sjst.scst.edu.ly

Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)

مجلة صرمان للعلوم والتقنية
Vol 8, No.2. Jun – Dec. 2026
Pages: 224 ~ 238

Biometric Authentication for Bank Card Users in Libya: An Exploratory Study of Usability and User Acceptance in High-Security Systems

Salem Abdesalam Alamouri*, Fathi Hamhoum
Faculty of Science, University of Azzawia, Azzawia, Libya

Salem712083@gmail.com

Abstract
Digital banking in Libya still relies almost entirely on personal identification numbers (PINs) to verify card holders. This paper reports a Human-Computer Interaction (HCI), human-centered design field study asking whether biometric authentication — fingerprint or facial recognition — could offer a more usable, acceptable verification experience, centered on usability and user acceptance rather than security engineering, since no biometric banking system yet exists in Libya to evaluate directly. A structured survey was administered in Al-Zawiya during 2026 to three linked stakeholder groups: bank card holders (n = 100), merchants operating point-of-sale devices (n = 30), and bank employees (n = 20), for a combined sample of 150. Perceived ease of use — the study's central construct — was rated favorably by all three groups and, uniquely, showed no significant cross-group difference (Kruskal-Wallis, p = 0.854); future behavioral intention among customers was the highest-scoring dimension measured (M = 4.23). Item-level analysis surfaced two findings a composite mean would hide: a privacy paradox, where customers reported little acute worry about data misuse (10–12% agreement) yet unanimously wanted clear legal protection (100%); and a hardware gap, where no bank employee agreed current point-of-sale terminals can be upgraded for biometrics (0% agreement). Adoption enthusiasm formed a statistically confirmed "readiness gradient," highest among customers and most measured among employees closest to operational realities. The paper closes with usability-centered recommendations — modality choice, layered biometric-plus-PIN verification, and hardware-first investment — contributing to HCI literature on pre-implementation evaluation of biometric systems in high-security financial contexts.

Keywords: *Human-Computer Interaction, human-centered design, usability, perceived ease of use, user acceptance, biometric authentication, digital banking, Libya.*

Submitted: 27/05/2026 *Accepted: 11 /07/2026*

I. Introduction

Libyan banks confirm a card holder's identity almost exclusively through a PIN, even as fingerprint and facial recognition have become routine elsewhere. No Libyan bank yet offers biometric verification, though many customers already use fingerprint attendance at work. This paper is framed as a human-centered HCI study, not a security or cryptography study: it asks whether biometric authentication could give Libyan bank users an easier, clearer, more satisfying

experience than a PIN, while security, trust, and privacy are measured as factors that condition that experience rather than as the paper's primary object.

No local study has examined how ready Libyan customers, merchants, and bank employees are for this shift, or how they weigh usability against privacy and infrastructural concerns. This paper addresses that gap and contributes: the first multi-stakeholder biometric-banking usability survey conducted in Libya; a cross-group comparison revealing a statistically confirmed "readiness gradient"; and item-level results — a privacy paradox and a concrete point-of-sale (POS) hardware gap — hidden inside axis-level averages.

1. Research Questions

RQ1: How do Libyan bank customers perceive the usability (ease of use), usefulness, trust, and privacy implications of biometric authentication? RQ2: How ready do merchants and bank employees consider themselves and the surrounding infrastructure to be for biometric adoption? RQ3: What barriers and enablers most likely shape successful biometric-banking adoption in Libya, and do these differ systematically across stakeholder groups or by customer gender?

2. Working Hypotheses

Grounded in the Technology Acceptance Model (TAM) [1], three directional hypotheses guided item design and are revisited against the descriptive and inferential results in Section IV: H1 — perceived ease of use is positively associated with future adoption intention; H2 — perceived trust and security are positively associated with future adoption intention; H3 — perceived readiness for biometric adoption differs across customers, merchants, and bank employees. These are treated as working expectations for an exploratory, correlational study rather than as claims tested through controlled experimentation or confirmatory modeling.

II. Related Work

Two frameworks anchor this study's constructs. Davis's Technology Acceptance Model holds that adoption intention is shaped mainly by perceived usefulness and perceived ease of use [1]; Venkatesh et al.'s Unified Theory of Acceptance and Use of Technology (UTAUT) adds social influence and facilitating conditions [2]. Biometric-specific extensions add trust and privacy as further, partly independent, determinants: Lancelot Miltgen et al. found privacy and trust predict biometric acceptance independently of usefulness and ease of use [3], an extension this paper's instrument follows and that anticipates the privacy paradox in Section IV.

Recent empirical work (2021–2026) situates the present findings regionally. Bhat, Islam, and Mir surveyed 610 bank customers and found attitude toward biometrics raises perceived ease of

use and security, which raise usefulness and, ultimately, adoption intention [4] — a chain broadly consistent with the pattern observed here. Noori found performance expectancy, effort expectancy, and perceived security each significantly predicted biometric-banking intention among 391 Iraqi customers [5], and a 2026 systematic review of biometric authentication in mobile banking confirmed that user-facing empirical evidence from Arab banking markets generally remains sparse [6]. Wang confirmed ease of use as a strong FinTech adoption predictor generally [7], and Rukhiran et al. showed the same TAM relationships hold for face-recognition attendance systems in Thailand [8]. Regionally, Alnaas found significant regulatory, electronic, and cultural barriers to e-banking adoption among Libyan bank managers in Tobruk [9], and a technical assessment of Libyan banking security similarly found limited staff security-awareness and unresolved regulatory gaps [10]. A Gulf-wide systematic review found trust and regulatory clarity dominate digital-payment adoption once a usability baseline is met [11], anticipating this paper's own finding that ease of use is rated favorably while trust- and privacy-related dimensions vary more. Two further recent studies inform this paper's methodology: Allafi and Darem found biometric authentication earns the highest usability-and-security satisfaction among online authentication methods [13], and Mujinga applied exploratory factor analysis to online-banking authentication usability, a technique this paper's Section III and Appendix explain was not viable here given the instrument's short subscales [14].

No published study, to the authors' knowledge, has examined biometric-authentication usability and acceptance among Libyan bank customers, merchants, and staff together. This is the gap the present study addresses.

III. Methodology

1. Design, Population, and Sampling

This exploratory, descriptive, quantitative study measures pre-implementation perceptions rather than evaluating a live system, since no Libyan bank currently offers biometric verification. Data were collected in Al-Zawiya during 2026 using convenience sampling across three groups: bank card holders (n = 100), merchants operating POS devices (n = 30), and bank employees across technical and non-technical roles (n = 20), for a combined sample of 150. The employee sample, though sufficient for descriptive and non-parametric comparison, is small in absolute terms and drawn from a single city; results for this group should be interpreted cautiously given its limited size and the potential for sampling bias, and are best read as indicative rather than representative of Libyan bank staff generally.

sjst.scst.edu.ly
Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)
مجلة صرمان للعلوم والتقنية
Vol 8, No.2. Jun – Dec. 2026
Pages: 224 ~ 238

2. Instrument and Content Validity

Three parallel questionnaires (customer: 21 items, seven three-item axes; merchant and employee: 14 items each, five axes) used five-point Likert items (1 = strongly disagree to 5 = strongly agree), closing with one open-ended question. Ease of use was treated, by design, as the central construct. Item wording was reviewed for content validity and conceptual fit by academic staff with backgrounds in computer science, human-computer interaction, and banking technology prior to distribution, and adjusted for clarity based on that review; a formal pilot test with a separate respondent sample was not conducted, which is noted as a limitation in Section VI. The preamble anchored biometrics to the fingerprint attendance systems already common in Libyan workplaces so the concept was concrete even for respondents without banking-specific exposure.

3. Data Analysis

Responses were analyzed descriptively (means, SDs, 95% CIs, "agree/strongly agree" percentages) and inferentially in Python (SciPy). Cronbach's alpha [12] proved low or negative for several short, high-agreement axes (Appendix, Table A1); given the exploratory design and two-to-three-item subscales, these estimates were interpreted cautiously rather than used for item retention (Section V). The non-parametric Kruskal-Wallis H-test (with epsilon-squared effect size) compared the three groups on shared dimensions, and Mann-Whitney U (with rank-biserial effect size) compared male and female customers; both suit ordinal, non-normal Likert data better than ANOVA/t-tests. Spearman's rank correlation, more appropriate than Pearson's for ordinal data, measured association between customer axis scores.

IV. Results and Discussion

1. Sample and Demographics

Fig. 1 shows the sample composition (N = 150). Customers were 68% male, concentrated at 31–50 years (78%) and bachelor's-level education (79%); 77% had prior exposure to some biometric system, chiefly through workplace fingerprint attendance (76% of employers) — evidence the interaction mechanic is not unfamiliar even though never applied to banking (Table 1). Merchants (n = 30) were entirely male and 31–50 years (86.7%); all operated a POS device and 80.0% had prior biometric exposure. Employees (n = 20) spanned cashiers, IT/network specialists, analysts, auditors, and department heads; 70.0% had over ten years of banking experience and all reported a technical background.

sjst.scst.edu.ly
Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)
مجلة صرمان للعلوم والتقنية
Vol 8, No.2. Jun – Dec. 2026
Pages: 224 ~ 238

Fig. 1. Study Sample Composition (N = 150)

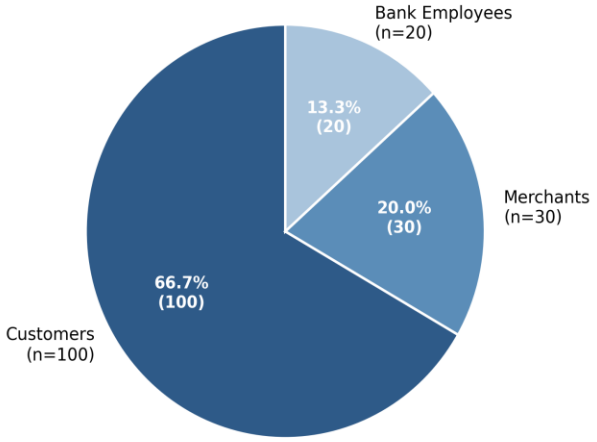

Figure. 1. Composition of the overall study sample by stakeholder group (N = 150).

Table 1. Demographic and Behavioral Profile of Customer Respondents (n = 100)

Characteristic	Category	n	%
Gender	Male / Female	68 / 32	68.0 / 32.0
Age	31–50 years	78	78.0
Education	Bachelor's degree	79	79.0
Prior biometric exposure	Yes	77	77.0
Employer fingerprint attendance	Yes	76	76.0

2. Customer Perception: Usability Is Not the Barrier

Table 2 and Fig. 2 report axis-level statistics. Future intention scored highest (M = 4.23, SD = 0.36, 86.0% agreement), followed by trust and security (M = 4.16, 85.7%) and usefulness (M = 4.15, 84.0%). Ease of use — this study's central construct — scored strongly (M = 4.08, 79.0%), indicating customers already expect biometric verification to be straightforward; consistent with TAM [1], [4], this ease-of-use association carries through to strong stated willingness to use it, though it reflects a belief extrapolated from workplace fingerprint attendance rather than banking-specific experience. Privacy scored lowest (M = 3.36, only 40.7% agreement) and most divided.

Item-level detail (Appendix, Table A2) reveals a privacy paradox: only 12.0% of customers agree they are worried about data misuse and 10.0% fear a breach, yet 100.0% agree clear legal protection is needed — customers are not worried today because no system exists yet to worry about, but are unambiguous that any future system must carry explicit legal safeguards. Practically, the barrier to adoption is less about the biometric modality itself and more about who holds the data, under what law, with what recourse.

SJST
sjst.scst.edu.ly
Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)
مجلة صرمان للعلوم والتقنية
Vol 8, No.2. Jun – Dec. 2026
Pages: 224 ~ 238

Table 2. Descriptive Statistics for Customer Perception Axes (n = 100)

Axis	Mean	SD	% Agree	Rank
Awareness & Knowledge	3.98	0.77	74.3	6
Perceived Ease of Use	4.08	0.53	79.0	4
Perceived Usefulness	4.15	0.50	84.0	3
Trust & Security	4.16	0.57	85.7	2
Privacy Concerns	3.36	0.35	40.7	7
Future Behavioral Intention	4.23	0.36	86.0	1
Perceived Readiness	3.77	0.43	64.7	5

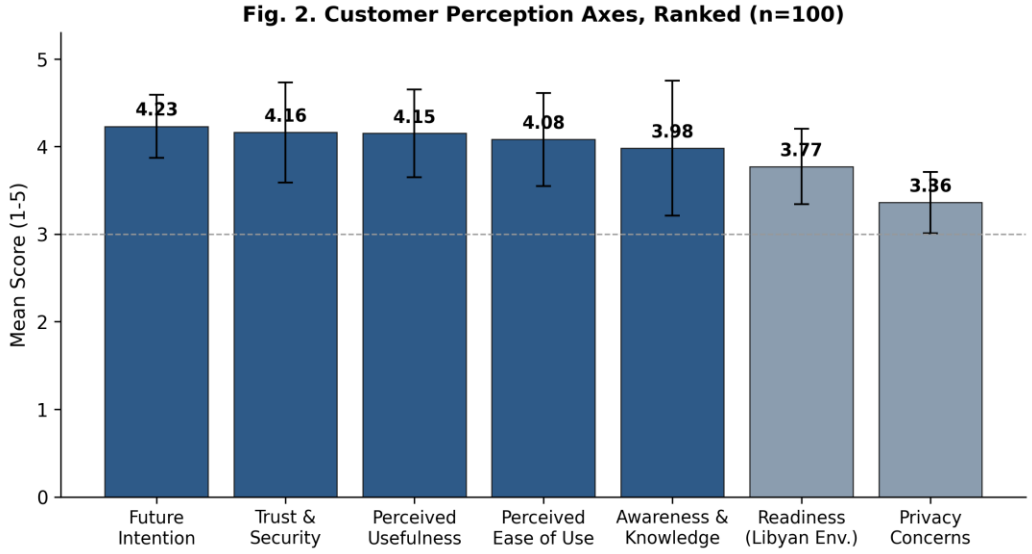

Figure. 2. Mean scores of the seven customer perception axes, with error bars (± 1 SD).

3. Merchants and Bank Employees: The Hardware Gap

Merchants (Table 3) rated ease of use highest (M = 4.08, 81.1%) and benefit/security favorably (M = 3.83, 71.1%); the challenges-and-concerns axis, phrased toward worry, produced the lowest merchant mean (M = 2.38, 13.3% agreement) — reassuring, since low agreement with worry items signals limited perceived risk. Employees rated ease of use highest of any employee axis (M = 4.15, 85.0%) and security/technical aspects similarly (M = 4.02, 85.0%); infrastructure readiness was lowest (M = 3.42, 48.3%) — the single lowest axis-level mean recorded across all three questionnaires. Item-level detail (Appendix, Table A3) is the most consequential finding in the study: while employees expressed reasonable confidence in basic servers and networks (70.0% agreement) and power/connectivity stability (75.0%), zero employees agreed current POS devices in the Libyan market can be upgraded for biometrics (0.0% agreement) — the only item, across all items surveyed in all three questionnaires, to receive zero agreement. This identifies POS hardware, not network or server capacity, as the concrete binding constraint on any near-term rollout (Section V).

SJST
sjst.scst.edu.ly
Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)
مجلة صرمان للعلوم والتقنية
Vol 8, No.2. Jun – Dec. 2026
Pages: 224 ~ 238

Table 3. Descriptive Statistics for Merchant and Bank-Employee Perception Axes

Merchant Axis (n=30)	**Mean**	**SD**	**% Agree**
Ease of Use	4.08	0.67	81.1
Perceived Benefit / Security	3.83	0.62	71.1
Challenges & Concerns (reverse)	2.38	0.79	13.3
Future Intention to Adopt	3.81	0.75	70.0
Employee Axis (n=20)	**Mean**	**SD**	**% Agree**
Infrastructure Readiness	3.42	0.89	48.3
Security & Technical Aspects	4.02	0.57	85.0
Ease of Use (Employee View)	4.15	0.66	85.0

4. Cross-Group Comparison: The Readiness Gradient

Table 4 and Fig. 3 compare shared dimensions across groups. Ease of use is remarkably consistent (customers 4.08, merchants 4.08, employees 4.15) — the clearest cross-group finding, confirmed statistically by Kruskal-Wallis ($H = 0.32$, $df = 2$, $p = 0.854$, $\varepsilon^2 \approx 0.00$): usability is not perceived as a barrier by any group. Awareness/readiness ($H = 14.99$, $p < 0.001$, $\varepsilon^2 = 0.09$), perceived benefit/security ($H = 12.71$, $p = 0.002$, $\varepsilon^2 = 0.07$), and future intention ($H = 17.87$, $df = 1$, $p < 0.001$, $\varepsilon^2 = 0.13$, customers vs. merchants only, since employees lack a directly comparable item set) all differ significantly across groups, declining steadily from customers through merchants to employees — a pattern this paper calls the readiness gradient: enthusiasm is highest furthest from deployment realities and most tempered closest to them, a sensible asymmetry rather than a contradiction, now statistically confirmed rather than only descriptive.

5. Post-Hoc Pairwise Comparisons

Because the omnibus Kruskal-Wallis test only establishes that at least one group differs, Table 5 reports pairwise Mann-Whitney U follow-up tests (Bonferroni-adjusted $\alpha = 0.017$ for three-way comparisons) for the three significant dimensions. Awareness/readiness differs sharply between customers and employees ($p < 0.001$) and between merchants and employees ($p = 0.010$), but not between customers and merchants ($p = 0.122$) — the split falls specifically at the employee boundary, consistent with employees' closer, more technically grounded view of infrastructure. Benefit/security differs significantly only between customers and merchants ($p = 0.001$); the merchant–employee gap ($p = 0.056$) narrowly misses the adjusted threshold. Future intention was measurable only for customers and merchants, where the gap is the strongest effect in the entire pairwise analysis ($p < 0.001$, $r = -0.49$). Ease of use shows no significant pairwise gap anywhere (all $p > 0.5$), reinforcing that this is the one dimension on which every stakeholder group genuinely agrees.

Table A5 (Appendix) compares male (n=68) and female (n=32) customers via Mann-Whitney U; no axis showed a significant gender difference (all $p > 0.05$). Privacy concern was nearly

identical (M = 3.36 both, p = 0.769, negligible effect), and the largest raw gap — awareness — fell short of significance (p = 0.093, small effect). This sample does not support a materially different adoption path by gender, addressing RQ3's gender-difference component directly.

Table 4. Comparative Mean Scores Across Shared Dimensions, by Stakeholder Group

Shared Dimension	Customers	Merchants	Employees
Perceived Ease of Use	4.08	4.08	4.15
Awareness / Readiness	3.98	3.77	3.42
Benefit / Security	4.16	3.83	4.02
Future Intention	4.23	3.81	—

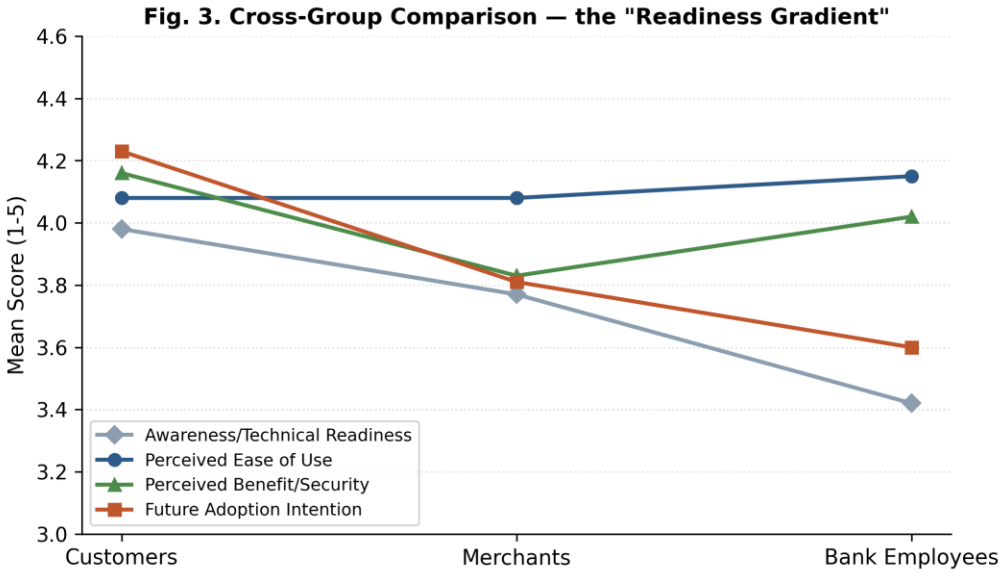

Fig. 3. Comparative perception trends across the three stakeholder groups — the "readiness gradient."

Table 5. Post-Hoc Pairwise Mann-Whitney U Comparisons (Bonferroni-Adjusted α = 0.017)

Dimension	Pairwise Comparison	U	p-value	Rank-biserial r
Awareness / Readiness	Customer vs. Merchant	1777.0	0.122 (ns)	−0.19
Awareness / Readiness	Customer vs. Employee	1515.5	< 0.001 **	−0.52
Awareness / Readiness	Merchant vs. Employee	426.0	0.010 **	−0.42
Ease of Use	Customer vs. Merchant	1525.5	0.888 (ns)	−0.02
Ease of Use	Customer vs. Employee	932.0	0.629 (ns)	0.07
Ease of Use	Merchant vs. Employee	272.0	0.572 (ns)	0.09
Benefit / Security	Customer vs. Merchant	2107.5	0.001 **	−0.41
Benefit / Security	Customer vs. Employee	1176.0	0.206 (ns)	−0.18
Benefit / Security	Merchant vs. Employee	207.0	0.056 (ns)	0.31
Future Intention	Customer vs. Merchant	2234.5	< 0.001 **	−0.49

6. Weak Correlations and the Ceiling Effect

Spearman correlations among the seven customer axes (Appendix, Table A4) were uniformly weak (strongest: privacy–readiness ρ = 0.28; most pairs |ρ| < 0.15) — Pearson's r produced

materially the same pattern, supporting the choice of Spearman as the more appropriate ordinal measure. At this pre-adoption stage, customers do not yet hold one unified attitude in which finding the technology easy predicts trusting or wanting to use it; these beliefs are held largely independently, consistent with judging each construct on its own terms absent an operating system to form one settled impression of. This also explains the low or negative Cronbach's alpha values (Appendix, Table A1): where responses cluster tightly at "agree"/"strongly agree" (a ceiling effect), alpha is starved of the variance it needs to detect covariance regardless of whether the construct is conceptually coherent — future intention illustrates this cleanly, combining the highest mean (4.23) with a negative alpha (−0.28).

Taken together, H1 receives mixed support — ease of use and future intention are both rated highly, but their weak direct correlation ($\rho = -0.08$) suggests the relationship is not straightforwardly linear at the individual level in this sample. H2 is better supported: trust and security ($M = 4.16$) track closely with future intention ($M = 4.23$) at the group level. H3 is clearly supported: the Kruskal-Wallis results confirm perceived readiness differs significantly across the three stakeholder groups.

7. Implications for HCI Design and Practice

From an HCI design standpoint: usability is already high, so design effort is better spent reducing cognitive load around trust and consent (short-form data-use disclosures rather than legal boilerplate), supporting a visible low-friction PIN fallback when a scan fails, and offering both fingerprint and facial modalities so users are not forced into one. Practically, banks should budget for POS-hardware replacement ahead of network upgrades and pair biometrics with PIN for high-value transactions (Section VI, R2); regulators should publish biometric-specific data-governance rules before any pilot, directly answering the unanimous demand for legal protection (Section IV); and solution providers should design for Libya's actual conditions — intermittent power, aging POS fleets, and a customer base already comfortable with fingerprint interaction through workplace attendance.

V. Recommendations

R1 — Offer a choice between fingerprint and facial recognition rather than mandating one. **R2 (central) —** Layer biometrics with a PIN for high-value transactions: this single design choice resolves the privacy paradox (unanimous demand for legal protection alongside little acute daily worry) while fully preserving the ease-of-use advantage all three groups rated highly. **R3 —** Publish clear data-governance rules — storage, retention, breach notification — before any pilot.

sjst.scst.edu.ly
Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)
مجلة صرمان للعلوم والتقنية
Vol 8, No.2. Jun – Dec. 2026
Pages: 224 ~ 238

R4 — Prioritize POS-hardware replacement over network investment: zero employees found current terminals upgradeable, while confidence in servers and networks was comparatively higher. **R5** — Invest in merchant and front-line staff training. **R6** — Begin with a phased, hardware-first pilot limited to branches with confirmed compatibility.

Fig. 4. Empirically-Informed Adoption Pathway

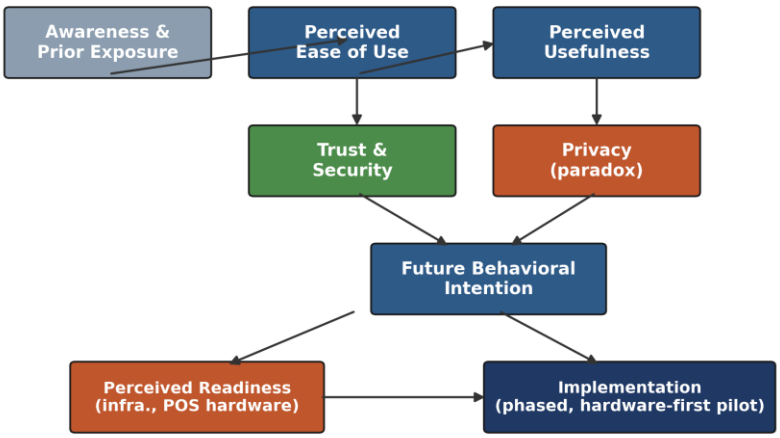

Figure 4. Empirically-informed adoption pathway synthesizing this paper's constructs and recommendations — a conceptual synthesis, not an independently validated structural model.

VI. Limitations and Threats to Validity

The sample is drawn from a single city (Al-Zawiya) using convenience sampling and cannot represent Libya as a whole; the merchant sample was entirely male and age-concentrated, and the employee sample (n = 20) uniformly technical and small in absolute terms — both likely reflecting who was accessible during data collection, and both warrant stratified, larger sampling in follow-up work. No formal pilot test with a separate respondent group preceded full deployment; item wording was instead reviewed for content validity by academic staff in computer science, HCI, and banking technology (Section III), but a dedicated pilot remains a methodological gap. Low internal-consistency estimates (Appendix, Table A1), attributable to short subscales and ceiling effects rather than incoherent design, still limit confidence in each axis as a precise unidimensional measure. All responses reflect anticipated rather than experienced use, since no biometric system currently exists in Libyan banking, and the complete absence of substantive open-ended responses prevented qualitative triangulation.

Internal validity is limited by the absence of random assignment and by convenience sampling. **External validity** is limited to Al-Zawiya and to respondents willing to complete a survey about an unused technology. **Construct validity** is constrained by the purpose-built, non-validated

instrument and short subscales (Section V). **Statistical conclusion validity** is supported by non-parametric tests and effect sizes, but remains limited by modest merchant and employee sample sizes, which reduce power to detect smaller true effects.

VII. Future Work

Priorities include: a larger, stratified, multi-city sample supporting confirmatory factor analysis or Structural Equation Modeling to formally validate the adoption pathway (Fig. 4), currently a conceptual synthesis; a working prototype evaluated through usability testing, think-aloud protocols, and eye-tracking to check attitudinal findings against observed behavior; a longitudinal pilot deployment at a limited number of ATMs or POS terminals comparing stated intention against actual uptake; a comparative study of fingerprint versus facial-recognition modalities specifically; a focused qualitative study clarifying what "legal protection" means to Libyan customers; and a vendor-level survey of POS hardware, converting the perceptual hardware-gap finding into a concrete procurement specification ahead of any mobile-banking deployment.

VIII. Practical Contributions and Deployment Roadmap

This study contributes in three directions. To Libyan banking, it supplies the first evidence-based readiness assessment for biometric authentication, identifying POS-hardware replacement and data governance as the two concrete prerequisites for a pilot. To HCI, it demonstrates a pre-implementation evaluation method — combining axis- and item-level analysis with non-parametric significance testing and post-hoc comparisons — for a system that does not yet exist. To Libya's digital-transformation agenda, it shows a FinTech transition can be evaluated on usability grounds before committing infrastructure spending.

Translating these findings into a deployment sequence: Phase 1 (0–6 months) — audit and replace incompatible POS hardware at a small number of pilot branches, and publish data-governance rules addressing the unanimous demand for legal protection (Section IV). Phase 2 (6–12 months) — run a hardware-first pilot offering both fingerprint and facial modalities with mandatory PIN fallback for high-value transactions (R2), collecting usage logs alongside a follow-up survey. Phase 3 (12–24 months) — expand to additional branches and cities only after Phase 2 confirms the readiness gradient narrows in practice, not only in survey response.

IX. Conclusion

This study asked whether biometric authentication could give Libyan bank card users an experience easier and more usable than PIN-based verification while preserving required security.

Survey data from 150 respondents across three stakeholder groups in Al-Zawiya suggest a cautiously optimistic answer: perceived ease of use was rated highly and consistently, and future intention among customers was the highest-scoring construct measured. A statistically confirmed readiness gradient showed enthusiasm declining from customers to merchants to employees, who identified POS-hardware upgradeability, not network capacity, as the single most concrete obstacle; a privacy paradox combined little acute worry with unanimous demand for legal protection. These findings position Libya's banking sector as usability-ready for a phased, hardware-first move toward biometric authentication, provided user choice, layered security, and transparent data governance are designed in from the outset.

X. Acknowledgment

The author thanks the customers, merchants, and bank employees in Al-Zawiya who volunteered their time to complete the survey underlying this study.

References

[1] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," MIS Quarterly, vol. 13, no. 3, pp. 319–340, 1989.
[2] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," MIS Quarterly, vol. 27, no. 3, pp. 425–478, 2003.
[3] C. Lancelot Miltgen, A. Popovič, and T. Oliveira, "Determinants of end-user acceptance of biometrics: Integrating the 'Big 3' of technology acceptance with privacy context," Decision Support Systems, vol. 56, no. 1, pp. 103–114, 2013.
[4] S. A. Bhat, S. B. Islam, and M. F. Mir, "Consumers' attitude toward biometric banking services: An empirical evaluation of determinants and outcomes," Journal of Financial Services Marketing, vol. 29, pp. 1572–1588, 2024. doi: 10.1057/s41264-024-00285-5.
[5] M. A. Noori, "Biometric authentication technology acceptance in mobile banking in Iraq," NeuroQuantology, vol. 20, no. 7, pp. 3004–3019, 2022.
[6] H. Naji Ali and S. S. M. Al-Dabbagh, "A systematic literature review on biometric authentication in mobile banking," F1000Research, vol. 15, art. 5, 2026. doi: 10.12688/f1000research.173855.2.
[7] J. S. Wang, "Exploring biometric identification in FinTech applications based on the modified TAM," Financial Innovation, vol. 7, art. 42, 2021.
[8] M. Rukhiran, S. Wong-In, and P. Netinant, "User acceptance factors related to biometric recognition technologies of examination attendance in higher education: TAM model," Sustainability, vol. 15, no. 4, art. 3092, 2023.
[9] H. Alnaas, "The barriers of adoption the e-banking in the Libyan banks — A case study of commercial banks in Tobruk city," Open Journal of Business and Management, vol. 10, no. 1, pp. 501–524, 2022.

[10] S. Benqdara, A. Sultan, and A. Elfergani, "Assessment of security issues in banking sector of Libya," International Journal of Computer Applications, vol. 176, no. 13, pp. 12–17, 2020.
[11] W. A. Alkhowaiter, "Digital payment and banking adoption research in Gulf countries: A systematic literature review," International Journal of Information Management, vol. 53, art. 102102, 2020.
[12] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," Psychometrika, vol. 16, no. 3, pp. 297–334, 1951.
[13] R. Allafi and A. A. Darem, "Usability and security in online authentication systems," International Journal of Advanced and Applied Sciences, vol. 12, no. 6, pp. 1–12, 2025.
[14] M. Mujinga, "Usable security of online banking authentication: An exploratory factor analysis," Journal of Information Systems and Informatics, vol. 6, no. 1, pp. 409–420, 2024.
[15] J. Cohen, Statistical Power Analysis for the Behavioral Sciences, 2nd ed. Hillsdale, NJ, USA: Lawrence Erlbaum Associates, 1988.

SJST
sjst.scst.edu.ly
Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)
مجلة صرمان للعلوم والتقنية
Vol 8, No.2. Jun – Dec. 2026
Pages: 224 ~ 238

Appendix

Tables A1–A5 provide item-level and supplementary detail supporting the axis-level results in Section IV, including full reliability results for transparency.

Table A1. Cronbach's Alpha Reliability by Customer Axis (Reported for Transparency)

Axis	Cronbach's α	Interpretation
Awareness & Knowledge	0.67	Acceptable
Perceived Ease of Use	0.03	Low (ceiling effect)
Perceived Usefulness	0.11	Low (ceiling effect)
Trust & Security	0.40	Weak–moderate
Privacy Concerns	−0.10	Not interpretable
Future Behavioral Intention	−0.28	Not interpretable (ceiling effect)
Perceived Readiness	−0.01	Not interpretable

Low or negative values reflect short (2–3 item) subscales combined with ceiling-effect response clustering (Section V), not necessarily incoherent item design.

Table A2. Selected Item-Level Detail — Customer Privacy and Readiness Items

#	Item (English translation)	Mean	SD	%≥4
Q13	Concerned about misuse of my biometric data.	2.79	0.73	12.0
Q14	Fear fingerprint data could be hacked or leaked.	2.76	0.64	10.0
Q15	Clear laws are needed to protect biometric data.	4.54	0.50	100.0
Q19	Libyan banks will be able to implement biometric systems.	3.33	0.74	49.0

Table A3. Selected Item-Level Detail — Bank-Employee Infrastructure Items

#	Item (English translation)	Mean	SD	%≥4
Q1	Basic infrastructure (servers, networks) exists.	4.00	0.79	70.0
Q2	Current POS devices in market can be upgraded.	2.50	0.51	0.0
Q3	Continuous power/internet connectivity is sufficient.	3.75	0.44	75.0

Table A4. Spearman Rank Correlation Matrix Among Customer Perception Axes (n = 100)

Axis	Aware.	EoU	Useful.	Trust	Privacy	Intent	Ready.
Awareness	1.00	0.20	0.09	−0.01	0.12	0.09	−0.03
Ease of Use	0.20	1.00	0.21	−0.09	0.04	−0.08	0.03
Usefulness	0.09	0.21	1.00	0.16	−0.05	0.01	0.02
Trust	−0.01	−0.09	0.16	1.00	0.00	0.09	0.01
Privacy	0.12	0.04	−0.05	0.00	1.00	0.03	0.28
Future Int.	0.09	−0.08	0.01	0.09	0.03	1.00	0.15
Readiness	−0.03	0.03	0.02	0.01	0.28	0.15	1.00

sjst.scst.edu.ly
Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)
مجلة صرمان للعلوم والتقنية
Vol 8, No.2. Jun – Dec. 2026
Pages: 224 ~ 238

Table A5. Gender Comparison Among Customers — Mann-Whitney U Test with Effect Size

Axis	Male (n=68)	Female (n=32)	p-value	Rank-biserial r
Awareness & Knowledge	4.07	3.80	0.093 (ns)	−0.207
Perceived Ease of Use	4.12	3.99	0.460 (ns)	−0.091
Perceived Usefulness	4.20	4.06	0.435 (ns)	−0.095
Trust & Security	4.16	4.17	0.991 (ns)	0.002
Privacy Concerns	3.36	3.36	0.769 (ns)	0.035
Future Behavioral Intention	4.24	4.21	0.929 (ns)	0.011
Perceived Readiness	3.75	3.80	0.672 (ns)	0.051

ns = not significant at α = 0.05. Rank-biserial r follows conventional small (~0.1) / medium (~0.3) / large (~0.5) benchmarks; all values here are negligible to small.