



# CUSTOMER PERCEPTION OF AI-BASED FRAUD DETECTION AND SECURITY IN DIGITAL BANKING

<sup>1</sup> W. Infant Emiliya, <sup>2</sup> Dr. S. Leema Rosaline

<sup>1</sup> Research Scholar, <sup>2</sup> Assistant Professor, Research Supervisor

<sup>1</sup>Department of Commerce, Nirmala College for Women, Coimbatore.

**Abstract :** The study entitled “Customer Perception of AI-Based Fraud Detection and Security in Digital Banking” aims to examine customer perceptions of artificial intelligence (AI)-based fraud detection and security features in digital banking in Coimbatore City. The increasing use of digital banking has created a need for effective security measures to identify suspicious transactions, prevent fraudulent activities, and protect customer information. AI-based systems help banks monitor transaction patterns, detect unusual activities, and provide real-time security alerts. However, customer awareness, perceived safety, trust, and privacy concerns may influence their willingness to use AI-enabled banking services. The study adopts a descriptive and analytical research design, with a proposed sample of 250 digital banking customers in Coimbatore City. Primary data are collected through a structured questionnaire, while secondary data are obtained from relevant journals, books, and reports. The data are analysed using percentage analysis, descriptive statistics, reliability analysis, factor analysis, correlation, multiple regression, and the chi-square test. The study seeks to understand the factors influencing customer confidence and acceptance of AI-based fraud detection and security features. The findings are expected to help banks improve customer awareness, strengthen data privacy practices, enhance transparency, and build trust in AI-enabled digital banking services.

**Index Terms:** Artificial Intelligence, Fraud Detection, Digital Banking, Customer Perception, Customer Trust, Data Privacy, Perceived Security, Coimbatore City.

## I. INTRODUCTION

Artificial Intelligence (AI) has become an important technology in the digital banking sector, particularly in identifying suspicious transactions, detecting fraudulent activities, monitoring unusual customer behaviour and strengthening transaction security. The increasing use of mobile banking, internet banking, digital payment applications and online fund transfers has created a need for effective mechanisms to protect customers against financial fraud. Traditional fraud detection systems often depend on predefined rules and may struggle to identify complex or rapidly changing fraud patterns. AI-based fraud detection systems use machine learning algorithms, behavioural analytics and pattern recognition to examine transaction data, identify unusual activities and generate alerts for potentially fraudulent transactions. These technologies can help banks improve fraud detection speed, reduce financial losses and enhance the security of digital banking services. However, the effectiveness of these systems also depends on customers' awareness of AI-based security features, their perceived safety while conducting digital transactions, their trust in banking institutions and their concerns regarding data privacy. Customers may hesitate to use AI-enabled banking services if they fear unauthorised access to personal information, incorrect fraud alerts, unfair transaction blocking or a lack of transparency in automated decisions. Therefore, understanding customer perceptions is essential for improving the acceptance and effectiveness of AI-based fraud detection. The present study examines customer perception of AI-based fraud detection and security in digital banking, focusing on security awareness, perceived safety, customer trust, privacy concerns and willingness to use AI-enabled banking services. The findings are intended to help banks strengthen customer confidence, improve security communication and promote the responsible use of AI in digital banking.

## II. STATEMENT OF THE PROBLEM

The rapid growth of digital banking has increased the importance of protecting customers against cyber fraud, unauthorised transactions, phishing attacks and identity theft. Although AI-based fraud detection systems can help banks identify suspicious transactions and monitor unusual banking activities, the successful implementation of these technologies does not automatically ensure customer confidence or acceptance. Customers may have limited awareness of how AI detects fraudulent transactions and may question the accuracy, reliability and transparency of automated security decisions. Concerns about personal data collection, privacy breaches, false fraud alerts and the temporary blocking of genuine transactions may further influence their willingness to use AI-enabled banking services. In addition, differences in customers' technological knowledge and previous digital banking experiences may affect their perceptions of security and trust. Therefore, it is necessary to examine how security awareness,

perceived safety, customer trust and privacy concerns influence customers' willingness to use AI-based fraud detection and security services in digital banking. The study seeks to identify the major factors shaping customer perceptions and provide suggestions for improving security awareness, privacy protection and trust in AI-enabled banking services.

### III. OBJECTIVES OF THE STUDY

1. To assess customers' awareness of AI-based fraud detection and security features in digital banking.
2. To examine customers' perceptions of safety and trust in AI-enabled fraud detection systems.
3. To identify the major privacy concerns associated with AI-based digital banking security.
4. To analyse the relationship between security awareness, perceived safety, customer trust, privacy concerns and willingness to use AI-enabled banking services.
5. To determine the influence of perceived safety, customer trust and privacy concerns on willingness to use AI-based fraud detection services.
6. To examine the association between selected demographic characteristics and customers' awareness and willingness to use AI-enabled banking security services.

### IV. REVIEW OF LITERATURE

1. Ngai et al. (2011), "The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature." The authors reviewed the application of data-mining techniques in financial fraud detection and developed a classification framework for understanding different fraud detection approaches. The study highlighted the importance of analytical techniques in identifying suspicious patterns and supporting financial institutions in fraud prevention. It provides a conceptual foundation for understanding the technological role of AI and data analytics in financial security. However, its primary focus is on detection techniques rather than customer trust or acceptance.
2. Arner, Barberis, and Buckley (2016), "The Evolution of Fintech: A New Post-Crisis Paradigm?" The authors examined the development of financial technology and its implications for financial services and regulation. The study discussed the transformation of financial services through digital innovation and technology-driven processes. Its relevance to the present research lies in explaining the broader technological environment in which AI-enabled banking security systems operate and the importance of appropriate regulatory and institutional safeguards. The article is a broad fintech study rather than a direct empirical investigation of customer perceptions of AI fraud detection.
3. Vives (2019), "Digital Disruption in Banking." Vives examined the effects of digital technology and new entrants on the banking industry, including changes in competition, customer relationships and financial intermediation. The study explained how technological developments reshape banking services and create new opportunities as well as challenges for established financial institutions. It provides a useful background for examining customer confidence in technology-enabled banking. Its contribution is primarily at the banking-industry level rather than a direct assessment of AI fraud detection acceptance.
4. McKinsey & Company (2020), "The Future of Payments: The Digitalization of Payments and Its Impact on the Financial Services Industry." McKinsey's industry research on digital payments and financial technology has discussed the changing payment environment, evolving customer expectations and the need for secure, reliable digital financial services. Such industry analysis provides contextual support for examining fraud prevention and customer confidence in digital transactions. However, industry reports should be distinguished from peer-reviewed empirical studies, and the precise title and publication details of any specific report should be verified before inclusion in a formal reference list.
5. Davis (1989), "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." Davis developed and tested the Technology Acceptance Model (TAM), identifying perceived usefulness and perceived ease of use as important determinants of technology acceptance. The model provides a foundation for examining customers' willingness to use AI-enabled banking security services. In the present study, customers may be more willing to accept AI fraud detection when they believe that it improves transaction security and is easy to understand and use. The original study did not specifically investigate AI or banking fraud detection, but its theoretical framework is relevant to adoption research.
6. Pavlou (2003), "Consumer Acceptance of Electronic Commerce—Integrating Trust and Risk with the Technology Acceptance Model." Pavlou integrated trust and perceived risk into the Technology Acceptance Model to explain consumer acceptance of electronic commerce. The study demonstrated the relevance of trust and risk perceptions when individuals decide whether to engage in technology-mediated transactions. This framework is relevant to AI-enabled banking because customers may evaluate not only the usefulness of fraud detection but also the reliability of the system and the risks associated with sharing financial information. The study focused on electronic commerce rather than AI-based banking security specifically.
7. Srivastava and Sharma (2024), "Customer Trust and Data Privacy in Digital Banking Services – A Study in Context of Artificial Intelligence." The authors investigated customer trust, data privacy and AI in digital banking using responses from 206 participants. The study employed Spearman's rank correlation to examine the relationships between perceived security features, AI quality, customer satisfaction and trust. The findings indicated significant positive relationships between security features, AI quality, customer satisfaction and customer trust. This study is particularly relevant because it examines the relationship between security perceptions and trust in AI-enabled digital banking.
8. Yaseen and Al-Amarneh (2025), "Adoption of Artificial Intelligence-Driven Fraud Detection in Banking: The Role of Trust, Transparency, and Fairness Perception in Financial Institutions in the United Arab Emirates and Qatar." The authors examined the adoption of AI-driven fraud detection in financial institutions, focusing on trust, transparency and perceived fairness. The study highlighted the importance of explainable AI systems, transparent decision-making and fairness-sensitive implementation for encouraging acceptance of AI-based fraud detection. Its findings provide a relevant conceptual basis for investigating how customer trust and perceptions of fair treatment may affect willingness to use AI-enabled security services.
9. Haque et al. (2025), "Responsible AI Governance in Banking: An Empirical Study of Fraud Detection, Privacy Protection, and Customer Trust Among US Practitioners." This study examined AI-based fraud detection, privacy protection, responsible governance and trust among banking, fintech and information-technology professionals in the United States. The researchers analysed 165 usable responses using descriptive statistics, Pearson correlation and multiple regression. Their findings indicated positive relationships between trust, perceived fraud detection effectiveness and privacy protection, while perceived privacy risk was negatively associated with trust. The study reinforces the importance of privacy safeguards and responsible AI governance in

strengthening confidence in banking security systems. Its respondents were industry professionals rather than bank customers, which is an important distinction when applying its findings to customer perception research.

10. Madhana et al. (2026), “An AI-Driven Framework for Cybersecurity Awareness and User Trust in Indian Digital Banking.” The researchers examined cybersecurity awareness, perceived threats, educational support and user trust in Indian digital banking. The study collected responses from more than 500 university students across India and used statistical modelling alongside AI-based predictive analytics. Its focus on cybersecurity awareness and trust is closely related to the present study, particularly the need to understand how awareness and perceptions of digital threats affect customers' confidence in digital banking. The university-student sample, however, may not fully represent customers across all age groups and occupations.

11. “AI-Driven Cybersecurity in Mobile Financial Services: Enhancing Fraud Detection and Privacy in Emerging Markets” (2025). This study used a mixed-method approach involving a quantitative survey of 151 respondents and qualitative analysis of open-ended responses. It examined AI-based fraud detection alongside user privacy concerns in mobile financial services. The reported results indicated that respondents recognised the benefits of AI fraud detection while expressing concerns about privacy, transparency and control over personal information. The study is relevant to the present research because it demonstrates why the technical benefits of AI need to be examined alongside customer concerns and trust.

**Research gap:** The literature indicates that fraud detection technology, cybersecurity awareness, privacy protection and customer trust are closely related research areas. Nevertheless, the present study brings together five specific customer-level dimensions—security awareness, perceived safety, trust, privacy concerns and willingness to use AI-based fraud detection—in a single empirical framework. It also proposes factor analysis, correlation, regression and chi-square testing to examine both the structure of customer perceptions and the relationships among the variables.

## V. RESEARCH METHODOLOGY

### 5.1 Research design

The study adopts a descriptive and analytical research design. The descriptive component examines customers' awareness, perceptions and concerns regarding AI-based fraud detection, while the analytical component investigates relationships among security awareness, perceived safety, trust, privacy concerns and willingness to use AI-enabled banking services.

### 5.2 Area of the study

The study is conducted in Coimbatore City, Tamil Nadu, focusing on customers who use digital banking services offered by banks. The study examines customer perceptions of AI-based fraud detection and security, with particular reference to security awareness, perceived safety, customer trust, privacy concerns and willingness to use AI-enabled banking services.

### 5.3 Population and sample size

The population comprises customers who use digital banking services and have experience with, or awareness of, digital banking security features. The sample size is 250 respondents.

### 5.4 Sampling technique

Convenience sampling used to recruit eligible digital banking customers who are accessible and willing to participate. The study should report the actual recruitment procedure and eligibility criteria.

### 5.5 Sources of data

- Primary data: Responses collected through a structured questionnaire from digital banking customers.
- Secondary data: Peer-reviewed journal articles, books, RBI publications and relevant research reports on digital banking, AI-based fraud detection, cybersecurity, privacy and technology acceptance.

### 5.6 Questionnaire design

The questionnaire contains two sections:

- Section A – Demographic and usage profile: Gender, age, educational qualification, occupation, monthly income, frequency of digital banking use and awareness of AI-based security features.
- Section B – Research variables: Security awareness, perceived safety, customer trust, privacy concerns and willingness to use AI-enabled fraud detection.

### 5.7 Hypotheses

H<sub>01</sub>: There is no significant relationship between security awareness and willingness to use AI-based fraud detection.

H<sub>02</sub>: There is no significant relationship between perceived safety and willingness to use AI-based fraud detection.

H<sub>03</sub>: There is no significant relationship between customer trust and willingness to use AI-based fraud detection.

H<sub>04</sub>: There is no significant relationship between privacy concerns and willingness to use AI-based fraud detection.

H<sub>05</sub>: Security awareness, perceived safety, customer trust and privacy concerns do not significantly predict willingness to use AI-based fraud detection.

H<sub>06</sub>: There is no significant association between educational qualification and awareness of AI-based fraud detection.

A 5% level of significance ( $(p < 0.05)$ ) used for hypothesis testing.

## VI. DATA ANALYSIS AND INTERPRETATION

### 6.1 Demographic Profile of Respondents

TABLE I. DEMOGRAPHIC PROFILE OF RESPONDENTS

| Demographic variable | Category       | Frequency | Percentage |
|----------------------|----------------|-----------|------------|
| Gender               | Male           | 138       | 55.2       |
|                      | Female         | 112       | 44.8       |
| Age                  | 18–25 years    | 55        | 22.0       |
|                      | 26–35 years    | 85        | 34.0       |
|                      | 36–45 years    | 62        | 24.8       |
|                      | 46–55 years    | 32        | 12.8       |
|                      | Above 55 years | 16        | 6.4        |

|           |                           |     |       |
|-----------|---------------------------|-----|-------|
| Education | School / Higher Secondary | 30  | 12.0  |
|           | Diploma / UG              | 130 | 52.0  |
|           | PG and above              | 90  | 36.0  |
| Total     |                           | 250 | 100.0 |

Interpretation: The suggested distribution indicates that male respondents constitute 55.2% of the sample, while female respondents account for 44.8%. The 26–35 years age group represents the largest category (34%). Diploma and undergraduate-qualified respondents constitute 52% of the sample. This table describes the sample composition; the actual demographic findings should be calculated from the collected questionnaires.

## 6.2 Awareness of AI-Based Fraud Detection

TABLE II. AWARENESS OF AI-BASED FRAUD DETECTION

| Awareness level    | Frequency | Percentage |
|--------------------|-----------|------------|
| High awareness     | 75        | 30.0       |
| Moderate awareness | 110       | 44.0       |
| Low awareness      | 65        | 26.0       |
| Total              | 250       | 100.0      |

Interpretation: The proposed distribution shows that 44% of respondents fall within the moderate-awareness category, followed by 30% with high awareness and 26% with low awareness. This suggests that customers may have some familiarity with AI-based security features but may need further education on how suspicious transactions are detected, how fraud alerts operate and how to respond to security warnings.

## 6.3 Descriptive Statistics of Research Variables

TABLE III. DESCRIPTIVE STATISTICS OF RESEARCH VARIABLES

| Research variable     | Mean | Standard deviation | Suggested interpretation |
|-----------------------|------|--------------------|--------------------------|
| Security awareness    | 3.58 | 0.76               | Moderately high          |
| Perceived safety      | 3.71 | 0.72               | Moderately high          |
| Customer trust        | 3.55 | 0.79               | Moderately high          |
| Privacy concerns      | 3.82 | 0.81               | Relatively high          |
| Willingness to use AI | 3.76 | 0.73               | Moderately high          |

Interpretation: The proposed mean scores indicate relatively high privacy concerns, with a mean of 3.82, followed by willingness to use AI-based security services (3.76) and perceived safety (3.71). Security awareness and customer trust have mean scores of 3.58 and 3.55, respectively. This pattern would suggest that customers can recognise the potential benefits of AI-based fraud detection while continuing to have concerns about personal information and system reliability. The actual interpretation should follow the scale's predefined scoring criteria.

## 6.4 Correlation Analysis

Objective: To examine the relationships between security awareness, perceived safety, customer trust, privacy concerns and willingness to use AI-based fraud detection.

TABLE IV. CORRELATION MATRIX

| Variables             | Awareness | Safety | Trust | Privacy concerns | Willingness |
|-----------------------|-----------|--------|-------|------------------|-------------|
| Security awareness    | 1.00      | 0.48   | 0.45  | -0.20            | 0.42        |
| Perceived safety      | 0.48      | 1.00   | 0.62  | -0.35            | 0.59        |
| Customer trust        | 0.45      | 0.62   | 1.00  | -0.40            | 0.66        |
| Privacy concerns      | -0.20     | -0.35  | -0.40 | 1.00             | -0.32       |
| Willingness to use AI | 0.42      | 0.59   | 0.66  | -0.32            | 1.00        |

Interpretation: The proposed pattern suggests positive relationships between willingness to use AI-based fraud detection and security awareness, perceived safety and customer trust. Customer trust has the strongest positive correlation with willingness to use AI ( $r=0.66$ ). Privacy concerns show a negative relationship with willingness to use AI ( $r=-0.32$ ). This would suggest that trust-building and privacy safeguards may be important for encouraging customer acceptance. Correlation alone does not establish causation.

## 6.5 Multiple Regression Analysis

Dependent variable: Willingness to use AI-based fraud detection.

Independent variables: Security awareness, perceived safety, customer trust and privacy concerns.

The regression model is:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \epsilon$$

Where  $(Y)$  represents willingness to use AI, and  $(X_1)$  to  $(X_4)$  represent the four independent variables.

TABLE V. MULTIPLE REGRESSION ANALYSIS

| Independent variable | Standardised $\beta$ | Suggested significance |
|----------------------|----------------------|------------------------|
| Security awareness   | 0.16                 | $p = 0.006$            |
| Perceived safety     | 0.27                 | $p < 0.001$            |
| Customer trust       | 0.38                 | $p < 0.001$            |
| Privacy concerns     | -0.17                | $p = 0.003$            |

Interpretation: Under this proposed pattern, customer trust is the strongest positive predictor of willingness to use AI-based fraud detection, followed by perceived safety and security awareness. Privacy concerns have a negative association with willingness to use AI. If these patterns are confirmed in the collected data, they would indicate that customers are more likely to accept AI-based

security services when they trust the bank and believe its systems can protect their transactions. Banks would also need to address privacy concerns through transparent data practices and appropriate security safeguards.

## 6.6 Chi-Square Test

**Objective:** To examine whether educational qualification is associated with awareness of AI-based fraud detection.

**H0:** There is no significant association between educational qualification and awareness of AI-based fraud detection.

**H1:** There is a significant association between educational qualification and awareness of AI-based fraud detection.

**TABLE VI. CHI-SQUARE TEST**

| Test statistic         | Value                 |
|------------------------|-----------------------|
| Pearson chi-square     | 12.84                 |
| Degrees of freedom     | 4                     |
| Significance (p-value) | 0.012                 |
| Decision at 5% level   | Reject H <sub>0</sub> |

Interpretation: If the actual chi-square result were  $\chi^2=12.84$ , with 4 degrees of freedom and  $(p=0.012)$ , there would be a statistically significant association between educational qualification and awareness of AI-based fraud detection. The null hypothesis would be rejected at the 5% level. This would indicate that awareness levels differ across educational categories, although the test alone would not establish which categories differ most or whether education causes greater awareness. The observed frequency table and expected cell counts must be checked to ensure the chi-square assumptions are satisfied.

## VII. FINDINGS OF THE STUDY

**Demographic profile:** Examine the distribution of respondents by gender, age, education, occupation and income to understand the composition of the sample.

**Security awareness:** Determine the proportion of respondents with high, moderate and low awareness of AI-based fraud detection and digital security features.

**Perceived safety:** Assess whether customers feel that AI-based security systems help protect digital transactions and identify suspicious activities.

**Customer trust:** Examine customers' confidence in banks' ability to detect fraud accurately, protect financial information and handle suspicious transactions responsibly.

**Privacy concerns:** Identify concerns relating to the collection, storage, use and possible unauthorised disclosure of personal and financial data.

**Willingness to use AI:** Measure customers' willingness to continue using or adopt AI-enabled fraud detection and security services.

**Factor analysis:** Determine whether the questionnaire items group into meaningful dimensions and whether the proposed five constructs are supported by the data.

**Correlation analysis:** Establish the direction and strength of relationships among awareness, perceived safety, trust, privacy concerns and willingness to use AI.

**Regression analysis:** Identify which variables significantly predict willingness to use AI-based fraud detection when the other predictors are considered simultaneously.

**Chi-square analysis:** Examine whether awareness is associated with selected demographic characteristics, including educational qualification.

## VIII. SUGGESTIONS

Banks should strengthen customer awareness of AI-based fraud detection through regular digital-literacy programmes, simple security guides and clear explanations of how suspicious transactions are identified. Customers should receive timely alerts for unusual transactions, along with practical instructions for verifying transactions and reporting suspected fraud. Banks should improve transparency by explaining how customer information is collected, used and protected, while providing accessible privacy settings and clear consent procedures where applicable. Regular testing and monitoring of AI systems should be conducted to minimise missed fraud, false alerts and unnecessary blocking of genuine transactions. Customers should also have access to human assistance when automated security systems flag transactions or restrict account activity. A clear grievance-redressal mechanism should provide complaint reference numbers, expected resolution times and updates on disputed transactions. Banks should collect feedback from customers across age, educational and income groups to identify differences in awareness and accessibility. Finally, AI systems should be supported by appropriate data protection, accountability, human oversight and regular performance reviews to build customer trust and encourage responsible adoption of digital banking security services.

## IX. CONCLUSION

The study focuses on customer perception of AI-based fraud detection and security in digital banking, with particular emphasis on security awareness, perceived safety, customer trust, privacy concerns and willingness to use AI-enabled services. AI has the potential to strengthen fraud detection by identifying suspicious transaction patterns and enabling timely alerts. However, customer acceptance depends not only on technological capability but also on confidence in the bank's security practices, transparency and responsible handling of personal information. The proposed analytical framework uses descriptive statistics, reliability analysis, exploratory factor analysis, correlation, multiple regression and chi-square testing to examine these dimensions. If the proposed relationships are supported by the actual data, customer trust and perceived safety may emerge as important predictors of willingness to use AI, while privacy concerns may act as a barrier. Banks should therefore combine effective fraud detection with transparent communication, privacy protection, customer education and accessible human support. Such measures can help improve customer confidence and promote the responsible use of AI in digital banking.

**REFERENCES**

1. Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of fintech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47(4), 1271–1319.
2. 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>
3. Haque, M. N., et al. (2025). Responsible AI governance in banking: An empirical study of fraud detection, privacy protection, and customer trust among US practitioners. *Journal of Primeasia*, 6(1), 1–10. <https://doi.org/10.25163/primeasia.6110903>
4. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3), 559–569. <https://doi.org/10.1016/j.dss.2010.08.006>
5. Pavlou, P. A. (2003). Consumer acceptance of electronic commerce—Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101–134. <https://doi.org/10.1080/10864415.2003.11044275>
6. Srivastava, S., & Sharma, S. (2024). Customer trust and data privacy in digital banking services – A study in context of artificial intelligence. *ShodhKosh: Journal of Visual and Performing Arts*, 5(1). <https://doi.org/10.29121/shodhkosh.v5.i1.2024.3505>
7. Vives, X. (2019). Digital disruption in banking. *Annual Review of Financial Economics*, 11, 243–272. <https://doi.org/10.1146/annurev-financial-100719-120854>
8. Yaseen, H., & Al-Amarneh, A. (2025). Adoption of artificial intelligence-driven fraud detection in banking: The role of trust, transparency, and fairness perception in financial institutions in the United Arab Emirates and Qatar. *Journal of Risk and Financial Management*, 18(4), Article 217. <https://doi.org/10.3390/jrfm18040217>
9. Reserve Bank of India. (2025). Annual report 2024–25. Reserve Bank of India. <https://www.rbi.org.in/scripts/AnnualReportPublications.aspx?Id=1436>
10. Madhana, B., Shaik, D., Tank, G., Bahl, A., et al. (2026). An AI-driven framework for cybersecurity awareness and user trust in Indian digital banking. *Scientific Reports*. <https://doi.org/10.1038/s41598-026-55966-z>.