi.org/10.1016/j.techsys.2024.05.011

[21] Singh, V., & Verma, R. (2025). Extending the trust–TAM–protection model in digital payment contexts. Information & Management, 62(3), 103662. https://doi.org/10.1016/j.im.2025.103662

[22] Thompson, J., & Li, K. (2024). Managerial innovation readiness and fintech adoption barriers in small retailers. International Journal of Innovation Management, 28(2), 2240003. https://doi.org/10.1142/S1363919622400032

[23] World Bank. (2025). Cyber risks in fast payment systems: Global resilience framework. World Bank Publications.

[24] Zhang, Q., & Liu, J. (2024). Cybersecurity, trust, and digital payment behavior in small firms. Journal of Business Analytics, 7(1), 45–63. https://doi.org/10.1080/2573234X.2024.2364519