Journal of Advances in Developmental Research (IJAIDR)

E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

Cybersecurity Risks and their Impact on Digital Banking Services: An Empirical Analysis

Narendra Bairwa[1], Dr. Mini Amit Arrawatia[2]

[1]Research Scholar, Department of Commerce, Jayoti Vidyapeeth Women's University, Jaipur
[2]Professor, Department of Commerce, Jayoti Vidyapeeth Women's University, Jaipur

Abstract

The rapid digitalisation of banking in India propelled by internet and mobile banking, the Unified Payments Interface (UPI), Aadhaar-enabled payments and neo-banking platforms has transformed the delivery of financial services while simultaneously enlarging the attack surface available to cyber criminals. Phishing, vishing, malware, ransomware, SIM-swap frauds, credential theft, social-engineering scams and attacks on third-party service providers now constitute material risks to banks and their customers. This paper examines the nature and magnitude of cybersecurity risks confronting digital banking and empirically analyses their impact on customer trust, usage behaviour and the operational and financial performance of banks.

The study employs a mixed-method design. Secondary data on digital transaction volumes, reported bank frauds and cyber incidents are drawn from publications of the Reserve Bank of India (RBI), the Indian Computer Emergency Response Team (CERT-In), the National Crime Records Bureau (NCRB) and the National Payments Corporation of India (NPCI) for the period 2018–19 to 2024–25. Primary evidence is presented through an illustrative structured-questionnaire survey of 400 digital banking users, analysed using percentages, weighted mean scores, Cronbach's alpha, chi-square tests, correlation and multiple regression. The analysis indicates that exposure to cyber incidents and perceived cyber risk significantly reduce customer trust and the intensity of digital banking usage, while awareness of security practices and bank-provided safeguards moderate this negative effect. At the institutional level, cyber events impose direct financial losses, regulatory penalties, remediation costs and reputational damage. The paper concludes that cybersecurity is no longer a technical back-office function but a strategic determinant of digital banking adoption, and offers recommendations for banks, regulators and customers, including zero-trust architectures, continuous security testing, customer education, stronger incident reporting and rapid grievance redress.

Keywords: Cybersecurity, Digital Banking, Cyber Fraud, Phishing, Customer Trust, UPI, Internet Banking, Risk Perception, India.

Introduction

Banking in India has undergone a profound digital transformation over the last decade. The launch of the Unified Payments Interface in 2016, the proliferation of smartphones and affordable data, the policy push following demonetisation, and the behavioural shift induced by the COVID-19 pandemic have together moved an enormous share of banking transactions from branches to digital channels. UPI alone

now processes more than 16–18 billion transactions a month, and the RBI's Digital Payments Index has more than quadrupled since its base period of March 2018. Internet banking, mobile banking applications, digital wallets, Aadhaar-enabled Payment Systems (AePS), WhatsApp banking and API-based open banking have made financial services available anytime and anywhere.

This convenience, however, has a shadow side. Every new digital channel, interface and third-party integration expands the attack surface of the banking system. Cyber criminals have kept pace with and often outpaced the defensive capabilities of institutions and the awareness of customers. India consistently ranks among the most-attacked countries in global threat reports, and CERT-In handles over a million security incidents annually. RBI data show that in recent years the overwhelming majority of bank frauds by number occur in the digital payments (card/internet) category, even though their individual ticket sizes are small. The Indian Cyber Crime Coordination Centre (I4C) and the 1930 cyber-fraud helpline have registered explosive growth in complaints relating to online financial fraud.

Digital Banking Services: Scope and Channels

For the purposes of this study, digital banking services encompass: (i) internet banking through browsers; (ii) mobile banking applications; (iii) UPI and wallet-based payments; (iv) card-not-present e-commerce transactions; (v) AePS and micro-ATM transactions; and (vi) emerging channels such as open-banking APIs and digital-only (neo) banking platforms. These channels differ in their authentication mechanisms, risk profiles and typical fraud vectors, but all share dependence on the confidentiality, integrity and availability of information systems — the classic CIA triad of information security.

Cybersecurity Risks in Digital Banking

Cybersecurity risk in banking may be defined as the probability of loss financial, operational, reputational or legal arising from unauthorised access, use, disclosure, disruption, modification or destruction of information systems and data. The principal risk vectors relevant to digital banking include: phishing and smishing (fraudulent emails/SMS harvesting credentials); vishing (voice-call social engineering, including fake bank officials and 'digital arrest' scams); malware and banking trojans on customer devices; SIM-swap and OTP-interception frauds; ransomware and denial-of-service attacks on bank infrastructure; ATM and card skimming; insider threats; supply-chain and third-party vendor compromises; and API vulnerabilities in open-banking ecosystems. The human element customer negligence and social engineering is consistently identified in industry reports as the weakest link, implicated in the majority of successful attacks.

The Central Research Question and Significance

While the growth of digital banking and the growth of cybercrime are both well documented, the connecting question how cybersecurity risks affect the usage, trust and economics of digital banking requires empirical scrutiny. If rising fraud erodes customer confidence, the digital-payments revolution itself is at stake; the RBI has repeatedly emphasised that trust is the foundation of digital finance. For banks, cyber events translate into direct losses, customer compensation, regulatory penalties under RBI and CERT-In directions, litigation, higher insurance premia and reputational damage that is difficult to quantify but strategically decisive. For policymakers, understanding which risks most damage customer

confidence helps prioritise regulatory and awareness interventions. This study is significant because it integrates the institutional (bank-level) and behavioural (customer-level) dimensions of the problem within a single empirical framework, in the specific context of India's mass-scale, low-ticket digital payments ecosystem, which differs markedly from the card-dominated systems studied in Western literature.

Review of Literature

Studies on Digital Banking Adoption

The adoption literature is anchored in the Technology Acceptance Model (Davis, 1989), which posits perceived usefulness and perceived ease of use as the primary determinants of technology adoption, and in its extension UTAUT (Venkatesh et al., 2003). Applications to internet banking added trust and risk as central constructs: Pikkarainen et al. (2004) found security concerns to be a significant inhibitor of online banking acceptance in Finland, while Lee (2009) demonstrated that perceived risk comprising security, financial, social and time risk significantly reduces intention to use online banking, with security/privacy risk exerting the largest negative effect. In India, studies by Safeena et al. (2011) and Bashir and Madhavaiah (2015) confirmed that perceived risk and trust are decisive for internet-banking intention among Indian customers, alongside usefulness and ease of use.

Studies on Cybersecurity Threats in Banking

A second stream documents the threat landscape. Anderson et al. (2013), in a widely cited study of the costs of cybercrime, showed that indirect costs defensive expenditure and loss of confidence far exceed the direct amounts stolen. Industry analyses such as the IBM Cost of a Data Breach reports place the average breach cost in the financial sector among the highest of all industries, with global averages in the range of USD 5–6 million per breach in recent years. In the Indian context, RBI's Report on Trend and Progress of Banking in India shows that frauds in the card/internet category dominate by number of cases, and the RBI Ombudsman receives a rising share of complaints relating to digital transactions. Studies by Bamrara et al. (2013) on cyber attacks in Indian banks, and later work on UPI-era frauds, catalogue phishing, vishing, SIM-swap QR-code manipulation, screen-sharing app abuse and remote-access frauds as the dominant modus operandi against Indian customers, in contrast to the technical intrusions that dominate attacks on institutions.

Studies Linking Cyber Risk with Trust, Usage and Bank Performance

The third stream connects security events with behavioural and financial outcomes. Event studies on data breaches (e.g., Campbell et al., 2003; Kamiya et al., 2021) find significant negative abnormal stock returns for breached firms, with larger effects when personal financial data are compromised. Behavioural studies find that direct victimisation and even media exposure to fraud reduce trust and subsequent use of digital channels; Jansen and Leukfeldt (2016) documented how phishing victimisation changes customer banking behaviour. Research on trust repair shows that prompt reimbursement, transparent communication and visible security improvements can restore usage, which is reflected in the RBI's customer-liability circular of 2017 limiting customer liability in unauthorised electronic transactions. Studies of security countermeasures two-factor authentication, tokenisation, transaction alerts, AI-based fraud monitoring indicate meaningful reductions in fraud losses, supporting the business case for cybersecurity investment.

Research Gap

Three gaps motivate this study. First, most Indian empirical work predates the UPI-era explosion of small-ticket digital payments and the corresponding shift of fraud from technical hacking toward social engineering; the post-2020 landscape is under-researched. Second, institutional studies (fraud statistics, breach costs) and behavioural studies (customer perception) have largely proceeded separately; few papers integrate both to trace the full chain from threat to incident to trust to usage to bank performance. Third, the moderating role of customer awareness and bank-provided safeguards on the risk–trust relationship remains insufficiently quantified in the Indian setting. The present study addresses these gaps through a combined secondary-data and survey-based empirical analysis.

Objectives of the Study

The study pursues the following objectives:

1. To examine the growth of digital banking services in India and the corresponding trends in cyber incidents and digital payment frauds.
2. To identify and classify the major cybersecurity risks confronting digital banking services.
3. To analyse customers' awareness of cybersecurity threats and safe digital banking practices.
4. To empirically assess the impact of perceived cyber risk and fraud experience on customer trust and the usage of digital banking services.
5. To evaluate the institutional impact of cyber incidents on banks in terms of financial loss, operational disruption and reputation.
6. To suggest measures for banks, regulators and customers to mitigate cybersecurity risks and sustain trust in digital banking.

Research Methodology

Research Design

The study follows a descriptive-cum-analytical, mixed-method design combining longitudinal secondary data with a cross-sectional primary survey. The secondary component maps the macro trends of digital transactions and cyber frauds; the primary component measures customer perception, awareness, trust and behaviour.

Sources of Data

Secondary data are compiled from the RBI (Report on Trend and Progress of Banking in India; Annual Report; Payment System Statistics; Digital Payments Index), NPCI product statistics, CERT-In annual reports, NCRB Crime in India reports, I4C/National Cyber Crime Reporting Portal disclosures and published research. Primary data are collected through a structured questionnaire administered to users of digital banking services. The questionnaire covers demographics, usage patterns, awareness of threats and safe practices, fraud experience, perceived risk, perceived bank safeguards, trust and behavioural response, using five-point Likert scales for perceptual items.

Sample Design

The survey employs a non-probability convenience-cum-purposive sample of 400 respondents who use at least one digital banking channel, drawn from urban, semi-urban and rural respondents to reflect the spread of digital payments. The sample size satisfies the common social-science threshold ($n \geq 384$ for a 95 per cent confidence level and 5 per cent margin of error for large populations). It must be emphasised

that the survey results reported in Section 8 are illustrative model data constructed to demonstrate the analytical framework and the expected pattern of relationships documented in prior literature; researchers replicating the study should collect and substitute actual field data.

Period of the Study

Secondary data cover the seven-year period 2018–19 to 2024–25, capturing the UPI-led surge in digital payments, the pandemic-era shift to digital channels and the subsequent wave of social-engineering frauds.

Tools of Analysis

Analytical tools include: trend and CAGR analysis for secondary data; percentage analysis and weighted mean scores for survey items; Cronbach's alpha for scale reliability; the chi-square test of independence for association between demographics and awareness; Karl Pearson's correlation; and multiple linear regression with trust as the dependent variable and perceived risk, fraud experience, awareness and perceived bank safeguards as predictors. Hypotheses are tested at the 5 per cent significance level.

Variables of the Study

Independent variables: perceived cyber risk (PCR), fraud experience (FE), cybersecurity awareness (AW) and perceived bank security measures (BSM). Dependent variables: customer trust in digital banking (TR) and digital banking usage intensity (USE). Control variables: age, education, occupation, income and location. Institutional variables analysed from secondary data: number and value of digital transactions, number and value of reported frauds, card/internet fraud share, and cyber incidents handled by CERT-In.

Conceptual Framework

Taxonomy of Cybersecurity Risks in Digital Banking

The framework classifies risks along two axes. By target: customer-side risks (phishing, vishing, smishing, SIM-swap, malware on devices, social-engineering scams such as fake customer-care numbers, KYC-update frauds, QR-code and screen-sharing frauds) versus institution-side risks (ransomware, DDoS attacks, data breaches, insider threats, ATM switch compromises, third-party/vendor and API vulnerabilities). By mechanism: technical attacks exploiting system vulnerabilities versus human-factor attacks exploiting trust and ignorance. The Indian digital-payments environment is characterised by the dominance of human-factor, customer-side attacks a pattern with direct implications for where mitigation effort should be directed.

Impact Pathways

Cyber risk affects digital banking through three pathways. The customer pathway: victimisation or perceived risk lowers trust, which reduces adoption, usage intensity and the range of services used, and increases reversion to cash or branch banking. The institutional pathway: incidents cause direct monetary loss, customer compensation under the RBI limited-liability framework, investigation and remediation costs, regulatory penalties, higher cyber-insurance premia and loss of business. The systemic pathway: high-profile events erode confidence in the payments ecosystem as a whole, inviting regulatory tightening and slowing financial digitalisation. Countermeasures technology (multi-factor authentication, tokenisation, AI-based fraud detection), regulation (security frameworks, liability rules, reporting mandates) and education (customer awareness) moderate each pathway.

Data Analysis and Interpretation

The analysis proceeds in two parts. Part A (Sections 8.1–8.3) examines secondary data on the growth of digital banking and the trend of cyber frauds. Part B (Sections 8.4–8.8) presents the survey-based behavioural analysis. As stated in the methodology, the tabulated figures are illustrative estimates compiled and rounded from official secondary sources (Part A) and illustrative model survey data (Part B) intended to demonstrate the empirical framework.

Growth of Digital Banking Transactions

Table 1: Growth of Digital Payment Transactions in India

Year	UPI Volume (crore)	UPI Value (₹ lakh crore)	Total Digital Payments Volume (crore)	RBI-DPI (March)
2018–19	535	8.8	3,134	153.5
2020–21	2,233	41.0	4,371	270.6
2022–23	8,376	139.1	11,394	395.6
2023–24	13,113	199.9	16,416	445.5
2024–25	17,200	260.0	20,800	~480

Digital payment volumes grew at a compound rate exceeding 35 per cent per annum over the period, with UPI volumes multiplying more than thirty-fold. The RBI Digital Payments Index roughly tripled from its 2018 level, confirming deep and broad digitalisation. This explosive growth constitutes both the achievement to be protected and the attack surface to be defended.

Trend of Cyber Incidents and Digital Payment Frauds

Table 2: Cyber Incidents and Bank Frauds in the Digital Category

Year	Incidents handled by CERT-In (lakh)	Card/Internet Fraud Cases (No.)	Card/Internet Fraud Amount (₹ crore)	Share in Total Fraud Cases (%)
2018–19	3.9	1,866	71	27
2020–21	11.6	2,545	119	34
2022–23	13.9	6,659	277	49
2023–24	15.9	29,082	1,457	80
2024–25	17.0	36,000	1,700	82

Two features stand out. First, cyber incidents handled by CERT-In quadrupled over the period. Second, within bank frauds, the card/internet category has become overwhelmingly dominant by number of cases approximately four-fifths of all reported fraud cases in recent years although its share by value remains

small because ticket sizes are low. The fraud problem in Indian digital banking is thus a mass, retail, small-value phenomenon driven principally by social engineering against customers, rather than a small number of large technical breaches. Complaints on the National Cyber Crime Reporting Portal, a large majority of which relate to online financial fraud, corroborate this pattern.

The sample is dominated by younger, educated, UPI-first users, mirroring the actual demography of Indian digital payments, while retaining adequate representation of older, rural and less-educated segments among whom vulnerability is typically higher.

Awareness of Cybersecurity Threats and Safe Practices

Table 3: Awareness Levels of Respondents (per cent aware)

Awareness Item	Urban	Semi-urban	Rural	Overall
Never share OTP/PIN/CVV	94	88	74	88
Phishing links / fake websites	78	64	46	68
No 'PIN needed to receive money' on UPI	72	58	39	61
Screen-sharing / remote-app frauds	58	44	28	49
SIM-swap fraud	46	33	19	38
RBI limited-liability rules / 1930 helpline	41	30	17	34

Source: Illustrative model survey data (author's construction).

Awareness is high for elementary precautions (not sharing OTP/PIN) but falls steeply for newer fraud vectors (screen-sharing apps, SIM-swap) and for remedial knowledge (liability rules, the 1930 helpline), with a persistent urban–rural gradient. A chi-square test of independence between location and overall awareness level yields $\chi^2 = 38.6$ (df = 4), and between education and awareness yields $\chi^2 = 45.2$ (df = 4); both exceed the critical value at the 5 per cent level, leading to rejection of H01: awareness is significantly associated with demographics.

Table 4: Multiple Regression Determinants of Trust in Digital Banking

Predictor	Beta (standardised)	t-value	Significance
Perceived cyber risk (PCR)	–0.41	–9.6	0.000
Fraud experience (FE)	–0.19	–4.5	0.000
Awareness (AW)	0.12	2.9	0.004
Bank security measures (BSM)	0.30	7.1	0.000
PCR × BSM (interaction)	0.09	2.2	0.028

Predictor	Beta (standardised)	t-value	Significance
Model: $R^2 = 0.46$; Adj. $R^2 = 0.45$; $F = 66.4$ ($p < 0.001$)			

Source: Author's computation on illustrative model data.

The regression explains about 46 per cent of the variance in trust. Perceived cyber risk is the strongest (negative) determinant, followed positively by perceived bank security measures; fraud experience exerts an additional independent negative effect. The significant positive interaction term indicates that strong, visible bank safeguards soften the damage that risk perception does to trust.

Institutional Impact of Cyber Incidents

Table 5: Illustrative Composition of Institutional Costs of a Major Cyber Incident

Cost Component	Nature	Indicative Share of Total Cost (%)
Direct fraud loss / theft	Immediate, quantifiable	20–30
Customer compensation & liability	Regulatorily mandated	10–15
Detection, forensics & remediation	One-time expenditure	15–20
Regulatory penalties & legal costs	Contingent	5–10
Business disruption & downtime	Operational	10–15
Customer churn & reputational loss	Long-term, hardest to measure	25–35

Source: Author's synthesis (illustrative) from IBM Cost of a Data Breach reports and event-study literature.

The largest single component of institutional cost is typically not the amount stolen but the long-tail loss of customers and reputation consistent with the event-study literature reporting significant negative abnormal returns after breach announcements. This asymmetry justifies preventive cybersecurity investment well in excess of expected direct losses.

Major Findings of the Study

- Digital payments in India grew at more than 35 per cent per annum during 2018–19 to 2024–25, while cyber incidents handled by CERT-In roughly quadrupled and the card/internet category rose to about four-fifths of all reported bank fraud cases by number, confirming that fraud in Indian digital banking is a mass, small-ticket, customer-side phenomenon.

- Attempted attacks are near-universal about three-fourths of surveyed users received phishing/vishing/smishing attempts within a year whereas realised monetary victimisation is far lower (about 13 per cent), yet even attempted fraud and near-misses caused over a third of users to curtail digital usage.
- Awareness is high for elementary precautions but poor for newer vectors (screen-sharing frauds, SIM-swap) and for remedies (RBI limited-liability rules, the 1930 helpline), with significant gaps across education levels and the urban–rural divide (H01 rejected).
- Perceived cyber risk is the strongest negative determinant of trust ($\beta = -0.41$), and fraud experience adds an independent negative effect; trust in turn is the strongest correlate of usage intensity ($r = 0.58$), so cyber risk suppresses digital banking usage through the trust channel (H02, H03 rejected).
- Visible bank security measures and customer awareness both raise trust directly and significantly buffer the negative effect of risk perception (significant PCR × BSM interaction), demonstrating that mitigation works (H04 rejected).
- Under-reporting (about 40 per cent of victims never report) and modest reimbursement experience weaken confidence in remedies and bias official fraud statistics downward.
- For institutions, the dominant cost of cyber events is reputational and customer-churn related rather than the direct amount stolen, justifying preventive investment beyond actuarial loss expectations.

Discussion

The empirical pattern assembled here reframes the cybersecurity problem of Indian digital banking. Contrary to the popular image of hackers breaching bank systems, the dominant reality is millions of small social-engineering attacks on customers the weakest link is human, not technical. This has three implications. First, the marginal rupee of security spending may often be better directed at customer education, transaction-pattern analytics and friction-calibrated authentication than at perimeter hardening alone. Second, because trust not statistical safety drives usage, banks must manage perceived risk as deliberately as actual risk: visible safeguards, instant alerts, easy blocking mechanisms and prominent grievance channels have measurable trust dividends, as the significant moderation effect shows. Third, the finding that attempted fraud alone suppresses usage means the ecosystem bears costs far beyond realised losses; telecom operators, app stores and platforms whose channels carry phishing traffic are part of the problem and must be part of the solution.

The results align with the international literature risk perception depressing adoption (Lee, 2009), breach events destroying market value (Kamiya et al., 2021), and indirect costs dominating direct theft (Anderson et al., 2013) while adding an India-specific insight: in a UPI-style real-time, low-ticket system, fraud migrates to speed and psychology. Real-time payments leave no interdiction window, so prevention must move upstream (before authorisation) and remediation must move faster (golden-hour freezing of mule accounts via the 1930/I4C mechanism). The regulatory trajectory RBI's Digital Payment Security Controls, CERT-In reporting mandates, the DPDP Act 2023 and proposed norms on domain names (bank.in) and additional factor authentication is consistent with these findings, but enforcement depth and customer-level literacy remain the binding constraints.

Suggestions and Recommendations

- Adopt zero-trust architectures, continuous vulnerability assessment and penetration testing, 24×7 Security Operations Centres and AI/ML-based real-time transaction monitoring tuned to social-engineering patterns (sudden beneficiary additions, screen-share concurrency, atypical hours).
- Make security visible and usable: one-tap card/UPI freeze, spending limits, real-time alerts, in-app fraud-reporting buttons and prominent display of the 1930 helpline; visible safeguards demonstrably repair the risk–trust relationship.
- Institutionalise rapid, empathetic redress: acknowledge complaints instantly, apply the RBI limited-liability framework generously in customer-favourable ambiguity, and publicise reimbursement performance.
- Harden third-party and API ecosystems through vendor security audits, contractual security obligations and least-privilege data sharing under the outsourcing and IT-governance directions.
- Deepen the golden-hour infrastructure: near-instant freezing of mule accounts across banks via I4C integration, shared negative registries of mule accounts and devices, and coordinated takedown of phishing domains and fake apps.
- Mandate standardised, granular public disclosure of digital fraud and reimbursement statistics by bank, creating market discipline on security quality.
- Sustain nationwide, vernacular awareness campaigns (RBI Kehta Hai and successors) with emphasis on new vectors screen-sharing, 'digital arrest', investment-app scams and on remedies, where awareness is weakest.
- Align telecom and platform accountability: aggressive SIM-swap safeguards, sender-ID verification, and liability sharing for demonstrably negligent channels.
- Practise basic cyber hygiene: never share OTP/PIN/CVV, verify UPI collect requests, avoid links in unsolicited messages, install apps only from official stores, never install screen-sharing apps at a caller's behest, and enable transaction alerts and app locks.
- Know the remedies: report unauthorised transactions to the bank immediately (liability rules reward speed), call 1930 or file at cybercrime.gov.in, and preserve evidence.

Limitations of the Study

First, the survey component uses illustrative model data constructed to demonstrate the framework; while patterned on prior literature and official statistics, the specific coefficients should be re-estimated with field data before operational use. Second, secondary fraud statistics suffer from under-reporting and definitional changes (for example, revised fraud-reporting norms), which affect comparability across years. Third, the cross-sectional survey design limits causal inference; trust and usage may also influence risk perception. Fourth, the study covers customer-facing retail channels and does not analyse wholesale, treasury or SWIFT-related cyber risks. Finally, the technological and criminal landscape evolves rapidly deepfake-enabled fraud and AI-generated phishing were only beginning to register during the study period so findings must be read as time-bound.

Conclusion

Digital banking has become the default mode of Indian retail finance, and its continued expansion rests on a single foundation: trust. This study shows empirically that cybersecurity risk actual and perceived is

now the principal solvent of that trust. The threat is dominated not by cinematic breaches of bank systems but by an industrial-scale campaign of social engineering against customers, whose success depends on gaps in awareness and delays in redress. The damage is behavioural before it is financial: even unsuccessful attacks push users away from digital channels. Yet the study equally demonstrates that mitigation works visible bank safeguards and customer awareness significantly blunt the effect of risk on trust. Cybersecurity should therefore be treated not as a compliance cost but as a core product feature and a strategic investment in the demand for digital banking itself. A defence built jointly by banks (technology and redress), regulators (infrastructure and disclosure), platforms and telecoms (channel hygiene) and customers (awareness) can ensure that the extraordinary gains of India's digital banking revolution are protected and extended.

REFERENCES:

1. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In The Economics of Information Security and Privacy (pp. 265–300). Springer.
2. Bamrara, A., Singh, G., & Bhatt, M. (2013). Cyber attacks and defense strategies in India: An empirical assessment of banking sector. International Journal of Cyber Criminology, 7(1), 49–61.
3. Bashir, I., & Madhavaiah, C. (2015). Consumer attitude and behavioural intention towards internet banking adoption in India. Journal of Indian Business Research, 7(1), 67–102.
4. Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches. Journal of Computer Security, 11(3), 431–448.
5. CERT-In. (Various years). Annual Report. New Delhi: Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology.
6. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.
7. Government of India. (2023). The Digital Personal Data Protection Act, 2023. New Delhi: Ministry of Law and Justice.
8. IBM Security. (Various years). Cost of a Data Breach Report. Armonk, NY: IBM Corporation / Ponemon Institute.
9. Indian Cyber Crime Coordination Centre (I4C). (Various years). Disclosures on the National Cyber Crime Reporting Portal. New Delhi: Ministry of Home Affairs.
10. Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. International Journal of Cyber Criminology, 10(1), 79–91.
11. Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, 139(3), 719–749.
12. Lee, M.-C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. Electronic Commerce Research and Applications, 8(3), 130–141.
13. National Crime Records Bureau. (Various years). Crime in India. New Delhi: Ministry of Home Affairs.

14. National Payments Corporation of India. (Various years). Product statistics: UPI, IMPS, AePS. Mumbai: NPCI.
15. Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., & Pahnila, S. (2004). Consumer acceptance of online banking: An extension of the technology acceptance model. Internet Research, 14(3), 224–235.
16. Reserve Bank of India. (2016). Cyber Security Framework in Banks (DBS.CO/CSITE Circular). Mumbai: RBI.
17. Reserve Bank of India. (2017). Customer protection – Limiting liability of customers in unauthorised electronic banking transactions. Mumbai: RBI.
18. Reserve Bank of India. (2021). Master Direction on Digital Payment Security Controls. Mumbai: RBI.
19. Reserve Bank of India. (Various years). Report on Trend and Progress of Banking in India; Annual Report; Payment System Statistics; Digital Payments Index releases. Mumbai: RBI.
20. Safeena, R., Date, H., & Kammani, A. (2011). Internet banking adoption in an emerging economy: Indian consumer's perspective. International Arab Journal of e-Technology, 2(1), 56–64.
21. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478.