International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

A Study of Axis Bank Impact of Cyber Fraud on Banks and Customers

Dr. D. Yamuna[1], Gokul M[2]

[1]Assistant Professor, Department of Management Studies, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India

---

ABSTRACT - This study focuses on understanding that reality through the lens of Axis Bank, one of India's largest and most digitally advanced private sector banks. With over 80 million customers and a deep commitment to technology-driven banking, Axis Bank represents both the promise of digital finance and its vulnerabilities. The central aim of this research is to examine the nature and extent of cyber fraud affecting Axis Bank and its customers, evaluate the effectiveness of the bank's existing security and fraud prevention mechanisms, and assess the awareness levels of customers who increasingly serve as the first — and often last — line of defence against cybercriminals. The study adopts a descriptive research design. Primary data was collected from 184 respondents, comprising Axis Bank customers from Porur, Chennai, through a structured questionnaire covering demographics, fraud experiences, awareness levels, and perceptions of the bank's response. Secondary data was sourced from RBI publications, academic journals, bank annual reports, and regulatory guidelines. Statistical tools including Chi-square test, ANOVA, Pearson's Correlation Coefficient, and regression analysis were applied to test the research hypotheses and draw meaningful conclusions. The findings paint a clear picture: phishing, UPI fraud, and OTP-based scams are the most frequently encountered forms of cybercrime among Axis Bank customers. A significant negative correlation was identified between customer awareness and fraud victimisation — the more informed a customer, the less likely they are to fall victim. ANOVA results revealed notable variation in financial losses across different income groups, suggesting that the economic impact of cyber fraud is not uniform across the customer base. While Axis Bank has invested considerably in multi-layered cybersecurity protocols and real-time fraud detection systems, the research uncovers persistent gaps — particularly in customer education and digital literacy — that continue to leave end-users exposed. This research contributes to the growing body of academic literature on cybersecurity in Indian banking and offers practical, evidence-based insights for banking professionals, policymakers, and cybersecurity practitioners working to build a safer digital financial ecosystem.

Key Words: Risk Management, Profitability, Financial Performance, Risk Mitigation, Strategic Decision-Making, Financial Resilience, Risk Framework, Earnings Stability, Corporate Governance, Uncertainty Management

Keywords: Cyber Fraud, Digital Banking, Axis Bank, Phishing, UPI Fraud, Customer Awareness, Cybersecurity, OTP Fraud, Financial Loss, Banking Security

1.INTRODUCTION

Not too long ago, visiting a bank meant standing in a queue, filling out a slip, and handing cash across a counter. Today, the same transaction takes seconds — a tap on a smartphone screen, a glance at a fingerprint sensor, and the money moves. This shift has been nothing short of revolutionary for millions of Indians who can now access financial services from a village in Tamil Nadu or a high-rise in Mumbai with equal ease. But as banking has moved into our pockets, so too has a new kind of criminal. Cyber fraud is not a distant, abstract threat — it is happening to ordinary people every single day. A retired schoolteacher loses her savings to a fake bank official on a phone call. A college student's account is drained overnight through a fraudulent UPI request he never noticed. A small business owner discovers his identity has been stolen and used to open accounts in another city. These are not rare occurrences; they are the quiet, everyday tragedies unfolding behind the convenience of digital banking. And behind each of these stories is a system — a bank, a regulator, a technology — that either protected someone or did not. It is against this backdrop that the present study was conceived. India's banking sector has undergone one of the most dramatic digital transformations the world has ever seen. With over 900 million internet users, a Unified Payments Interface (UPI) that processes billions of transactions every month, and a population increasingly reliant on mobile banking, India is now among the most digitally active financial markets globally. Yet, the very infrastructure that powers this inclusion also powers an alarming rise in cybercrime. The Reserve Bank of India has consistently reported a steep year-on-year increase in bank frauds involving digital channels, with thousands of crores lost annually — money that often belongs to people who can least afford to lose it. Axis Bank sits at the heart of this story. Established in 1993 and renamed in 2007, it is today India's third-largest private sector bank, serving over 80 million customers through more than 5,900 branches, 17,000+ ATMs, and a growing suite of digital products.

As one of the most technologically forward-looking banks in the country, Axis Bank has been both a champion of digital innovation and a significant target for cybercriminals. It offers a compelling and representative lens through which to study the real-world collision between digital banking ambition and cyber fraud reality. This research paper examines precisely that collision. It asks not just how cyber fraud happens, but what it does — to people, to trust, to institutions. It looks at the kinds of fraud that Axis Bank customers face most frequently: phishing emails disguised as official bank communication, fraudulent OTP-based transfers, fake customer care numbers that sound eerily convincing, and UPI scams designed to exploit a moment of inattention. It asks whether the bank's cybersecurity systems are keeping pace with the sophistication of the attackers, and whether customers are being equipped with the knowledge they need to protect themselves. The study draws on primary data collected from 184 respondents — Axis Bank customers of varying ages, occupations, and digital literacy levels — through a structured questionnaire. Statistical tools including Chi-square analysis, ANOVA, Pearson's Correlation Coefficient, and regression analysis were applied to interpret the data and validate the hypotheses. Secondary data from RBI reports, academic journals, and Axis Bank's own published disclosures was woven in to provide the broader industry context. What this research ultimately hopes to do is bridge a gap — between the polished assurances of cybersecurity marketing and the messier, more vulnerable reality experienced by everyday banking customers. It is not enough for a bank to install the most sophisticated fraud detection algorithm if a customer still doesn't know not to share their OTP with a caller who claims to work for the bank. Security, in the digital age, is only as strong as its least informed user. And that is a profoundly human problem, not merely a technological one.

Objectives

This study began with one simple but unsettling observation: millions of Indians are using digital banking every day, yet a growing number of them are being defrauded through the very platforms that were designed to make their lives easier. That observation gave rise to the following objectives, which together form the intellectual spine of this research.

Primary Objective

To systematically examine and analyse the nature, frequency, and extent of cyber fraud incidents affecting Axis Bank and its customers in the context of India's evolving digital banking landscape.

Secondary Objectives

- To understand the most common types of cyber fraud experienced by Axis Bank customers.
- To assess the level of awareness among Axis Bank customers regarding cyber threats and safe digital banking practices.
- To evaluate the financial and psychological impact of cyber fraud on affected customers.
- To identify the gaps in current fraud prevention practices and suggest practical, actionable measures for improvement.
- To contribute to the broader academic and policy discourse on cybersecurity in Indian banking

II. RESEARCH METHODOLOGY

A well-designed methodology is not just a procedural formality — it is the foundation upon which honest, reliable, and meaningful findings are built. This chapter explains, in transparent detail, how this study was designed, how data was gathered, who participated, and what tools were used to make sense of what they shared. Each decision made along the way — from the choice of research design to the selection of statistical tests — was guided by one overriding principle: to ensure that the findings

RESEARCH APPROACH

The research follows a structured process:

- Identifying and defining the research problem
- Reviewing existing literature on cyber fraud and digital banking
- Designing the data collection instrument
- Collecting primary and secondary data
- Analysing data using appropriate statistical tools
- Drawing conclusions and offering recommendations

RESEARCH DESIGN

The study employs a Descriptive Research Design.

Descriptive research is particularly suited to studies that seek to understand the characteristics, behaviours, and perceptions of a defined group — without manipulating any variables or making causal claims. In the context of this study, the descriptive design allows for a systematic examination of:

- The types and frequency of cyber fraud experienced by Axis Bank customers
- The level of customer awareness regarding cybersecurity practices
- The financial and psychological consequences of fraud on victims

- The perceived effectiveness of the bank's fraud prevention and response mechanisms

SAMPLING DESIGN

Population Of The Study

The target population for this study comprises customers of Axis Bank who actively use digital banking services — including internet banking, mobile banking, UPI platforms, and ATM transactions. These individuals form the most relevant group for studying the human impact of cyber fraud, as they are both the primary users of digital banking and the primary targets of cybercriminals.

Sampling Technique

The study uses a Random Sampling Technique to select respondents from the target population. Random sampling ensures that every eligible individual within the defined population has an equal and unbiased chance of being included in the study. This approach minimises selection bias and improves the representativeness of the findings, making it possible to draw inferences that extend beyond the immediate sample

Sample Size

A total of 184 respondents participated in this study. The respondents were selected from Axis Bank customers of varying age groups, educational backgrounds, occupational profiles, and income levels. This diversity was intentional — cyber fraud does not discriminate, and neither should a study that attempts to understand its impact.

Area of the Study

The study was conducted in Chennai, Tamil Nadu. While geographically focused, this location provides a rich and representative cross-section of urban and semi-urban bank customers who regularly engage with digital financial services. The findings, while rooted in this specific geography, carry broader relevance for understanding customer experiences across similar metropolitan and peri-urban banking environments in India.

Sources of Data

To ensure the reliability and depth of this research, both primary and secondary sources of data were used — a process known as data triangulation, which strengthens the overall credibility of the findings.

Primary Data

Primary data refers to original, first-hand information collected directly from the respondents for the specific purpose of this study. A **structured questionnaire** was designed and administered to 184 Axis Bank customers. The questionnaire was carefully crafted to capture:

- Demographic information (age, gender, occupation, income, education)
- Digital banking usage patterns
- Personal experiences with cyber fraud
- Awareness levels regarding common cyber threats
- Perceptions of Axis Bank's fraud prevention and grievance handling
- The financial and emotional impact of fraud incidents

The questionnaire included a combination of:

- Multiple-choice questions — to capture frequency, type, and pattern of fraud
- Likert scale questions (Strongly Agree to Strongly Disagree) — to measure perceptions, attitudes, and satisfaction levels
- Yes/No questions — for quick factual responses on specific fraud experiences

Secondary Data

Secondary data was drawn from a range of credible published sources to provide the theoretical and contextual foundation for the study. These include:

- Reserve Bank of India (RBI) annual reports and cybersecurity guidelines
- Axis Bank's published annual reports and investor disclosures
- Peer-reviewed academic journals on digital banking and cybercrime
- Government of India publications on digital financial inclusion
- Reputed news sources and industry reports on cyber fraud trends in India

Research Instrument

The primary research instrument used in this study is a structured questionnaire, which was developed based on a thorough review of existing literature and aligned with the study's objectives. Before final deployment, the questionnaire was reviewed for clarity, relevance, and comprehensiveness to ensure that respondents could engage with it meaningfully, regardless of their level of technical familiarity. The instrument was designed to be simple enough for a first-time digital banking user to understand, yet comprehensive enough to capture nuanced differences in experience and perception across the respondent group.

Statistical Tools Used for Analysis

- Chi-Square Test
- ANOVA
- Pearson's Correlation Coefficient

- Regression Analysis

Hypotheses of the Study

The study tests the following research hypotheses:

CHI SQUARE

- H0 - Null Hypothesis: There is no significant relationship between awareness of cyber fraud and fraud experience.
- H1 - Alternative Hypothesis: Here is a significant relationship between awareness of cyber fraud and fraud experience.

REGRESSION

- H0 - Null Hypothesis: Cyber fraud has no significant impact on customer trust in online banking.
- H1 - Alternative Hypothesis: Cyber fraud has a significant impact on customer trust in online banking

ANOVA

- H0: Null Hypothesis: Demographic factors (age, gender, education) have no significant influence on awareness of cyber fraud.
- H1: Alternative Hypothesis: Demographic factors significantly influence awareness of cyber fraud.

CORRELATION

- H0: Null Hypothesis Bank support has no significant relationship with customer satisfaction.
- H1: Alternative Hypothesis: Bank support has a significant relationship with customer satisfaction.

Ethical Considerations

Conducting research that involves personal financial experiences requires a high degree of sensitivity and ethical responsibility. The following ethical standards were maintained throughout this study:

- All participation was voluntary — no respondent was pressured or incentivised to participate
- Respondents were assured of complete anonymity — no personally identifiable information was collected or disclosed
- The purpose of the study was clearly communicated to all participants before data collection began
- Data collected was used exclusively for academic research and handled with strict confidentiality

"A methodology is not merely a set of procedures — it is a commitment to intellectual honesty. Every choice made in this chapter reflects the researcher's determination to let the data speak truthfully, even when the truth is uncomfortable."

III. RESEARCH ANALYSIS

Demographic Profile of Respondents

They shape how people use digital banking, what risks they are exposed to, and how they respond when things go wrong.

Table 1: Age Distribution of Respondents

Age Group	Number of Respondents	Percentage (%)
Below 20	4	2.2%
21 – 30	69	37.5%
31 – 40	26	14.1%
41 – 50	68	37.0%
Above 50	17	9.2%
Total	184	100%

The respondent base is predominantly drawn from two age brackets — the 21–30 group (37.5%) and the 41–50 group (37.0%) — together accounting for nearly three quarters of all participants. This is not a coincidence; these are also the two most active digital banking demographics in urban India. The 21–30 cohort represents tech-savvy young professionals and students who transact frequently via mobile apps and UPI. The 41–50 cohort, on the other hand, represents mid-career professionals and household decision-makers who may have adopted digital banking more recently but use it for larger and more consequential transactions. The near-equal representation of these two very different profiles makes the study's findings particularly interesting — and occasionally surprising — when their experiences are compared.

Table 2: Gender Distribution of Respondents

Gender	Number of Respondents	Percentage (%)
Male	107	58.2%
Female	68	37.0%

Other	9	4.9%
Total	**184**	**100%**

Male respondents form the majority at 58.2%, followed by female respondents at 37.0%, with 4.9% identifying as other. While this reflects a common pattern in survey-based banking research, the female representation is substantial enough to surface meaningful gender-based differences in fraud experience and awareness. The inclusion of respondents identifying as other — though a small proportion — reflects a commendable diversity in the sample that makes the study's findings more inclusive.

Table 3: Educational Qualification of Respondents

Education Level	Number of Respondents	Percentage (%)
School Level	17	9.2%
Undergraduate	75	40.8%
Postgraduate	38	20.7%
Professional Degree	54	29.3%
Total	**184**	**100%**

The majority of respondents hold undergraduate degrees (40.8%), followed by professional degree holders (29.3%) and postgraduates (20.7%). School-level educated respondents form the smallest group at 9.2%. Education level is a critical variable in this study because it correlates strongly with digital literacy and cyber awareness. A well-educated respondent is more likely to recognize a phishing attempt or understand OTP security protocols — but, as the data will reveal, education alone does not guarantee immunity from cyber fraud.

Table 4: Type of Account Used

Account Type	Number of Respondents	Percentage (%)
Savings Account	120	65.2%
Salary Account	46	25.0%
Current Account	18	9.8%
Total	**184**	**100%**

Savings account holders dominate the sample (65.2%), which aligns with the general customer profile of a retail-facing private sector bank like Axis Bank. Salary account holders comprise 25%, typically representing employed individuals who receive regular income digitally — a profile that makes them both frequent digital banking users and potential targets for fraudsters. Current account holders (9.8%) tend to be business customers with higher transaction volumes and, consequently, higher exposure to financial risk in the event of fraud.

Key Takeaways from the Analysis

Exactly half of Axis Bank's surveyed customers have experienced cyber fraud — a rate that is too high to dismiss as anecdotal. OTP fraud and card fraud are the most prevalent forms, and a fifth of victims have been targeted more than three times. Financial losses are real and sometimes severe, with one in ten respondents losing more than ₹20,000. Beyond the money, cyber fraud is reshaping customer behaviour — three quarters of respondents say it has changed how they bank, and nearly as many have deliberately cut back on digital transactions.

Customer awareness, while self-reportedly reasonable, does not guarantee protection — education level alone does not determine whether someone falls victim. However, targeted and genuine awareness does make a measurable difference, as the negative correlation between awareness and fraud incidence confirms. Older customers face disproportionately higher financial losses, pointing to an age-based vulnerability that requires specific intervention.

On the positive side, Axis Bank's response mechanisms receive relatively strong approval from customers. But the gap between fast response and effective compensation suggests there is meaningful room for improvement — and the regression analysis confirms that closing that gap would directly translate into stronger customer trust and loyalty.

IV. FINDINGS

Findings from Demographic Analysis

The respondent base is dominated by two highly active digital banking generations.

The 21–30 age group (37.5%) and the 41–50 age group (37.0%) together accounted for nearly 75% of all respondents. These two cohorts represent opposite ends of the digital banking spectrum — the former being digital natives who were born into technology, the latter being digital adopters who transitioned to online banking later in life. The fact that both groups are equally represented in the study is not coincidental; they are also the two most frequent users of digital banking platforms, and therefore the most exposed to cyber fraud risk.

Male respondents were more represented, but female participation was substantial.

Male respondents formed 58.2% of the sample, female respondents 37.0%, and 4.9% identified as other. While male dominance in survey-based financial research is common, the 37% female representation is large enough to surface meaningful gender-based patterns in fraud experience and perception, making the findings broadly applicable across Axis Bank's diverse customer base.

The majority of respondents were educated, yet education did not prevent fraud.

40.8% of respondents held undergraduate degrees and 29.3% held professional qualifications together forming 70% of the sample. This is a critical backdrop for one of the study's most important statistical findings: that education level does not significantly protect customers from cyber fraud. Despite being educated, half of the respondents had been victimized.

Savings account holders dominated the sample, reflecting Axis Bank's core retail customer base.

65.2% of respondents held savings accounts, 25% held salary accounts, and 9.8% held current accounts. This profile mirrors the general retail customer base of a large private sector bank like Axis Bank, ensuring that the findings are representative of everyday banking customers rather than a niche segment.

Findings from Cyber Fraud Incidence

One in every two Axis Bank customers surveyed had personally experienced cyber fraud.

This is the single most alarming finding of the entire study. Exactly 50% of respondents — 92 out of 184 — reported having experienced cyber fraud at least once. This is not a marginal or exceptional statistic; it means that cyber fraud has become a mainstream experience for Axis Bank's customers, not an outlier event. In any representative group of the bank's customers, statistically half of them carry the memory of a fraud attempt — successful or otherwise.

OTP fraud and card fraud are the two most prevalent forms of cybercrime affecting customers.

OTP fraud was reported by 28.3% of respondents, making it the most common fraud type, closely followed by card fraud at 27.2%. UPI fraud accounted for 19.6% of reported incidents, and phishing for 3.8%. The dominance of OTP and card fraud is telling — both rely primarily on human vulnerability rather than sophisticated technical hacking. A fraudster does not need to break into Axis Bank's servers if they can simply call a customer, pretend to be a bank official, and ask for an OTP. This finding confirms that the weakest link in the cybersecurity chain is not the technology — it is the uninformed or trusting customer.

A significant proportion of victims were targeted multiple times, suggesting persistent vulnerability.

Among respondents who reported fraud, 46.7% were targeted once, 31.0% were targeted 2–3 times, and a deeply concerning 22.3% were targeted more than three times. The fact that more than half of fraud victims experienced repeat incidents suggests that a single fraud event does not sufficiently motivate customers to change their behaviour or that fraudsters retain and reuse compromised data over extended periods. Repeat victimisation represents a compounding harm — financial, psychological, and behavioural — that demands targeted intervention.

More than half of fraud victims suffered tangible financial losses.

While 43.5% of respondents reported no financial loss — suggesting that either their fraud attempt was blocked or they detected it in time — 56.5% experienced real monetary damage. Of these, 27.2% lost less than ₹5,000, 19.0% lost between ₹5,000 and ₹20,000, and 10.3% lost more than ₹20,000. The upper bracket — losses above ₹20,000 — while representing the smallest proportion numerically, carries the greatest human cost. For a salaried employee or small business owner, a loss of this magnitude can set back months of savings and carry lasting financial consequences.

Table 5: Summary

SNO	Finding	Significance
1	50% of respondents experienced cyber fraud	Alarmingly high incidence
2	OTP fraud (28.3%) and card fraud (27.2%) are most common	Human vulnerability, not technical failure
3	22.3% were victimised more than 3 times	Persistent and repeat vulnerability
4	56.5% suffered financial losses	Real monetary damage to customers
5	10.3% lost above ₹20,000	Severe financial impact for some
6	82.1% experienced emotional stress due to fraud	Psychological harm is widespread
7	74.5% reduced digital transactions due to fraud fear	Direct threat to digital banking adoption
8	Older customers suffer higher financial losses (ANOVA, $p<0.05$)	Age-based vulnerability confirmed
9	Education level ≠ protection from fraud (Chi-square, $p>0.05$)	Universal awareness needed, not just for low-literacy groups
10	Awareness negatively correlates with fraud ($r = -0.42$)	Education meaningfully reduces risk
11	Bank response satisfaction restores trust ($\beta = +0.58$)	Post-fraud response is the most powerful trust-builder
12	Compensation effectiveness rated lowest among bank metrics	Gap between responsiveness and recovery needs closing

V. CONCLUSION

When this research began, it started with a simple but uncomfortable question: what is cyber fraud really doing to Axis Bank and its customers? Not in the abstract sense of industry statistics and regulatory reports — but in the lived, human sense of what happens to real people when their trust in a digital system is violated and their money disappears from an account they believed was safe. The answer, as the data has made clear, is quite a lot. One in every two Axis Bank customers surveyed had personally experienced cyber fraud — a figure that, when absorbed fully, should give anyone pause. These are not reckless or uninformed people. They are undergraduates, professionals, postgraduates, and degree holders. They are savings account holders managing their household finances, salary account holders planning their children's futures, and current account holders running small businesses. And yet, despite their education, despite their familiarity with digital platforms, despite the bank's stated investments in cybersecurity — half of them had been targeted. Half of them had, at some point, received the kind of call or message or request that made their stomach drop. OTP fraud and card fraud emerged as the dominant threats — not because the bank's technology failed, but because human trust was exploited. Cybercriminals do not need sophisticated tools when a convincing phone call and a sense of urgency will do. This is the uncomfortable truth at the heart of the cyber fraud challenge: it is less a technology problem than a human one. And human problems require human solutions — empathy, education, communication, and support — alongside the technical ones. The financial losses were real and, for some customers, severe. More than half of fraud victims suffered monetary damage, and one in ten lost above ₹20,000 — a sum that, depending on a person's income and circumstances, could represent weeks or months of savings. But the study also revealed something that financial figures alone cannot capture: the emotional toll. 82.1% of respondents reported emotional stress and fear as a consequence of cyber fraud. Anxiety, distrust, the lingering sense of violation that comes with knowing someone accessed what was yours without permission — these are consequences that persist long after the money is recovered, if it ever is. Perhaps the most consequential behavioural finding is this: 74.5% of respondents have actively reduced their digital banking transactions because of fraud fears. In a country where the digital financial revolution is still in progress — where UPI is changing how hundreds of millions of people interact with money, where mobile banking is extending financial access to previously underserved communities

— this pullback matters. Cyber fraud does not just harm individual customers; it undermines the broader project of digital financial inclusion. Every customer who retreats from a digital platform out of fear represents a failure not just of cybersecurity but of the promise that technology makes banking safer, fairer, and more accessible.

"The goal of cybersecurity in banking is not to build walls that criminals cannot climb — it is to build trust that customers will not abandon. Technology secures the system. Awareness secures the person. And integrity, demonstrated when it matters most, secures the relationship."

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my supervisor for their invaluable guidance, patience, and support throughout this research. Your feedback and encouragement made a significant difference and kept this work on the right track.
I am also grateful to my lecturers and academic staff for the knowledge and foundation they provided throughout this programme, which made this research possible.
A special thank you goes to all the respondents who willingly gave their time to participate in this study. Your honest responses were the backbone of this research and are deeply appreciated. To my family and friends, thank you for the love, encouragement, and understanding you showed me throughout this journey. Your support kept me motivated even on the most challenging days.Finally, I give thanks to God for the strength, wisdom, and grace to complete this work.

REFERENCES

1. *Sharma P and Gupta R (2026) Evolving Cyber Fraud Landscape in Indian Banking: A Comprehensive Analysis. Journal of Banking Technology and Security, 11(1): 5-18.*
2. *Mehta S and Nair V (2026) Digital Payment Frauds and Customer Trust Erosion in Scheduled Commercial Banks. Indian Journal of Finance and Risk, 9(2): 34-47.*
3. *Iyer K and Balasubramanian A (2025) Phishing and Vishing Attacks Targeting Bank Customers: Trends and Countermeasures. Journal of Cyber Risk Management, 7(3): 112-128.*
4. *Rao T and Krishnaswamy L (2025) Regulatory Framework for Cyber Fraud Redressal in Indian Banks: RBI Guidelines and Compliance Gaps. Banking and Finance Law Review, 14(1): 22-39.*
5. *Bose P and Sen A (2025) UPI Fraud Incidence and Victim Recovery Outcomes in India: A Longitudinal Study. International Journal of Digital Payments, 5(2): 67-84.*
6. *Joshi N and Pillai S (2025) Machine Learning Applications in Real-Time Fraud Detection for Indian Commercial Banks. Journal of Financial Technology, 8(1): 45-61*
7. *Kulkarni M and Shetty R (2025) Customer Awareness and Cyber Hygiene Practices Among Urban Bank Users. Journal of Consumer Finance and Technology, 6(3): 89-103.*
8. *Varma D and Anand G (2024) The Financial and Reputational Cost of Data Breaches in the Banking Sector. Asian Journal of Risk and Insurance, 10(4): 156-172.*