International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

A STUDY ON FACTORS INFLUENCING BANKING FRAUDS IN FINANCIAL SYSTEM

Girish Muthu. V
MBA Student (USN: 24MBAR0514), Faculty of Management Studies, CMS Business School, JAIN (Deemed-to-be University), Bangalore.
Dr. Anoop Jagetia
Professor, Faculty of Management Studies, CMS Business School, JAIN (Deemed-to-be University), Bangalore.

ABSTRACT

Banking fraud has emerged as a major threat to the stability, credibility, and operational efficiency of the financial system, particularly with the rapid expansion of digital banking channels. This study examines the factors influencing banking fraud in the financial system by focusing on three major determinants: internal control weakness, employee pressure and rationalization, and technological/cyber vulnerability. The study adopted a quantitative, descriptive-cum-explanatory research design and collected primary data through a structured questionnaire administered to bank employees. A total of 155 usable responses were analyzed using descriptive statistics, Cronbach's alpha, exploratory factor analysis, Pearson correlation, and multiple regression analysis. The findings revealed that respondents perceived banking fraud risk, internal control weakness, employee pressure, and technological vulnerability at a moderate level. However, the reliability and validity results showed that the measurement scales lacked internal consistency, and the factor structure was not adequately supported. Further, correlation and regression results indicated that none of the three independent variables had a statistically significant positive effect on banking fraud occurrence in the present sample. Therefore, the hypotheses were not supported. The study concludes that while banking fraud is recognized as a continuing organizational risk, the current instrument requires refinement for stronger empirical validation. The research highlights the need for better questionnaire design, stronger fraud-risk assessment frameworks, and an integrated managerial approach combining process controls, ethical culture, and digital resilience.

Keywords: Banking Fraud, Internal Control Weakness, Employee Pressure and Rationalization, Technological/Cyber Vulnerability, Financial System

1. INTRODUCTION

Banking fraud is one of the most critical and current challenges to the activities of the contemporary financial system. Its broad definition includes any deliberate act of defrauding, concealing, manipulating, or misusing institutional practices to receive illegal financial rewards, whether through insiders or outsiders, or through a case of colluding insiders and outsiders. It is not merely a personal financial loss — banking fraud compromises the reputation of institutions, the trustworthiness of depositors, distorts operational efficiency, overburdens the regulatory

system, and in the worst-case situation, makes the system unstable. Trust is a fundamental commodity in an economic arena, and fraud erodes it at the very core of banking relationships.

The conventional banking environment would tend to associate fraudulent practices with counterfeit documents, unauthorized withdrawals, falsified papers, forged records, embezzlement, and fraudulent intra-account deals. Modern banking, however, has been fully digitized and mobilized — real-time asset settlements, online transfers, application programming interfaces, remote onboarding, and integrated data systems are now prevalent. This has transformed the nature and speed of fraud. Phishing and online impersonation, identity theft, credit card fraud, mule accounts, social engineering, manipulation of online banking, insider-assisted control overrides, and abuse of online vulnerabilities represent the modern face of banking fraud.

The Indian banking scenario is particularly relevant to this study. Over the past decade, India has witnessed a spurt in digital payments, online banking, and mobile banking. While these developments have brought massive benefits in speed, accessibility, and financial inclusion, they have simultaneously expanded the opportunities for fraud. As more transactions shift to the digital sphere, threats of phishing, impersonation, fraudulent access, and manipulation of customer credentials have grown correspondingly. The Reserve Bank of India's revised Master Directions on Fraud Risk Management (2024) underscore that control override, reporting discipline, technology-enabled fraud, and operational negligence are the foremost regulatory priorities in India.

The research problem of this study is founded on a growing mismatch between the sophistication of current banking practices and the effectiveness of anti-fraud models. While banks now operate across physical, digital, third-party, API-enabled ecosystems, the theoretical literature on fraud is often fragmented — treating internal control failures, behavioral drivers, and cyber risk in isolation. The present study attempts to bridge this gap by constructing a parsimonious integrated model that tests the joint impact of internal control weakness, employee pressure and rationalization, and technological/cyber vulnerability on banking fraud in the Indian context.

1.1 Statement of the Research Problem

There is no consolidated empirical evidence on the combined impact of internal control weakness, employee pressure and rationalization, and technological/cyber vulnerability on the incidence of banking fraud in the financial system. The current study addresses this by operationalizing these constructs through a structured closed-ended questionnaire and establishing the relationship between them using appropriate statistical instruments.

1.2 Research Objectives

(i) To study the impact of internal control weakness on the occurrence of banking fraud in the financial system.

(ii) To examine the impact of employee pressure and rationalization on the incidence of banking fraud in the financial system.

(iii) To measure the impact of technological/cyber vulnerability on the presence of banking fraud in the financial system.

1.3 Research Hypotheses

H1: There is a positive significant impact of internal control weakness on the occurrence of banking fraud in the financial system.

H2: There is a strong positive impact of employee pressure and rationalization on the occurrence of banking fraud in the financial system.

H3: Technological/cyber vulnerability affects the occurrence of banking fraud in the financial system positively and significantly.

2. LITERATURE REVIEW

- Akinbowale et al. (2023) examined the integration of forensic accounting and big-data technology frameworks for internal fraud mitigation in the banking industry. They proposed a workable model where machine learning and analytical tools detect suspicious trends that conventional monitoring fails to identify, justifying technological and cyber vulnerability as an important explanatory variable in banking fraud.
- The Association of Certified Fraud Examiners (2024) report on occupational fraud is one of the most powerful empirical reference points. It indicates that over half of all fraud is attributable to internal controls not being in place or being overridden, while tips remain the most common detection method. This supports internal control weakness as a significant independent variable in explaining banking fraud.
- Basel Committee on Banking Supervision (2011) classifies fraud under operational risk emanating from failed processes, people, systems, or external events, underscoring the importance of governance, internal controls, and risk culture. Basel Committee (2023) further demonstrates that digitalization allows criminals to commit fraud at a larger scale and faster rate, creating an increasingly industrialized fraud ecosystem — directly endorsing technological and cyber vulnerability as a core explanatory variable.
- Kazemian et al. (2019) revealed that all four aspects of the fraud diamond — pressure, opportunity, rationalization, and capability — significantly influence employee misappropriation in Iranian banks, justifying both internal control weakness and employee pressure-rationalization as distinct explanatory domains. Kon et al. (2024), using PLS-SEM, found that pressure has both direct and indirect effects on the intention to commit fraud through rationalization and opportunity, substantiating the integration of employee pressure and rationalization into a single construct.
- Mangala and Soni (2022) demonstrated through a systematic literature review that banking fraud has developed beyond a single process misconduct to a larger risk area affected by governance, control quality, regulatory response, and technology. Reserve Bank of India (2024) further confirmed that internal control weakness, employee behavior, and technological vulnerability are contemporary regulatory priorities in India — not merely theoretical variables.
- Suh et al. (2018, 2019) established that anti-fraud investment reduces fraud indirectly by reinforcing ethical culture and monitoring control, and that decreasing opportunities is

closely related to decreased fraud risk. Suh and Shim (2020) linked ethical corporate culture to the effectiveness of anti-fraud measures, connecting employee rationalization to organizational culture conditions — not merely individual characteristics.

2.1 Theoretical Underpinnings

The main theoretical foundation is the Fraud Triangle Theory (Cressey), explaining occupational misconduct in terms of pressure, opportunity, and rationalization. Internal control weakness constitutes the opportunity structure; employee pressure and rationalization constitute the motivational-cognitive pathway; and technological/cyber vulnerability represents the digital opportunity and systemic exposure. The Fraud Diamond Theory extends the triangle by adding capability — particularly relevant in banking where privileged system access, seniority, and procedural knowledge enable perpetrators to both commit and conceal fraud. Agency Theory further informs the framework: the information asymmetry and imperfect monitoring inherent in bank principal-agent relationships create conditions where fraud can flourish under weak controls. Lastly, the Operational Risk framework (Basel Committee) validates the classification of technological vulnerability as a structural precursor of banking fraud alongside process and people failures.

2.2 Research Gaps

1. Much of the banking fraud literature relies on secondary data. There is limited survey-based evidence capturing how bank employees perceive institutional vulnerabilities prior to large fraud losses.
2. Governance, behavioural drivers, and digital fraud are largely studied in isolation; integrated empirical models are scarce.
3. Empirical evidence is geographically concentrated in South Korea, Malaysia, Indonesia, Iran, and Nigeria; Indian banking-specific evidence — especially given revised RBI fraud directions and rapid digital growth — is underrepresented.
4. Results on fraud theory components are inconsistent, warranting retesting in new contexts with clearly operationalized constructs.

3. METHODOLOGY

The research design is quantitative, descriptive-cum-explanatory. It is descriptive in characterizing respondents and generalizing the extent of agreement on fraud-related items; it is explanatory in establishing whether the chosen independent variables significantly explain variation in banking fraud occurrence or exposure. The philosophical orientation is positivist and the approach is deductive, with hypotheses derived from existing fraud theory and prior research. The study is non-experimental and cross-sectional.

The population comprises commercial bank employees in India. Stratified convenience sampling was employed to ensure representation across cooperative, foreign, private, public sector, and small finance banks. Primary data were collected using a 5-point Likert scale structured questionnaire (1 = Strongly Disagree, 5 = Strongly Agree) with 31 items spanning four constructs: Internal Control Weakness (ICW, Q8-Q13), Employee Pressure and Rationalization (EPR, Q14-Q19), Technological/Cyber Vulnerability (TCV, Q20-Q25), and Banking Fraud

Occurrence/Exposure (BF, Q26-Q31R). A total of 155 usable responses were obtained, consistent with the recommended sample size of 150-200 for reliability analysis, exploratory factor analysis, and multiple regression.

3.1 Demographic Profile of Respondents

The sample was virtually gender-balanced (78 females, 50.3%; 77 males, 49.7%). The dominant age groups were 36-45 years (29.0%) and 25-35 years (27.1%), indicating a middle-career respondent pool. Education was dominated by professional qualifications (29.0%) and postgraduate degrees (27.7%). By bank type, cooperative banks (27.1%) and foreign banks (26.5%) had the highest shares, followed by private sector banks (21.3%). The most represented functional areas were IT/Digital Banking (19.4%), Risk Management (16.8%), and Compliance (16.1%) — respondents with practical exposure to fraud-control processes.

4. DATA ANALYSIS AND RESULTS

4.1 Descriptive Statistics

All four construct means were closely clustered around the center of the 5-point scale, indicating moderate perceived fraud risk across dimensions. This suggests respondents recognized fraud vulnerabilities without expressing extreme or convergent views, yielding a balanced descriptive baseline. Table 1 presents the construct-level descriptive statistics.

Table 1: Construct-Level Descriptive Statistics

Construct	Code	Mean	SD	Interpretation
Internal Control Weakness	ICW	2.945	0.511	Moderate
Employee Pressure & Rationalization	EPR	3.104	0.553	Moderate
Technological/Cyber Vulnerability	TCV	2.970	0.535	Moderate
Banking Fraud Occurrence/Exposure	BF	2.995	0.523	Moderate

4.2 Reliability Analysis (Cronbach's Alpha)

After reverse-coding Item 31, Cronbach's alpha values remained extremely low across all constructs (Table 2). These values fall far below the commonly accepted threshold of 0.70, indicating that items grouped under each construct did not cohere as internally consistent latent scales. Hypothesis testing on the basis of these constructs must therefore be regarded as exploratory rather than confirmatory.

Table 2: Reliability Summary

Construct	Items	Cronbach's Alpha	Assessment
ICW	Q8-Q13	0.082	Unacceptable
EPR	Q14-Q19	0.180	Unacceptable
TCV	Q20-Q25	0.191	Unacceptable
BF	Q26-Q31R	0.078	Unacceptable

4.3 Factor Adequacy and Exploratory Factor Analysis

The Kaiser-Meyer-Olkin (KMO) measure was 0.443, below the acceptable threshold of 0.50, and Bartlett's Test of Sphericity was non-significant (χ^2 = 278.131, df = 276, p = 0.453). These results indicate that the inter-item correlation matrix was insufficiently robust to support a stable factor solution (Table 3). The scree plot exhibited a flat pattern with no convincing elbow, confirming that the questionnaire items did not empirically cluster into the anticipated four constructs.

Table 3: Factor Adequacy Diagnostics

Metric	Value
KMO Overall	0.443
Bartlett Chi-Square	278.131
Bartlett df	276
Bartlett p-value	0.453
Interpretation	Factor analysis not supported: KMO < .50 and Bartlett not significant

4.4 Pearson Correlation Analysis

Pearson correlation coefficients between the three explanatory constructs and banking fraud occurrence were all very weak and statistically non-significant (Table 4). Internal Control Weakness showed a slight negative correlation with Banking Fraud (r = -0.083, p = 0.306); Employee Pressure and Rationalization was also negligibly negative (r = -0.079, p = 0.331); Technological/Cyber Vulnerability showed a small positive correlation (r = 0.081, p = 0.318). All coefficients are approximately zero, indicating no significant linear relationship between the predictors and the dependent construct, consistent with the poor reliability results.

Table 4: Pearson Correlation Coefficients

Variable	ICW	EPR	TCV	BF
ICW	1	0.047	0.071	-0.083
EPR	0.047	1	0.013	-0.079
TCV	0.071	0.013	1	0.081
BF	-0.083	-0.079	0.081	1

4.5 Multiple Regression Analysis

The regression model was not statistically significant overall: $F(3, 151) = 1.032$, $p = 0.380$, $R^2 = 0.020$, adjusted $R^2 = 0.001$ (Table 5). The three predictors collectively explain only 2.0% of the variance in banking fraud occurrence — effectively negligible. At the individual predictor level, Internal Control Weakness had $\beta = -0.085$ ($p = 0.292$), Employee Pressure and Rationalization had $\beta = -0.076$ ($p = 0.350$), and Technological/Cyber Vulnerability had $\beta = 0.088$ ($p = 0.279$) — none statistically significant (Table 6). The direction of two coefficients is contrary to the theoretically predicted positive effects.

Table 5: Model Summary and ANOVA

R	R Square	Adjusted R Square	Std. Error	F	p-value
0.142	0.020	0.001	0.523	1.032	0.380

Table 6: Regression Coefficients

Predictor	B	Std. Error	Beta (β)	t	Sig.
(Constant)	3.219	0.397	-	8.113	0.000
Internal Control Weakness (ICW)	-0.087	0.083	-0.085	-1.056	0.292
Employee Pressure & Rationalization (EPR)	-0.071	0.076	-0.076	-0.938	0.350
Technological/Cyber Vulnerability (TCV)	0.086	0.079	0.088	1.086	0.279

4.6 Hypothesis-Wise Decisions

None of the three hypotheses were supported in this dataset. Table 7 summarizes the hypothesis decisions based on both Pearson correlation and multiple regression results.

Table 7: Final Hypothesis Decisions

Hypothesis	Path	Pearson r	r p-value	Regression Beta	Reg. p-value	Decision
H1	ICW → BF	-0.083	0.306	-0.085	0.292	Not Supported
H2	EPR → BF	-0.079	0.331	-0.076	0.350	Not Supported
H3	TCV → BF	0.081	0.318	0.088	0.279	Not Supported

5. FINDINGS AND DISCUSSION

The descriptive findings reveal that banking fraud is viewed as a moderate but persistent organizational risk across all three dimensions studied. Employee Pressure and Rationalization recorded the highest mean (3.104), followed by Banking Fraud Occurrence (2.995), Technological/Cyber Vulnerability (2.970), and Internal Control Weakness (2.945). Practically, respondents appear to regard fraud as driven more by organizational climate — ethical culture, target pressure, normalization of minor violations — than by hard control failures or technology gaps alone.

The most decisive study outcome, however, is the measurement failure. Cronbach's alpha values (0.078 to 0.191) are far below psychometric acceptability for all four constructs, and the KMO statistic (0.443) and non-significant Bartlett test confirm that the inter-item structure does not support a clean four-factor solution. This means that correlation and regression findings are not interpretable as evidence for or against the theoretical hypotheses; they reflect measurement inadequacy rather than genuine null relationships.

The most justifiable conclusion is not that internal controls, employee pressure, and cyber vulnerability are unrelated to banking fraud — the descriptive evidence and the broader literature are clear that they are — but that the present questionnaire design is insufficient to capture these constructs as stable latent variables in this sample. The research contributes a significant diagnostic observation: the risk of banking fraud is perceived to exist at moderate levels, but the current instrument requires substantial refinement before causal inference is warranted.

These results are consistent with findings from Rahmawati and Rahmawati (2022), whose context-sensitive results showed that fraud determinants can vary substantially across banking settings. They are also consistent with the general observation from Sood and Bhushan (2020) that fraud scholarship is fragmented, and that integrated perceptual frameworks are difficult to operationalize without extensive pilot validation.

6. MANAGERIAL IMPLICATIONS

Despite the null inferential results, the descriptive findings carry direct managerial significance. First, regarding internal controls, the moderate concern with poor segregation of duties, insufficient monitoring, and control overrides by senior officials should serve as a practical warning to managers. Even where survey instruments fail to produce significant regression effects, these operational exposures can be materially significant in real-world banking practice.

Second, the strongest descriptive concern — poor ethical culture enabling fraudulent behavior — signals that anti-fraud governance must go beyond surveillance and punishment. Banks should invest in realistic performance goal-setting, equitable workload distribution, whistleblower protection, ethical leadership, and clear disciplinary standards. Rationalization thrives where minor procedural violations are treated as acceptable, and culture-management tools are therefore indispensable complements to structural controls.

Third, with respect to digital and cyber risk, authentication mechanisms, employee fraud awareness, patch discipline, incident response speed, and third-party vendor management all require continued investment. IT teams must not be left as the sole owners of digital fraud governance — integration with audit, operations, compliance, and customer-awareness functions is essential.

Finally, the poor psychometric outcomes themselves carry a managerial implication: banks that rely exclusively on informal perception surveys for fraud-risk assessment may fundamentally misread their own vulnerability profile. Fraud governance must be evidence-based — perceptual data should be complemented with incident reporting, control-testing outcomes, audit findings, loss-event databases, and digital alert records.

7. LIMITATIONS AND SCOPE FOR FUTURE RESEARCH

The principal limitation of this study is the measurement weakness across all four constructs. Cronbach's alpha values and factorability diagnostics indicate that items did not form coherent latent scales, limiting the interpretability of inferential results. Second, the cross-sectional design captures perceptions at a single point in time, precluding causal inference or observation of how fraud conditions evolve following regulatory, technological, or organizational changes. Third, the dependent variable is perceived fraud exposure rather than actual fraud incidence, limiting correspondence to verified loss events. Fourth, the sampling skew toward IT/digital banking, risk management, and compliance functions may not adequately represent frontline operations.

Future research should begin with rigorous scale refinement — expert validation, pilot testing with item analysis, and elimination of overlapping indicators — before re-administering the questionnaire. Confirmatory factor analysis and structural equation modelling should be employed on a refined instrument to test for direct effects, mediation (e.g., ethical culture mediating the pressure-fraud path), and moderation. Longitudinal designs would enable observation of fraud conditions following RBI guidelines, cyber incidents, or training interventions. Comparative analysis across bank types (public, private, cooperative, small finance, foreign) and functional roles would illuminate context-specific fraud determinants. Mixed-method designs combining surveys with audit observations, incident reports, and interviews would provide richer triangulation.

8. CONCLUSION

This study set out to investigate the impact of internal control weakness, employee pressure and rationalization, and technological/cyber vulnerability on banking fraud occurrence in the Indian financial system. While the theoretical framework and integrated model are well-grounded in the Fraud Triangle, Fraud Diamond, Agency Theory, and Operational Risk literature, the empirical results were limited by measurement inadequacy: all four constructs showed unacceptable reliability, factor structure was not supported, and none of the three hypotheses were statistically confirmed.

However, the study makes meaningful contributions. Descriptively, it reveals that bank employees perceive fraud risk as a moderate but persistent multi-dimensional challenge spanning processes, people, and technology. Diagnostically, it demonstrates that integrated fraud theory requires equally integrated measurement — that well-designed constructs, expert-validated items, and pilot-tested questionnaires are prerequisites for credible perceptual research on banking fraud. Managerially, it reinforces that fraud governance must combine process controls, ethical culture, and digital resilience rather than relying on any single intervention. Together, these contributions advance both the scholarship and the practice of banking fraud prevention in the Indian context.

REFERENCES

Akinbowale, O. E., Mashigo, P., & Zerihun, M. F. (2023). The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry. Cogent Business & Management, 10(1), 2163560.

Association of Certified Fraud Examiners. (2024). Occupational Fraud 2024: A Report to the Nations.

Basel Committee on Banking Supervision. (2011). Principles for the Sound Management of Operational Risk.

Basel Committee on Banking Supervision. (2023). Digital Fraud and Banking: Supervisory and Financial Stability Implications.

International Monetary Fund. (2024). Global Financial Stability Report, Chapter 3: Cyber Risk — A Growing Concern for Macrofinancial Stability.

Kamdjoug, J. R. K., et al. (2024). Data analytics-based auditing: A case study of fraud detection in the banking context. Annals of Operations Research, 340, 1161–1188.

Kazemian, S., Said, J., Hady Nia, E., & Vakilifard, H. (2019). Examining fraud risk factors on asset misappropriation: Evidence from the Iranian banking industry. Journal of Financial Crime, 26(2), 447–463.

Kon, Z. S., et al. (2024). The influence of pressure on intention to commit fraud: The mediating role of rationalization and opportunities. Asian Journal of Business Ethics, 13(1), 175–195.

Mangala, D., & Soni, L. (2022). A systematic literature review on frauds in banking sector. Journal of Financial Crime, 30(1), 285–301.

Mita, A. F., Setyaningrum, D., & Rosdini, D. (2025). Internal audit quality and fraud risk management. International Journal of Disclosure and Governance.

Rahmawati, M., & Rahmawati, I. D. (2022). Unveiling employee fraud in banking: Understanding the influential factors.

Reserve Bank of India. (2024). Master Directions on Fraud Risk Management in Commercial Banks and All India Financial Institutions.

Said, J., Mohamad, N., & Kazimean, S. (2018). Empirical findings of mitigating asset misappropriation among bank employees: Fraud diamond theory perspective. International Journal of Management and Applied Science, 4(8), 94–98.

Sood, P., & Bhushan, P. (2020). A structured review and theme analysis of financial frauds in the banking industry. Asian Journal of Business Ethics, 9(2), 305–321.

Suh, J. B., Nicolaides, R., & Trafford, R. (2019). The effects of reducing opportunity and fraud risk factors on the occurrence of occupational fraud in financial institutions. International Journal of Law, Crime and Justice, 56, 79–88.

Suh, J. B., Shim, H. S., & Button, M. (2018). Exploring the impact of organizational investment on occupational fraud: Mediating effects of ethical culture and monitoring control. International Journal of Law, Crime and Justice, 53, 46–55.

Suh, J. B., & Shim, H. S. (2020). The effect of ethical corporate culture on anti-fraud strategies in South Korean financial companies. International Journal of Law, Crime and Justice, 60, 100361.