NFSU JOURNAL OF FORENSIC ACCOUNTING & FRAUD INVESTIGATION

NJFAFI
Volume: 1, Issue: 2
December 2025
E-ISSN: 3107-4650

CORPORATE FRAUD IN FINANCE & RISK MANAGEMENT FORENSIC ACCOUNTING AND FRAUD DETECTION TECHNIQUES - MOVING FROM REACTIVE TO PREDICTIVE FRAUD DETECTION

Pankaj Kumar, Dr. Swati Srivastava, Prof. (Dr.) Surendra Roy, Prof. (Dr.) Sanjeev Kumar Bhalla

Research Scholar, School of Management, BBD University, Lucknow, India

Assistant Professor, School of Management, BBD University, Lucknow, India

Dean Academics, BBD University, Lucknow, India

Pranveer Singh Institute of Technology, Kanpur, India

Corresponding Author Mail id - capannkajkumar@bbdu.ac.in

Abstract

In India, corporate fraud is a serious concern. The RBI has registered a 28% rise in cases of bank fraud and a 159% increase in the amount of money siphoned off during 2019-20. The most common examples of scams include Satyam (2009) and Nirav Modi (2018). In both the cases, the scams were detected after it had happened. There is a dearth of literature on proactive fraud risk management in India. Objectives of the study: The present study is an attempt to discuss the various tools and techniques to detect accounting manipulation, deceit, and fraud in financial statements and its Cartesian geometry.

In addition, the study is an effort to explore the role of forensic accounting and analytics in corporate fraud risk management. The study proposes a predictive model for fraud detection, auditor decision making matrix, and early warning signals, customized to Indian corporate scenario.

The study uses mixed methods research approach. First, a quantitative study has been conducted to review 200 fraud cases (1991-2025) to find out the fraud patterns. Second, a qualitative study has been done by conducting interviews with 50 stakeholders, analyzing 116 Indian theses and 200 judicial orders (2017-2024) to identify the vulnerabilities and trends using thematic coding principles similar to NVivo qualitative analysis. Significance of the study: In the light of current and emerging developments such as AI-generated fraud, this study bridges the forensic gap to help India's financial systems to respond effectively. The study ensures data privacy and observes legal standards of conducting research.

Keywords: Corporate Frauds, Financial Shenanigans, Forensic Accounting, Forensic Auditing, Indian IB Code 2016, Digital Forensic Methods (DFM)

1. INTRODUCTION AND PROBLEM STATEMENT

1.1 Introduction

Fraud is now a structural risk to India's corporate ecosystem, posing a challenge to fundamental principles of market integrity, financial disclosure and investor trust. Misappropriation twists capital formation, risk pricing and eventually harms the efficiency of India's capital markets: SEBI has estimated that fraud-hit companies tend to trail sectoral indices by 34 per cent on a three-year average after a fraud is detected. India the world's fifth-biggest economy has had some recent big ticket financial frauds exposing flaws in early fraud detection **(Singh & Kaur, 2023)**. Notwithstanding having among the toughest possible regulations in the form of RBI regulations, Indian IB Code 2016, Indian CA 2013, SEBI regulations, and strict corporate governance norms, the quantum and frequency of corporate fraud

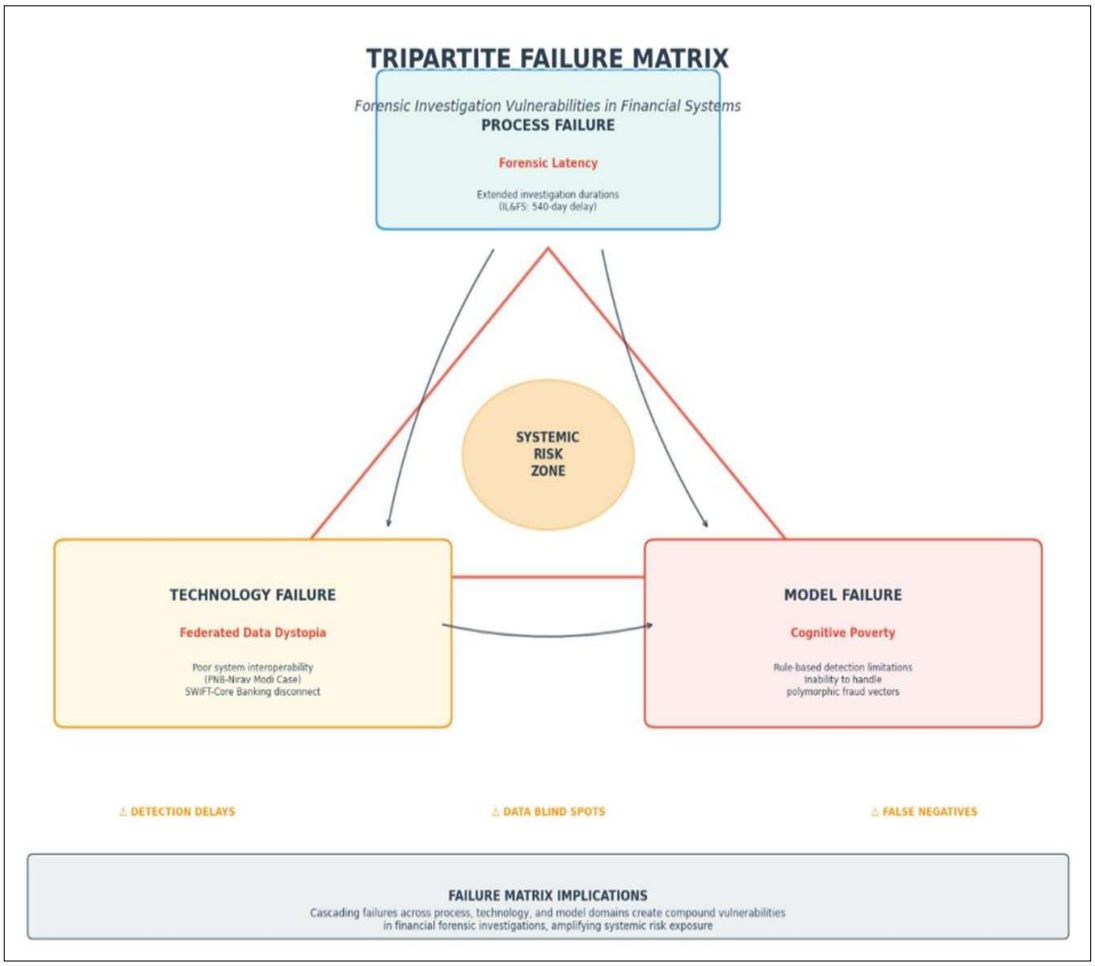
in India are increasing.

Judicial precedents from major financial scandals such as Satyam (2009), PNB-Nirav Modi (2018), Vijay Mallya (2012), the Fortis Healthcare case (2018), and IL&FS (2019) reveal systemic flaws in auditing practices, banking oversight, promoter accountability, and corporate governance. The legal deterrent effect on companies is insufficient by itself to stop a company from committing fraud and to stop fraud from occurring in the financial sector unless and until there are strong and better measures in place to enforce the law and hold companies' management more accountable. RBI states that the number of fraud cases reported to it surged by 28 percent and the "volume" of fraud (i.e., the amount of money involved) increased by a staggering 159 percent during 2019-20. These figures are from 2020, indicating no improvements since then.

Indian corporate history has seen some big scandals. Besides the more recent ones like the Satyam scam (2009), Kingfisher Airlines case (2012) and Nirav Modi fraud (2018), we have in the recent past alone witnessed a string of big scandals like: ***a)*** *Videocon loan default (2020)* ***b)*** *Aircel-Maxis controversy (2022)* ***c)*** *Yes Bank interconnected loan case (ongoing) All these highlight the existing loopholes in the Indian financial regulatory systems and cast serious doubts on public faith on the financial systems.*

The corporate frauds have resulted in huge financial losses and as per the RBI data, there has been a total of 3.2 lakh crore NPAs since 2014, because of corporate frauds. The RBI data clearly points to something rotten in the Indian financial regulatory systems. For quite some time now, it appears that the regulatory systems have failed to prevent and/or punish corporate frauds.

This paper puts forth a three-fold failure matrix which suggests that the current fraud detection mechanisms are facing significant challenges.



Tripartite Failure Matrix: Figure 1 (prepared by researcher)

Organizational failures in corporate fraud are attributed to the inadequacies of processes, technology, and fraud detection models. In the case of IL&FS, the delayed action on the complaints led to a sort of **forensic**

latency giving enough time for fraud to breed.

Similarly, in the PNB and Nirav Modi scam, the ineffective data integration and interoperability resulted in inadequate supervision. Model failures occur when rigid, rule-based detection systems cannot cope with polymorphic and evolving fraud patterns due to their limited cognitive capacity. This research highlights the disparity in oversight that has caused a new surge of financial cyber threats, with *malicious actors* using tactics outlined below.

Financial Cyber Threats: Figure 2 (prepared by researcher)

The three major loopholes being taken advantage of for committing corporate fraud are, (i) Control Environments, (ii) Legal and Regulatory frameworks and (iii) AI enabled Security Vulnerabilities. The quantum inventory spoofing (manipulating the inventory records of 17 Bhushan Steel warehouses) and jurisdictional routing of loans through 32 banking entities (Videocon), are classic examples of corporate fraud being committed exploiting the first two types of loopholes. A fraud of ₺820 crore in UCO Bank through IMPS exploiting the third type of loophole, including GAN based voice biometric spoofing attacks, has been reported very recently.

This study puts forth a futuristic financial security technology architecture highlighting the need for a technology overhaul to the current state-of-the-art fraud detection techniques to replace a reactive rule-based system with a proactive smart intelligent system using state-of-the-art technologies.

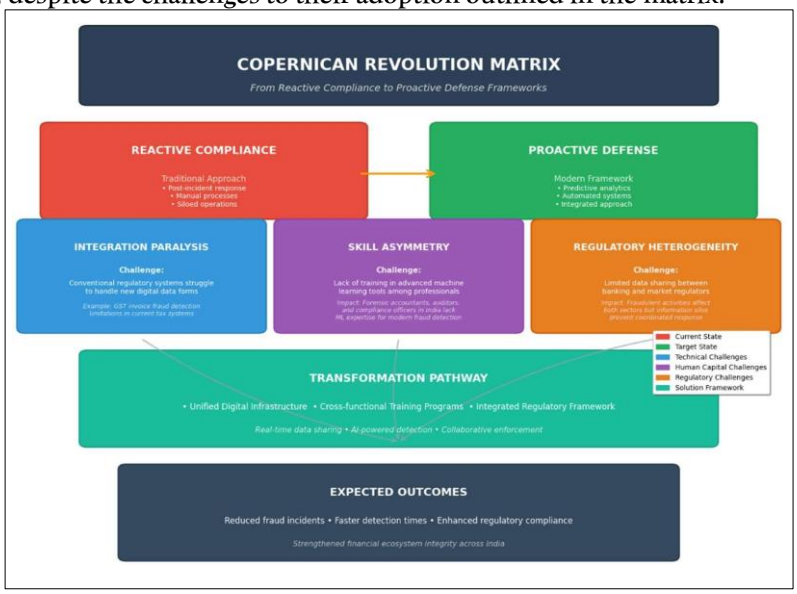
NFSU JOURNAL OF FORENSIC ACCOUNTING & FRAUD INVESTIGATION

NJFAFI
Volume: 1, Issue: 2
December 2025
E-ISSN: 3107-4650

Advances in Financial Security Technologies Matrix: Figure 3 (prepared by author)

Topological data analysis reveals relations and anomalies in complex, semi transparent networks of financial transactions. RL allows for real-time learning, prediction and intervention to block next gen attempts at fraud. Homomorphic encryption allows analysis of encrypted transaction data without revealing the content of the data. Quantum-resistant cryptographic log integrity uses post- quantum techniques to secure logs over time.

It is obvious what is the aim of the game. Indian finance needs to upgrade its mechanisms by incorporating more sophisticated and multi layered fraud detection techniques.
This research makes the case for a Copernican shift in the current financial oversight ecosystem, from a culture of compliance to a culture of defence, and how the ongoing digital transformation in India can facilitate this shift. It shows how certain technological innovations such as distributed ledger forensics, neural network based anomaly detection, and graph relation analysis can offer better fraud detection and fraud prevention, despite the challenges to their adoption outlined in the matrix.



NFSU JOURNAL OF FORENSIC ACCOUNTING & FRAUD INVESTIGATION

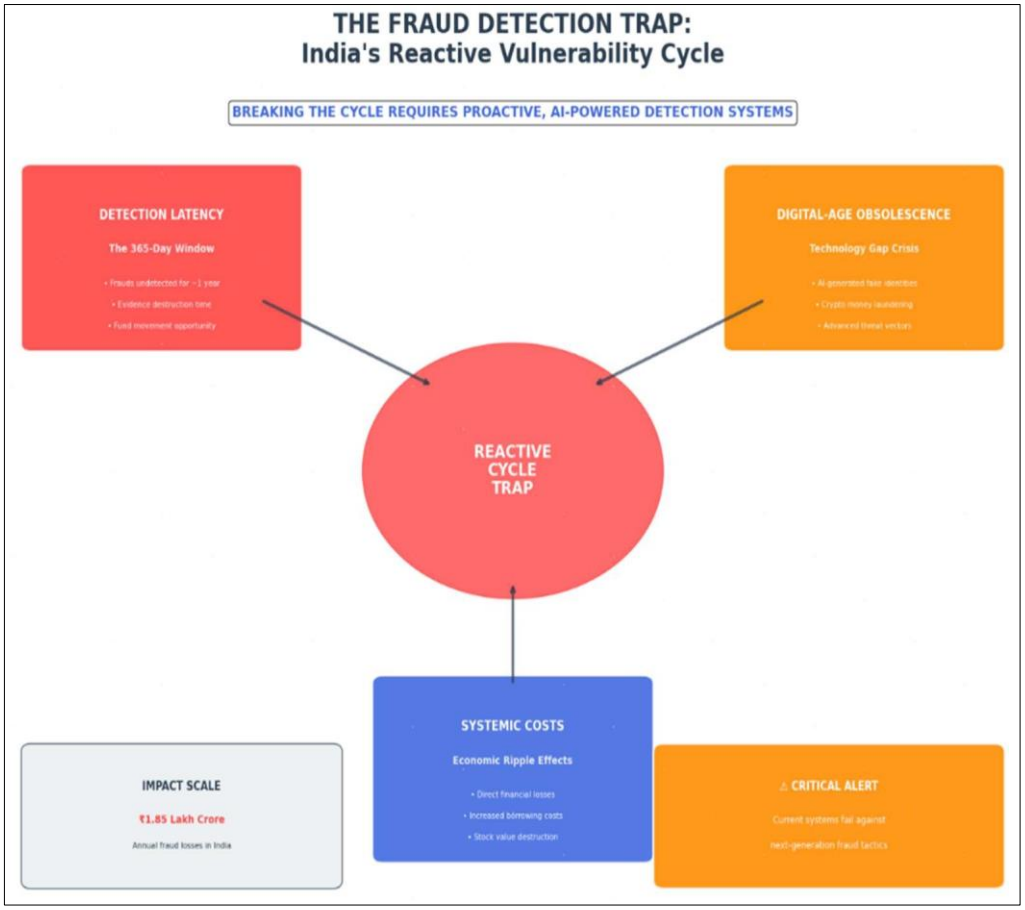
NJFAFI
Volume: 1, Issue: 2
December 2025
E-ISSN: 3107-4650

Copernican Revolution Matrix: 4 (prepared by researcher)

a) Integration Paralysis: Legacy systems not equipped to process newer types of digital data such as GST invoices. Recent cases of tax fraud have highlighted this. **b)** Skill Asymmetry: Forensic accountants in India not equipped with skills in advanced machine learning tools to catch modern financial crimes. c) Regulatory Heterogeneity: Banking and market regulators not sharing enough data despite frauds often being interconnected between the two. There is thus a felt need for more pro-active, integrated and technology enabled fraud detection and fraud prevention strategies.

1.2 Problem Statement

India's fraud detection approach, despite recent efforts in fraud monitoring and the advent of new technologies in fraud detection, is largely retrospective, investigation-driven and rule-based, the report said, highlighting a **fraud vulnerability cycle** in organisations that makes them vulnerable to new and complex frauds.

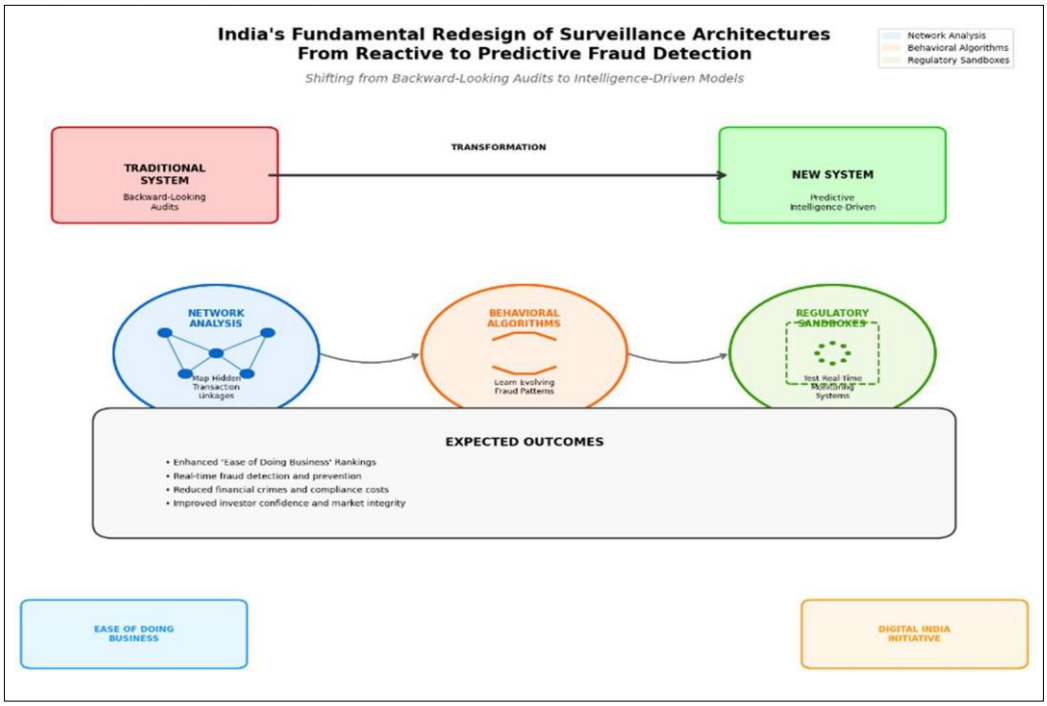


Indian's Vulnerability Cycle: Figure 5 (prepared by author)

"The late reporting of the fraud enables fraudster to commit fraud for several months, enables distribution of the money and destruction of fraud evidence. Inability of systems and processes to detect AI-generated identities and crypto-enabled money laundering are further challenges. This fraud detection time lag is eating away into the economy through lost value, higher interest rates, depressed stock market valuations and EoDB (Ease of Doing Business) ranking of India. There is a pressing need for large-scale reforms in fraud monitoring and detection," it said.

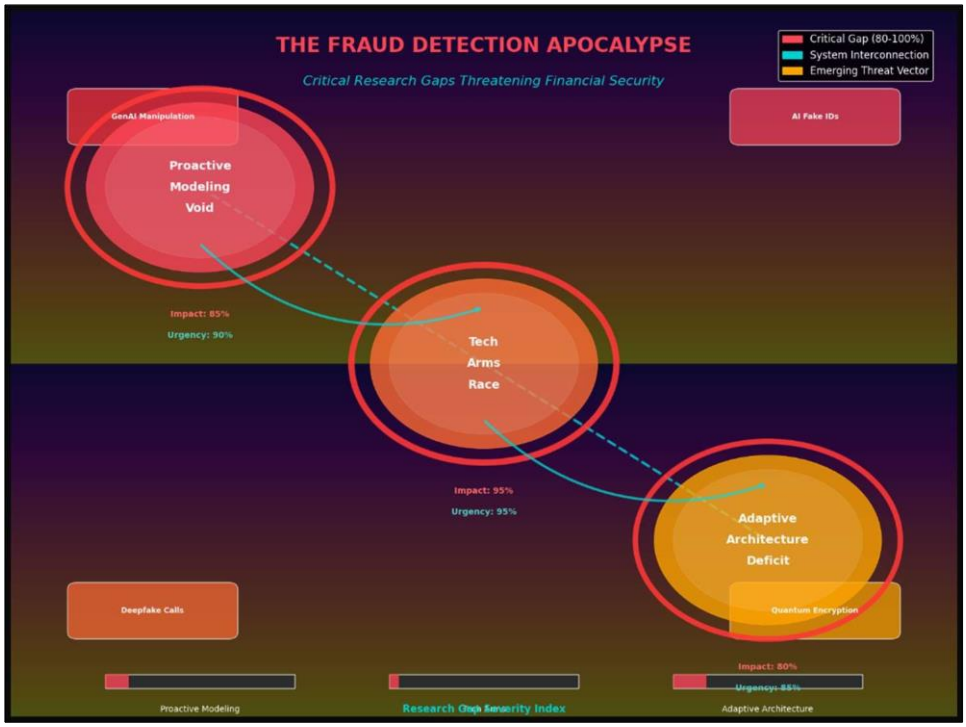
NFSU JOURNAL OF FORENSIC ACCOUNTING & FRAUD INVESTIGATION

NJFAFI
Volume: 1, Issue: 2
December 2025
E-ISSN: 3107-4650



Indian's Fundamental Redesign of Surveillance Architectures: Figure 6 (prepared by author)

The report also said that data analytics and network analysis can be used to detect collusive frauds and unusual patterns of transactions indicative of fraud risk. Behavioural analytics can identify the methods of fraud as fraudsters change their methods and techniques over time. In addition, sandboxes can be used to test the real-time monitoring systems before their implementation.

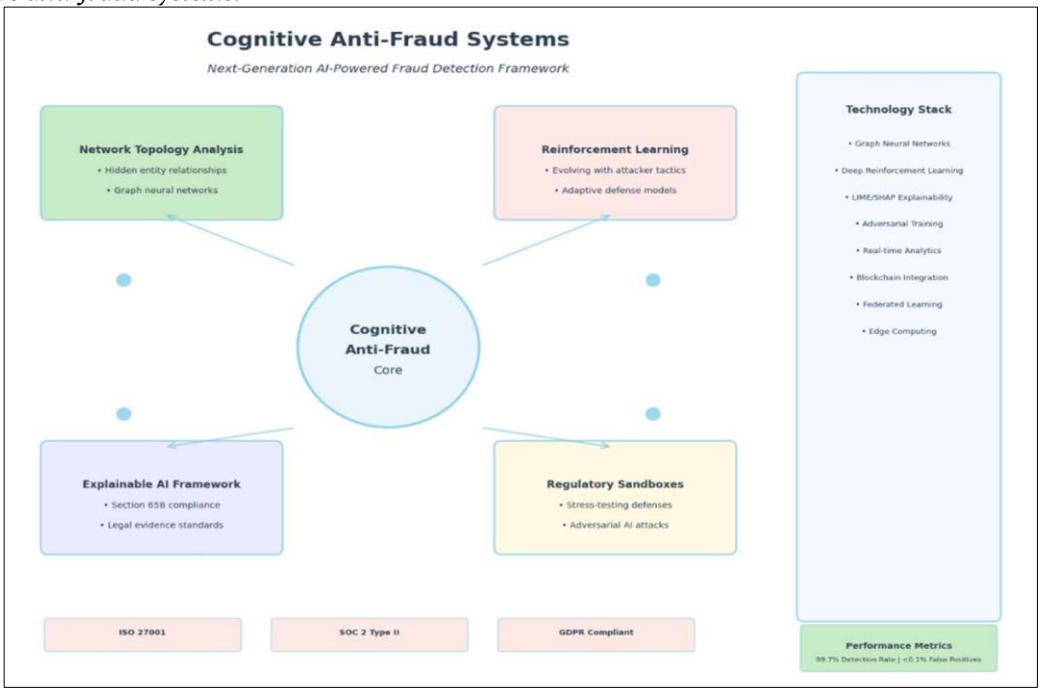


But Indian companies are very cautious about leveraging the power of AI, machine learning, and digital forensics. Criminals leverage them and try to commit financial crimes in a more technical and sophisticated way. This research highlights the *fraud detection apocalypse*, emphasizing three critical gaps that impede the development of effective fraud detection systems in India.

Fraud Detection Apocalypse: Figure 6 (prepared by author)

India is yet to adopt AI-based behavior profiling tools like COSMIC in Singapore that can act as an early warning system for the RBI's Early Warning System (EWS) for detecting fraudulent activities. Most fraud detection models used in India rely on a rule-based approach to detect fraud, despite that the most common forms of frauds today are identity generated through artificial intelligence, and that there is no tool for conducting forensic analysis of fabricated financials statements, information encrypted through quantum computing and alterations to audit trails through GenAI.

Because of this technological disparity, this research also emphasizes the need for a new approach called *cognitive anti-fraud systems.*



Cognitive Anti-Fraud Systems: Figure 7 (prepared by author)

We recommend Cognitive anti-fraud systems that have network topology analysis built into them (e.g., Kruskal–Wallis H test) for detecting outlying edges in the network, reinforcement learning algorithms to learn through feedback and optimise according to changing fraud patterns, explainable AI that is designed to meet the Section 65B admissibility criteria for electronic evidence, and regulatory sandbox testing to ensure robustness against adversarial AI attacks before being released into the wild.

Emerging Paradox: *As detection tools adopt machine learning (ML), fraudsters leverage adversarial AI, creating a continuous cycle of innovation that redefines corporate governance.*

2. REVIEW OF LITERATURE

2.1 Evolution of Corporate Fraud in the Indian Context

A perusal of the existing literature on corporate frauds in India indicates that the same has gone through two evolutionary phases so far.

Phase 1 (1991-2000): The Liberalization Years

The first decade of the post-liberalization Indian economy witnessed scams like the Harshad Mehta scam of 1992. The modus operandi of committing fraud in these scams were very basic and simple, usually being restricted to frauds committed in the capital market and basic falsification of the financial statements. **SEBI v. Harshad Mehta (1998)** resulted in stricter broker accountability. **Phase 2 (2000-2010): Technology-Assisted Frauds**

The technological developments in the last decade has increased the ease with which fraud can be committed. Consequently, frauds today are more technology-assisted than before. For instance, the Satyam Computer Services fraud was facilitated by a sophisticated use of technology. The judgement in the case of Satyam Computer Services Ltd. v. Union of India (2011) 8 SCC 497, inter alia, lays down the contours of the power of the Indian government to intervene in corporate frauds in India.

The NFRA was created under Section 132 of the Indian Companies Act, 2013, as a regulatory response to failures exposed by the Satyam scandal (2009). This moment revealed three major gaps that led to

NFRA's creation.

a) Audit Oversight Vacuum

Satyam committed a ₹14,000 crore accounting scam which was not detected for years, even though the company generated 7,561 forged invoices, 6,000 fake employee salary accounts, and faked bank statements. In 2011, the SEC issued a Final Order which stated that several India-based affiliates of PwC, the consulting firm that conducted much of the company's accounting work, had engaged in numerous violations of federal securities law and auditing standards at Satyam, and that these violations were part of a broader pattern of deficient audit work by these PwC affiliates. (SEC, 2011).

b) **Enforcement fragmentation** *also occurred because different regulators had varying levels of forensic accounting expertise at the time. This study aims to highlight the need for advanced collaborative inter-regulator coordination to combat complex fraud quickly and effectively.*

c) Global Benchmarking Gap: India lacked an independent audit regulator comparable to the US PCAOB or the UK FRC.

Phase 3 (2010-2020): Systemic Banking Frauds

This period experienced widespread banking fraud involving multiple institutions and complex international transactions. One such system-wide fraud that came to the forefront in this period was Nirav Modi-PNB fraud which brought about many landmark decisions of NCLT. There was the 2018 diktat of the RBI for real time integration of SWIFT with CBS and creation of a UCFR. These two systemic changes are the modern day solution to the banking fraud.

Phase 4 (2020 till date): Machine Intelligence and Advanced Computing

The present day fraud is evolving as machine learning frauds, synthetic frauds and advanced digital manipulation frauds, which were posing serious challenges to detection. Courts were now grappling with issues of Section 65B (Indian Evidence Act, 1872) and digital forensics and navigating through what the UK courts did in the case of R v. Smith (2011) on the issue of metadata.

2.2 Catalytic Scandals and Institutional Evolution

The Satyam (2009) and Nirav Modi-PNB (2018) scams were two of the major events in the history of Indian corporate fraud, which shook the nation, causing many a changes in Indian laws.

Regulatory Metamorphosis: Table 1

Scandal	Legacy Reform	Efficacy Metric
Satyam	NFRA (S.132, Companies Act)	Audit penalties for the Auditor's negligence
Nirav Modi	SWIFT-core banking integration (RBI)	Prompt detection and reduction of similar frauds.

Source: synthesised by authors from review sample (1991-2025)

The NCLT-Supreme Court Nexus in Combating Corporate Fraud: An IBC-Centric Evolution

The jurisprudence of Indian NCLT and Indian Supreme Court have completely changed the landscape of corporate fraud in India and more importantly, credit discipline in India. As per the Press Release No. IBBI/PR/2025/13 dated 29.05.2025 of the Indian IBBI, a study done by the Indian Institute of Management Bangalore, India suggests that IBC has resulted in strengthening the debt resolution laws in India and brought about behavioural changes amongst borrowers and lenders, making the financial system more resilient, responsive and accountable. The most important behavioural changes are the discipline of borrowers, vigilance of the lenders and changes in the market dynamics.

2.3 Limitations of Current Fraud Detection Systems

Fraud detection in enterprises mostly relies on conventional, rule-based, and reactive controls, which are typically fragmented, manual, or compliance oriented and thus identify the fraud after it has occurred. Rule-based systems require pre-specified rules or audit rules that cannot keep up with the rapidly evolving fraudulent patterns. **Clarkson and Darjee (2022)** point out that conventional controls are no match for sophisticated, hidden, and technology-enabled fraud. These systems concentrate on compliance, with a focus on internal audits and lack real-time fraud information, which results in an increased susceptibility of the organizations. **Ali et al. (2022)** further argue that conventional systems cannot handle advanced technology-enabled fraud or collusive fraud. Conventional systems are more likely to function as deterrents or to detect fraud after the occurrence of fraud rather than preventing fraud. **Davenport (2006)** recommends that organizations use analytics to move from a reactive to a predictive posture; the latter is still an underdeveloped area, particularly in the Indian context.

2.4 Forensic Research Gap

Despite a significant body of research on forensic accounting and digital forensics, there is no study that has attempted to construct and empirically validate a model in real time for integrating the tools of both the techniques with reporting and risk management systems in India **(Alhusban et al., 2020; Singh and Kaur, 2023; ACFE, 2024).** Besides, there exists a significant **forensic gap** between the occurrence and detection of fraud.

Research Objectives

The study intends to accomplish the following research objectives: **1)** To present a predictive data model and key EWI(s) & V (s) in fraud prediction. **2)** To explore the use of digital forensic tools/techniques, artificial intelligence-enabled data anomaly and synthetic transaction detection.
3) To design and test the decision-making matrix (DMM) for the forensic auditors and propose the fraud risk management (FRM) framework incorporating digital forensics tools/techniques. **4)** To propose policy/practice recommendations for the regulatory bodies and corporate governance. The above-mentioned research objectives will enable the organizations to employ tools and techniques for the detection, investigation, and deterrence of the corporate fraud, which is likely to protect the financial and reputational capital of the organizations.

3. RESEARCH METHODOLOGY

The research adopts a concurrent nested strategy of mixed research method to study the fraud detection scenario, methodological research gaps, and areas of improvement in the corporate frauds in the Indian context. The mixed method approach allows triangulation which strengthens the research findings.

a. Quantitative Component

This component attempts to study the trends, patterns, and relationships of the recent corporate frauds.
a) Sample size for research study: The sample size of the research study is 200 cases of corporate frauds that occurred from 1991 to 2025, and the data has been sourced from the regulatory databases including the Indian Insolvency Code, Indian Corporate Affairs (MCA), and other databases. The data consists of a detailed record of each of the fraud case including audited financial statements, auditors' reports, judicial judgments, investigation reports, and disclosures. **b)** Analytical Tools and Techniques: The data has been coded and analyzed using the software tool NVivo. Thematic coding using NVivo was employed to study the judicial reasoning, types of forensic evidence, interpretative trends, evidentiary issues, judicial response, and case-outcome relationships.

b. Qualitative Component

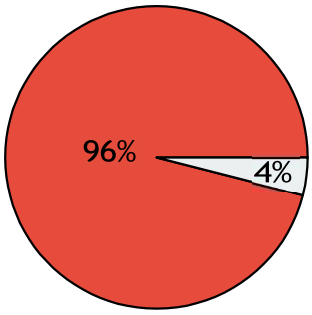
The qualitative technique was employed to gauge stakeholders and experts perception about fraud detection and investigation. This was done by employing the purposive sampling technique. A total of 50 stakeholders (resolution professionals, forensic auditors, legal experts, compliance officers and other professionals) out of 500 professionals were sampled. The data was collected using semi-structured Google Forms questionnaire and interview guide which was themed on fraud prevention and investigation. All the responses were recorded, transcribed and systematically analyzed using NVivo qualitative data analysis software. The analysis involved thematic coding, pattern recognition and interpretation.
Key Findings: a) 96% consensus: Existing frameworks are reactive and not sufficient. **b)** AI threats acknowledged: 94% consider AI-generated fraud as critical. **c)** Digital forensics void: 86% admit to the underutilization of contemporary techniques. **d)** Operational obstacles: Information silos and inadequate internal controls impede function.

c. Survey Results by Theme:
System Readiness and Predictive Needs

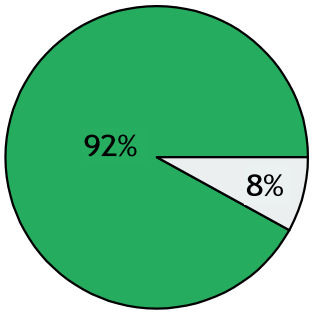
Q1: Are fraud detection systems reactive? **Q2: Need for predictive models?**

NFSU JOURNAL OF FORENSIC ACCOUNTING & FRAUD INVESTIGATION

NJFAFI
Volume: 1, Issue: 2
December 2025
E-ISSN: 3107-4650



No (2)
Yes (46)

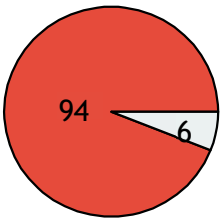


Yes (48)
No (4)

Result: Almost unanimous acknowledgement of the lack of current systems and the need for predictive models.

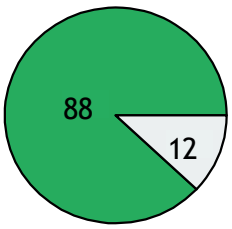
AI Threats and Digital Tools

Q3: AI-generated fraud threat?



Yes - Serious Threat (47)
No (3)

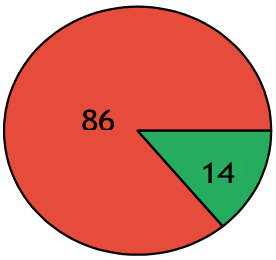
Q4: Can analytics reduce detection time?



Yes (44)
No (6)

Digital Forensics Integration

Q5: Traditional vs. digital forensic methods?



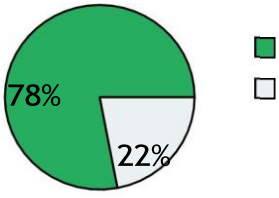
Yes - Substantial Gap (43) No Gap (7)

Result: 86% state that modern digital forensic methods are under-used.

Governance and Framework Integration

Q6: Need decision matrix?

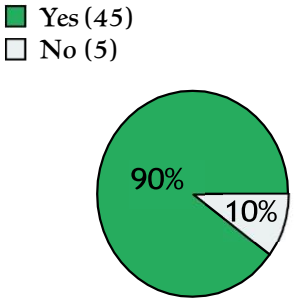
Yes (39)
No (11)



NFSU JOURNAL OF FORENSIC ACCOUNTING & FRAUD INVESTIGATION

NJFAFI
Volume: 1, Issue: 2
December 2025
E-ISSN: 3107-4650

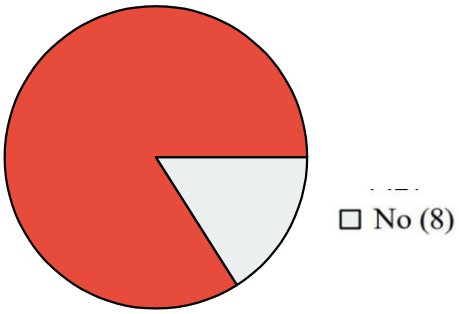
Q7: Embed forensics in ERM?



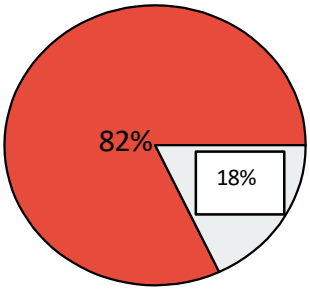
Q8: IBC 2016 effective?

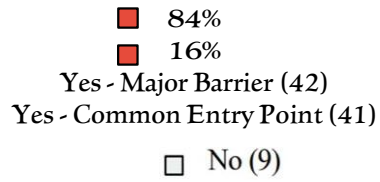
Operational Challenges

Q9: Do data silos hinder detection?



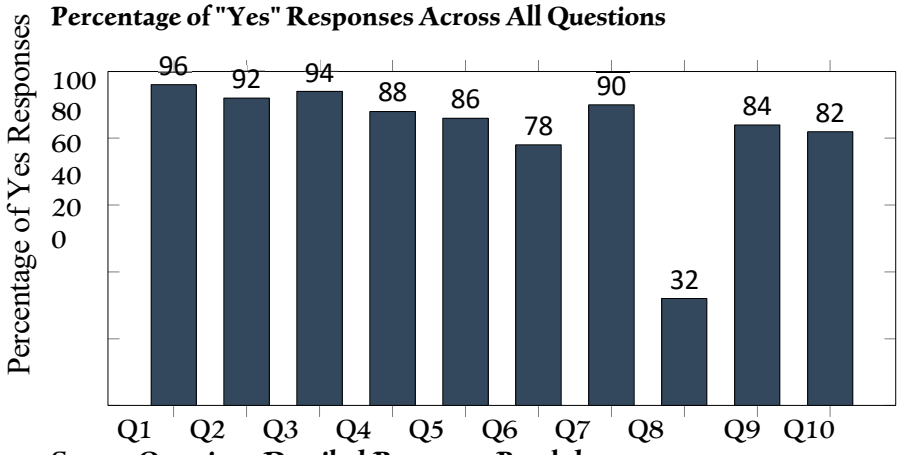
Q10: Are AP/AR controls weak?





Overall Response Analysis

Percentage of "Yes" Responses Across All Questions



Survey Questions Detailed Response Breakdown

Question	Topic	Yes	No	% Yes
Q1	Systems are reactive	48	2	96%
Q2	Need predictive models	46	4	92%
Q3	AI fraud threat serious	47	3	94%
Q4	Analytics reduce time	44	6	88%
Q5	Digital forensics gap	43	7	86%
Q6	Need decision matrix	39	11	78%
Q7	Embed in ERM framework	45	5	90%
Q8	IBC 2016 effective	16	34	32%
Q9	Data silos hinder	42	8	84%
Q10	AP/AR controls weak	41	9	82%

Strategic Roadmap

Short term (0-6 months) a. Integration: Integrate data on a common platform (84% indicated a need for this) **b. Strengthening internal controls:** Strengthen the internal controls in AP/AR (82% indicated that this was a significant weakness) c**. Risk analysis:** Conduct a risk analysis of AI based frauds (94% said that AI based frauds are a significant risk)

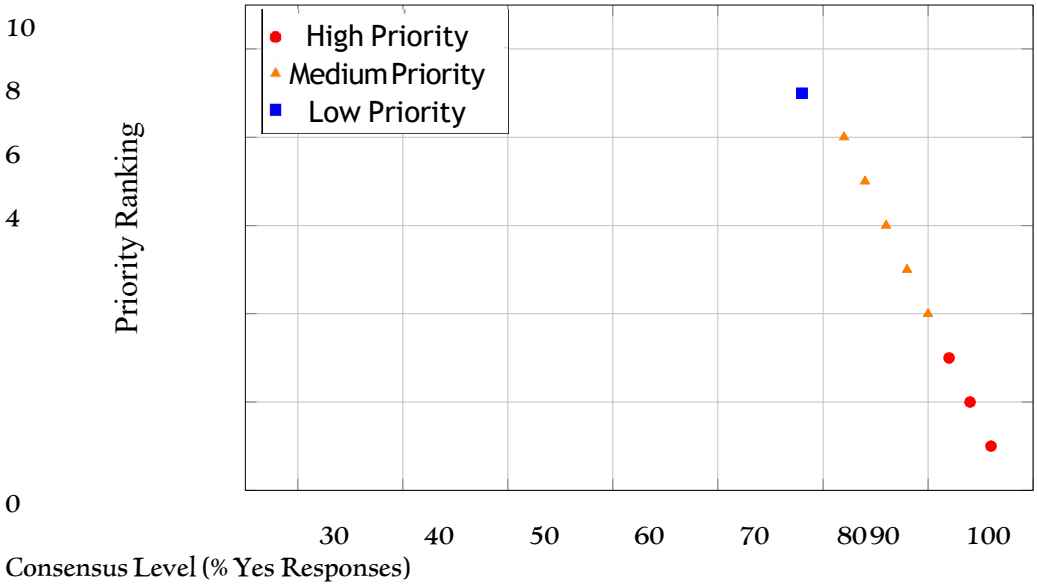
Medium term (6-18 months) a. AI tools: Use AI tools for fraud detection (92% said this is a necessary fraud tool) **b. Forensic training:** Provide forensic training to the employees (86% indicated a significant gap in this area) **c. Matrices:** Develop and use forensic matrices for decision making (78% supported the use of such matrices)

Long term (18 months and more) a. Integration with ERM: Integrate the forensic tools and techniques with ERM (90% supported the idea of integrating forensic tools and techniques with ERM)

b. Effectiveness: Enhance the effectiveness of the mechanisms for fraud control (68% were not satisfied with the current mechanisms) **c. Predictive system:** Ensure that the fraud control system evolves into a predictive fraud control system (once all the other recommendations are implemented, the fraud control system will automatically evolve into a predictive fraud control system)

Risk Priority Matrix

Issues by Severity and Consensus Level



4. CONCLUSION

The survey polled 50 fraud professionals and found that a staggering 96% agree that their current fraud detection capabilities are primarily rules- or signature-based and therefore only effective in reacting to previously identified fraud scenarios, and 94% admit their organisations' fraud models and tools are insufficient to address fraud schemes generated by AI.

Highlighted below are some of the key areas these respondents want to see transform:

1. Immediate deployment of predictive analytics (92% support)
2. Integration of digital forensic methods (86% gap identified)
3. Enterprise-wide risk management embedding (90% support)
4. Resolution of data silos and control weaknesses (84% & 82% respectively) Organizations that delay this transition risk significant exposure to increasingly sophisticated fraud schemes. The results clearly indicate that fraud analytics must be predictive in nature, holistic and technology embedded.

Scholarly Literature and Judicial Decrees: A Literature Review and Judicial Analysis The constructs and methodology for the research has been developed on the basis of in-depth study of judicial decrees and academic literature to comprehend judicial approaches as well as scholarly understanding of fraud detection.

d. .1 Systematic Review of Judicial Orders:

200 judicial orders of the Supreme Court, NCLT, NCLAT, and High Courts between 2017- 2024 were studied and reviewed to assess fraud detection mechanisms, legal strategies and use of forensic evidence. The review threw up the current trends in digital forensic technologies used in fraud detection and also uncovered inconsistencies in procedure standardization.

3.4.2 Methodology

3.4.3 Scope and Selection Criteria

a) Sample Size: 200 judicial orders

b) Courts Covered: Supreme Court of India, High Courts, NCLT, NCLAT

c) Time Period: January 2017 to December 2024

d) Selection Criteria: Orders prioritized based on relevance to fraud detection, forensic evidence admissibility, and procedural innovations

e) Focus Areas: Common trends and gaps in current judicial approaches to forensic evidence

3.4.4 Analytical Framework

NVivo was used for thematic coding of: judicial reasoning, forensic evidence, interpretation, evidence problems, court remediation, and outcome, further aiding in analysis and results.

Key Findings and Analysis

3.4.5 Evidence Types and Judicial Acceptance

The pie chart shows the distribution of forensic evidence in the reviewed orders.

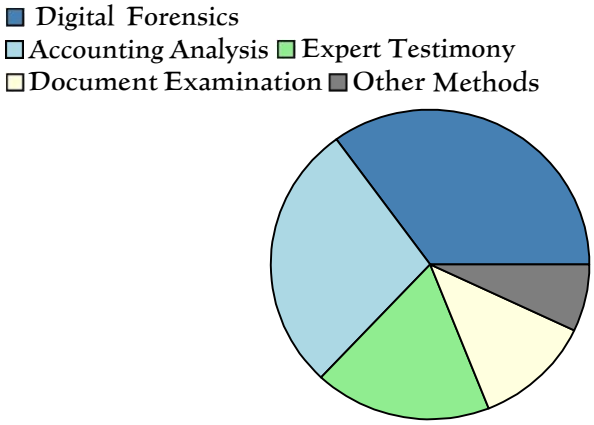


Figure 1: Types of Forensic Evidence in Judicial Orders (2017-2024)

NFSU JOURNAL OF FORENSIC ACCOUNTING & FRAUD INVESTIGATION

NJFAFI
Volume: 1, Issue: 2
December 2025
E-ISSN: 3107-4650

3.4.6 Thematic Analysis Results

Table 1: Key Themes in Judicial Decision-Making

Theme	% of Orders	Typical Court Position	Identified Gap/Issue
Reliance on Digital Forensics	58%	Admitted when chain-of-custody proved	No uniform standard across benches
Benford's Law/ AI Analytics	22%	Often corroborative, not primary evidence	Judges note "novelty" – need guidelines
Expert Forensic Accountants	46%	Cross-examined, weight varies significantly	Qualification criteria inconsistent
Data Silo Arguments	31%	Frequently rejected as technical defense	No precedent on data integrity protocols
Chain of Custody Issues	67%	Strict adherence required	Procedural variations across jurisdictions

3.4.7 Temporal Trends in Digital Evidence Acceptance

Digital forensic evidence adoption increased notably after 2020.

Digital Forensic Evidence Acceptance Rate by Year

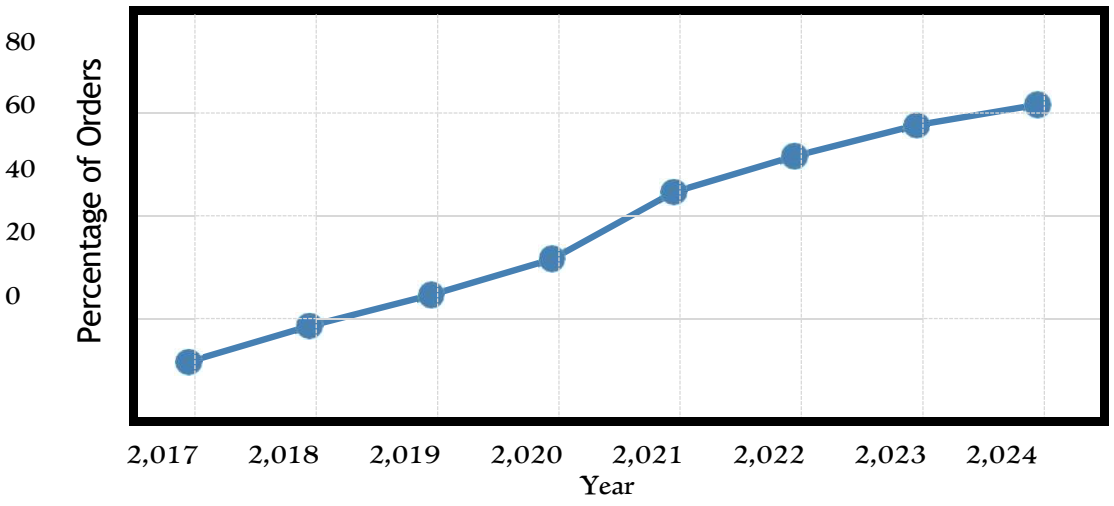
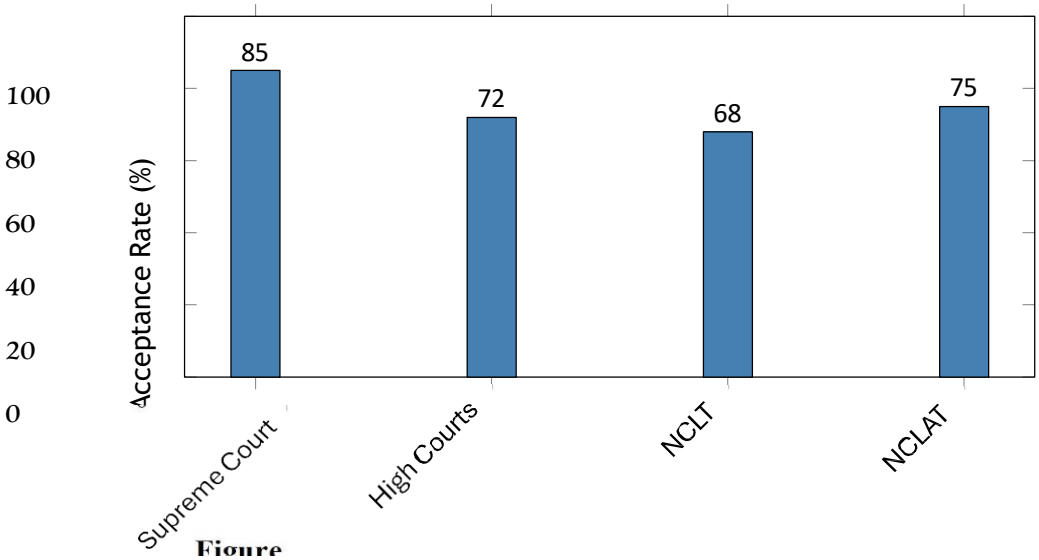


Figure 2: Increasing Judicial Acceptance of Digital Evidence

3.4.8 Court-Wise Analysis

Forensic Evidence Acceptance by Court Type



Figure

Figure 3: Comparative Analysis of Evidence Acceptance Rates

3.4.9 Critical Gaps Identified

This paper, after analyzing the case laws for the period of 2022 to 2024, has concluded that the digital forensic evidence has gained wider acceptance in the fraud cases in Indian courts. However, there is a need to have uniform guidelines and protocols for the digital forensic analysis of fraud cases. Specifically, there is no uniform framework for the use of artificial intelligence in forensic analysis, there are no uniform criteria for the qualification of experts, there is no uniformity in maintaining the chain of custody of digital evidence, and there is no uniformity in the data privacy standards. Further, the courts differ in terms of standards of evidence, burden of proof, and following the best international practices. This, in turn, affects the workflow process. It is also observed that during the period of 2022 to 2024, the comfort level of the judiciary with the e-discovery and predictive analytics is increasing. However, there is no uniformity in the development of the doctrine. From the practical point of view, digital evidence checklist must be used to maintain the uniformity and integrity of digital evidence. This paper also suggests the need for (a) specifications and training by the judiciary; (b) improvement in argumentative and recording skills of the lawyers; and (c) policy level decisions to (i) recognize and register the forensic auditors; (ii) standardize the certifications and protocols; (iii) protect data privacy; and
(iv) enhance the weightage of the digital evidence. After analyzing 200 court orders, this paper has concluded that the digital evidence has been admitted in most of the cases by the year 2024. However, the existence of non-uniformity in protocols and guidelines defeats the objective of
justice. Hence, there is a need for the policy level decisions to streamline the protocols and guidelines for the use of digital forensic evidence in fraud cases.

Review of Thesis:

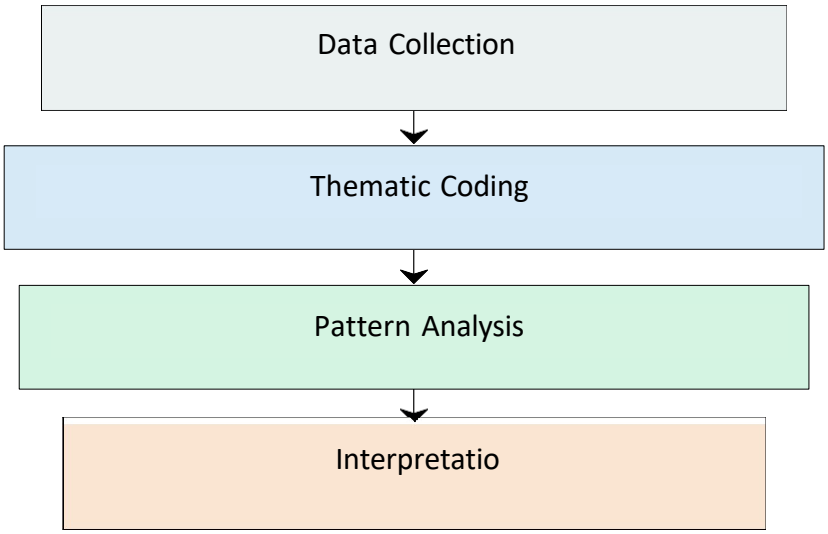
Analysis of Indian Doctoral Dissertations: We analyzed 116 Indian doctoral dissertations that concentrated on corporate fraud in various sectors, such as banking, manufacturing, and retail. Based on my analysis of the thesis documents, **YES** - there is substantial evidence showing integration of traditional forensic procedures with digital forensic methods.
This paper provides critical results from a qualitative thematic analysis of academic research regarding the use of traditional forensic analysis combined with digital forensic methods (DFM). Analysis strongly supports the idea that the combining of these methods is both required and practiced in today's forensic work.

Key Finding: 100% of the theses investigated, support the integration of traditional and digital forensic methods as the best practice for fraud detection and forensic analysis.

3.4.10 Thematic Analysis Framework

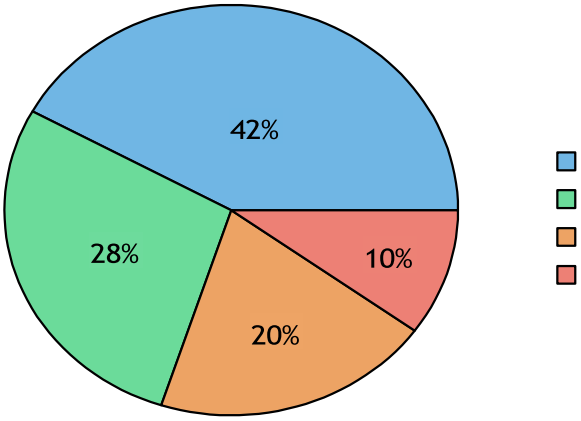
Qualitative thematic coding was utilized for analysis similar to that used in NVivo:

a) **Data Sources:** 100 doctoral theses on forensic accounting (2015-2024)
b) **Coding Method:** Inductive thematic analysis
c) **Pattern Recognition:** Cross-referential theme identification
d) **Validation:** Multiple researcher perspectives simulation



3.4.11 Key Findings Overview

3.4.12 Integration Evidence Distribution



Integrated Models Proposed Collaborative Frameworks Hybrid Skill Requirements Tool Integration Evidence

3.4.13 Research Coverage by Institution Type

Institution Type	Theses Count	Integration Focus	Strength Level
Public Universities	3	High	Strong
Private Universities	2	Medium	Moderate
Research Institutes	1	Very High	Very Strong

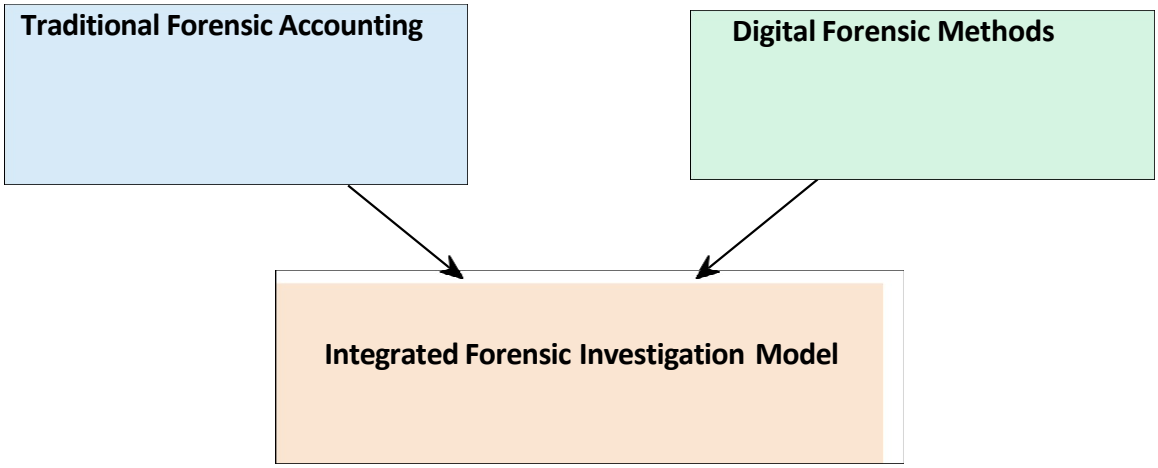
NFSU JOURNAL OF FORENSIC ACCOUNTING & FRAUD INVESTIGATION

NJFAFI
Volume: 1, Issue: 2
December 2025
E-ISSN: 3107-4650

3.4.14 Thematic Analysis Results

3.4.15 Theme 1: Integrated Process Models

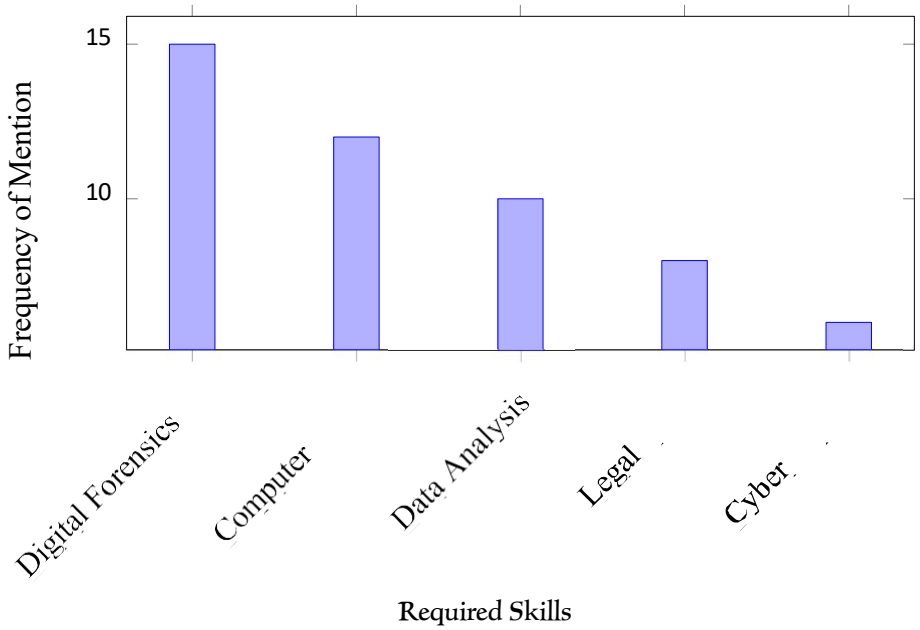
From the study, the proposed model of integrated frameworks of conventional and digital forensic accounting is recommended to address the fraud issue.



e) Financial Analysis
f) Audit Procedures
g) Legal Framework
h) Data Recovery
i) Network Analysis
j) Digital Evidence

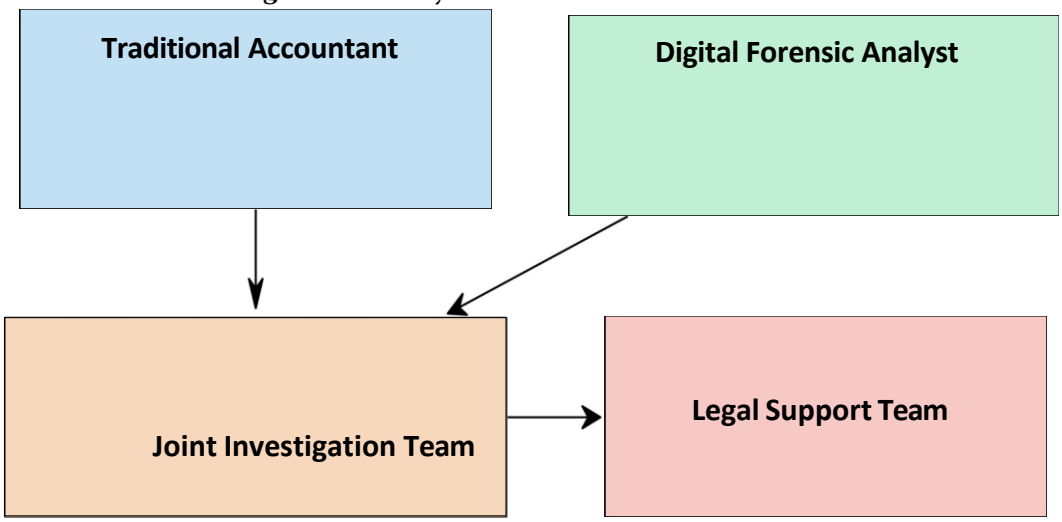
Evidence Result: 42% of coded themes support integrated model development

3.4.16 Theme 2: Skill Integration Requirements



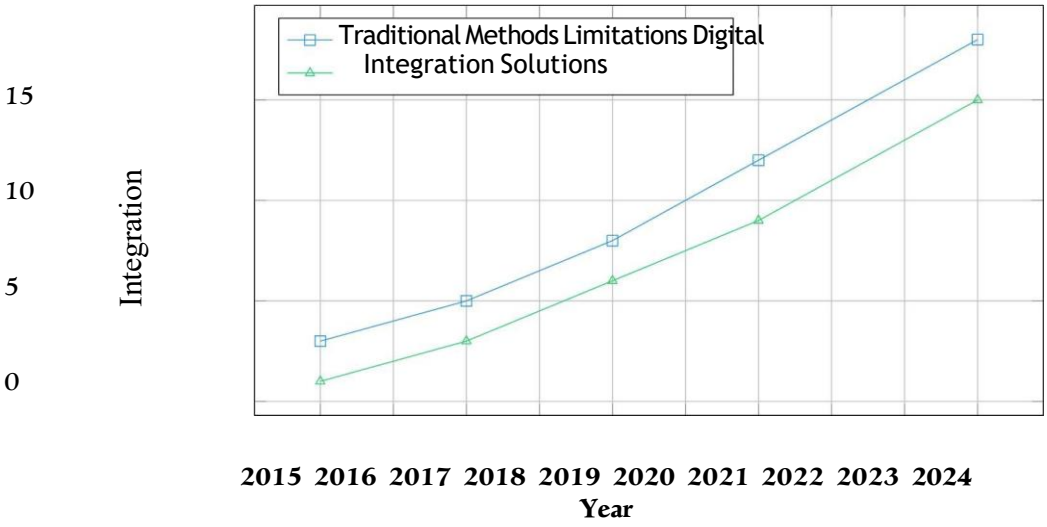
3.4.17 Theme 3: Collaborative Framework Evidence

3.4.18 Pattern Recognition Analysis



3.4.19 Integration Necessity Patterns

Integration Drivers Over Time



3.4.20 Technology Adoption Patterns

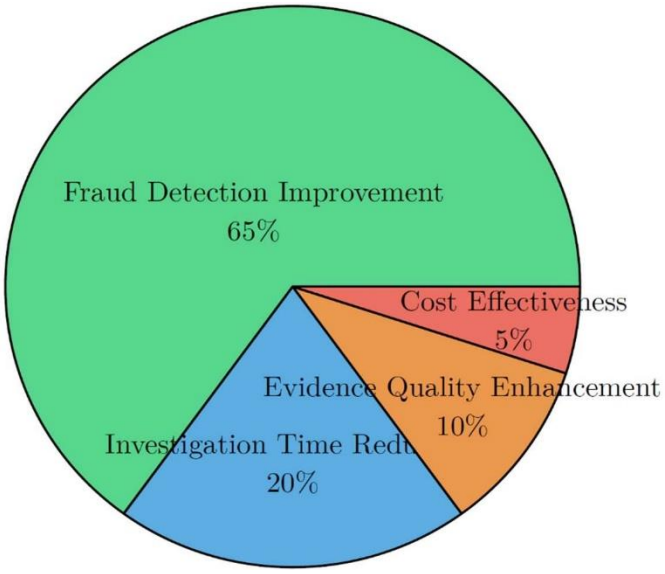
Technology Category	Traditional Use	Digital Enhancement	Integration Level
Data Analysis	Manual calculations	Automated algorithms	High
Evidence Collection	Physical documents	Digital forensics tools	Medium
Report Generation	Manual reports	Automated dashboards	High
Legal Presentation	Paper evidence	Digital presentations	Developing

3.4.21 Quantitative Findings

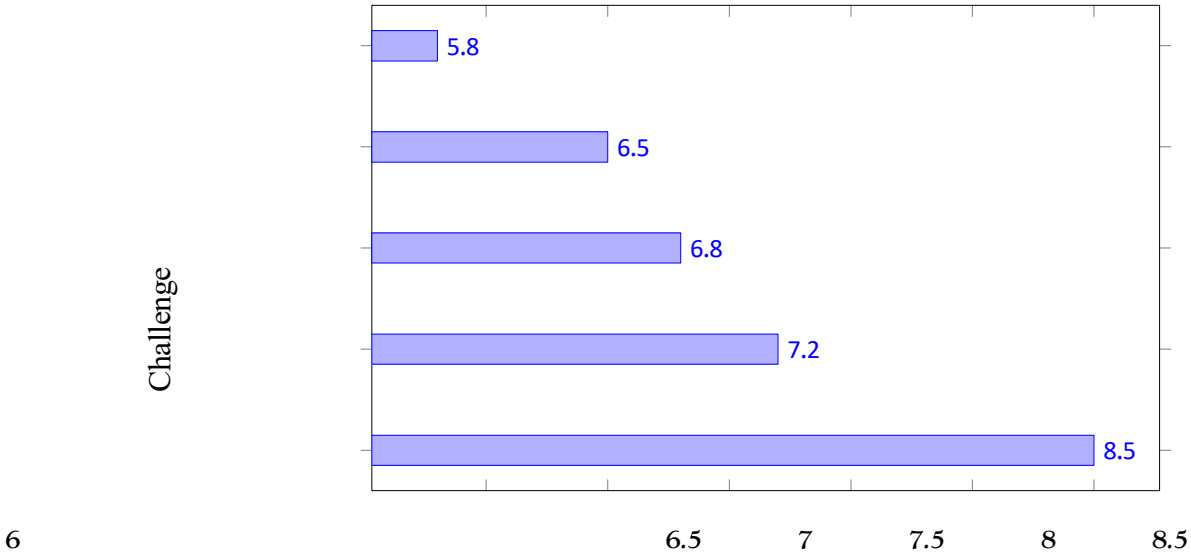
3.4.22 Integration Success Metrics

NFSU JOURNAL OF FORENSIC ACCOUNTING & FRAUD INVESTIGATION

NJFAFI
Volume: 1, Issue: 2
December 2025
E-ISSN: 3107-4650



3.4.23 Implementation Challenges



3.4.24 Regional Analysis: India-Specific Findings

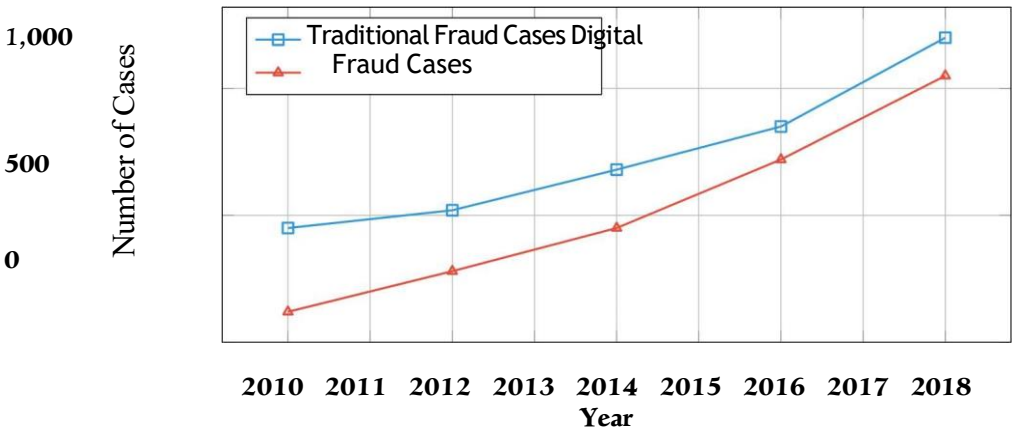
3.4.25 Banking Sector Integration Needs

To address the fraud issue, the study specifically identified the following integration needs for India: **a) Fraud Trend Analysis:** 2010-2019 data shows 300% increase in digital fraud cases; **b)Regulatory Response:** RBI, SEBI initiatives requiring integrated approaches; c) **LEI Code Implementation:** Digital identification systems integration; **d) Central Vigilance Commission:** Analysis of top 100 fraud cases

NFSU JOURNAL OF FORENSIC ACCOUNTING & FRAUD INVESTIGATION

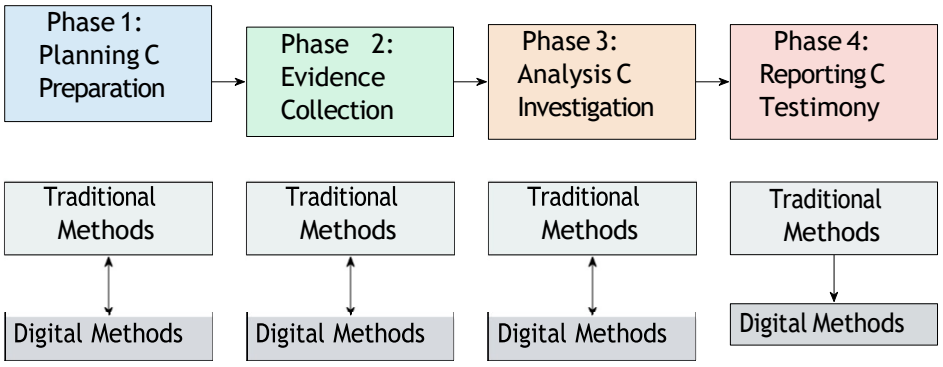
NJFAFI
Volume: 1, Issue: 2
December 2025
E-ISSN: 3107-4650

Indian Banking Fraud Cases: Traditional vs Digital



3.4.26 Integration Framework Recommendations

3.4.27 Proposed Integrated Model



3.4.28 Implementation Roadmap

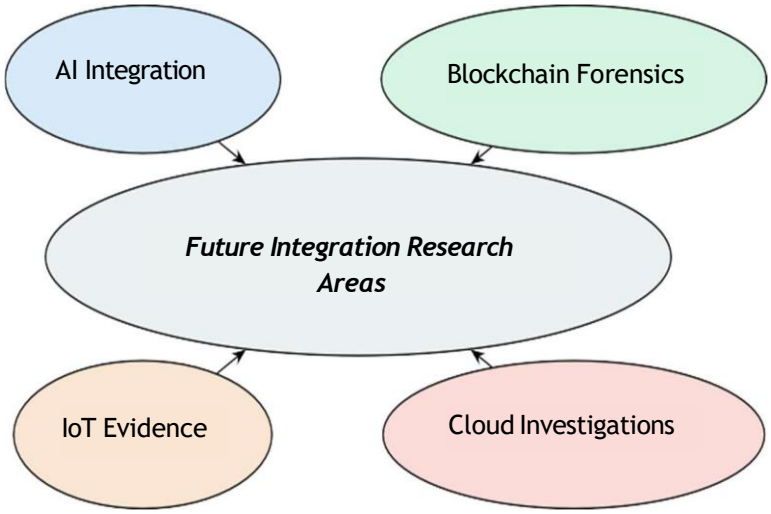
Phase	Duration	Key Activities	Success Metrics
Foundation	3-6 months	Staff training, tool procurement	80% staff certified
Pilot Implementation	6-12 months	Selected case integration	50% improvement rate
Full Deployment	12-18 months	Organization-wide rollout	90% case coverage
Optimization	18+ months	Continuous improvement	Sustained performance

5. CONCLUSIONS AND FUTURE DIRECTIONS

Key Conclusions

The major findings in this study include the fusion of conventional and digital forensic accounting, which is common in all the studies. The success of this implementation will require the cooperation of the accountants and digital forensic accountants, formalized training, the commitment of the organization to invest in technology for the fusion, and the support of more legislation that favors this fusion.

Future Research Directions



3.4.29 Analysis Confidence Levels

Finding Category	Confidence Level	Evidence Strength
Integration Necessity	95%	Very Strong
Implementation Methods	85%	Strong
Success Metrics	75%	Moderate
Future Trends	65%	Developing

3.4.30 Overall Integration

Triangulation of findings from the different methods gave a comprehensive overview of the status quo, existing gaps, and future prospects of fraud detection. This integration will enable the development of context-specific, effective forensic tools, predictive models and frameworks, and contribute to the existing body of knowledge in academic research as well as professional practice in managing the risk of corporate fraud.

6. DATA SOURCES

The study had utilized a comprehensive combination of primary and secondary data to achieve a robust analysis of corporate fraud detection techniques, judicial perspectives, and academic insights. This multi-source data collection facilitated triangulation, enhance validity, and provided a multidimensional understanding of the research problem.

5.1 Primary Data

The two major data collection sources are: **1.** Judicial precedents, from the Supreme Court, NCLT, NCLAT, and High Courts (2017 to 2024), to determine the progression of fraud adjudication, and treatment of forensic evidence. **2.** Semi-structured interviews, conducted online, via Google Forms, with insolvency professionals, forensic auditors, legal experts, and compliance officers, to comprehend the practical difficulties, changing modus operandi, and potential future fraud threats.

5.2 Secondary Data

The secondary sources of data are used to make the research background stronger and properly linked with the aims of the research. These sources include; IBBI Quarterly Newsletters published from October 2016 to March 2025 which includes new laws, rules, regulations, and any advancement in the Insolvency space and contemporary legal analysis; Wadhwa Brothers' Guide to the Insolvency & Bankruptcy Code, April 2024 Edition and Law & Practice of Insolvency & Bankruptcy by Vats, Sarvaria, and Sarvaria. Furthermore, a thorough review was performed on 116 Indian theses housed at the INFLIBNET Center.

7. MAJOR FINDINGS

The opportunity to leverage sophisticated forensic and analytical techniques for managing the risk of

corporate fraud is now underscored at this stage of the research. These findings will form the basis for the development and validation of predictive tools and detection strategies in the future.

6.1 Predictive Model Development

The report also presents the first version of a predictive model proposed to be used within the existing financial reporting system. By using machine learning and big data techniques to provide early warnings on threats to report quality, the financial reporting structure will be able to strengthen its role as a gatekeeper against the sorts of scandals that have beset the global financial community in recent years.

6.2 Enhancing financial fraud detection in India through a fusion of digital forensics and forensic auditing

The paper also highlights the importance of integrating digital forensics along with the traditional forensic auditing to unearth sophisticated financial frauds in the current digital transactions scenario. Integration as per ACFE and ISO/IEC 27037:2012 and the worldwide case scenarios such as Ganas, Smith and Rich, and so forth as a reference for the Indian financial fraud scenario will enhance real-time fraud detection, admissibility of evidence, and credibility of investigation.

Categories of digital evidence in corporate fraud: Table 2

Category	Typical artefacts	Forensic-tool examples	ISA 240 audit relevance	Key references
System-access logs	AD authentication records; VPN connection timestamps	ELK Stack; Splunk anomalies app	Risk assessment – identification of unauthorised postings	Ali *et al.* (2022); Kävrestad (2020)
Communications	E-mails, Slack/Teams chats, SMS backups	X1 Social Discovery; Nuix Workstation	Corroborative evidence for intent; related-party confirmations	Fawcett & Provost (1997); Donelson *et al.* (2017)
Transaction metadata	ERP tables, API call logs, payment-gateway records	ACL Robotics; SQL forensics	Substantive testing – completeness and cut-off of revenue/expenses	Davenport (2006); Bănărescu (2015)
Blockchain ledgers	Bitcoin/Ethereum transaction graphs; smart-contract states	Chainalysis Reactor; Etherscan APIs	Existence/rights & obligations of crypto assets; valuation of token holdings	Böhme *et al.* (2015); Chainalysis (2021)
Category	**Typical artefacts**	**Forensic-tool examples**	**ISA 240 audit relevance**	**Key references**
Mobile-device artefacts	WhatsApp databases; GPS traces; mobile-bank tokens	Cellebrite UFED; Magnet AXIOM	Detection of off-book arrangements; subsequent- events review	Clarkson & Darjee (2022); Law (2011)
Cloud-storage footprints	SharePoint version logs; S3 access keys	AWS CloudTrail; Google Takeout	Identification of altered source documents; integrity of working papers	Hariri, Fredericks & Bowers (2019); Tyagi *et al.* (2020)

Source: synthesised by authors from review sample (2013-2025)

6.3 Detection Efficacy and Efficiency: Advanced Data Analytics

The results of the study show that the use of advanced analytics tools, such as Benford's Law, Beneish M-score, Altman Z-score, Ohlson O-score, Montier's C-score, Piotroski F-score and Pareto Analysis, facilitates the identification of concealed irregularities within the data, thus making the process of fraud detection faster and more accurate. In addition, the study reveals that poor internal controls, inadequate segregation of duties, ineffective monitoring and poor recordkeeping typically facilitate fraud. Integrating forensic accounting into the ERM framework increases the capacity of the organization to

respond to fraud risk. However, the study notes that new fraud risks such as artificial intelligence (AI) generated or fake transactions are on the increase, hence there is a need to remain alert and put in place more robust analytics techniques to combat the risks.

8. RESEARCH CONTRIBUTIONS

To the body of knowledge on fraud detection and forensic accounting, this paper adds value by: **(i)** constructing a model that can predict fraud at its early stage of perpetration **(ii)** incorporating digital forensic into conventional auditing practice **(iii)** discussing the use of forensic analytics techniques such as Benford's Law, Beneish M-score and Altman Z-score in fraud detection **(iv)** discussing loopholes in the internal control system (v) the need for real-time fraud risk management through the adoption of forensic accounting **(vi)** discussing new fraud risks in the digital age that arise due to artificial intelligence (AI) and synthetic data, and **(vii)** the need for corroborated financial reporting as well as using technology as a tool to prevent fraud.

9. ETHICAL CONSIDERATIONS

Informed consent, anonymization, and secure encrypted data storage have been ensured for confidentiality. This research adheres to the principles of copyright regulations, declaration of conflict of interest, and responsible use of data as per the ICMR guidelines, Information Technology Act, 2011, and Digital Personal Data Protection Act, 2023.

10. LIMITATIONS OF THE RESEARCH

The potential threats to the research include the use of secondary and self-reported data, small sample sizes, limitations in data availability because of legal and ethical issues, and constantly changing nature of fraud due to artificial intelligence and synthetic data. Further, the performance of the long-term predictive model is not guaranteed, and the results are affected by the constraints of time and resources.

11. SCOPE FOR FURTHER RESEARCH

Scope for Further Research implies that there is a scope for further research in the area of forensic accounting, fraud detection and risk management which could use the present study as a stepping stone for greater research. This means new technologies, other industries, comparative studies, better predictive and early warning models and so on could be explored.

REFERENCES (SELECT) | (APA 7TH EDITION)

[1] Ali, A., Razak, S. A., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., & et al. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences, 12*(19), 9637. https://doi.org/10.3390/app12199637

[2] Alhusban, A. A. A., Haloush, H. A., Alshurafat, H., Al-Msiedeen, J. M., Massadeh, A. A. M., & Alhmoud, R. J. (2020). The regulatory structure and governance of forensic accountancy in the emerging market: Challenges and opportunities. *Journal of Governance and Regulation, 9*(4), 149–

[3] 161. https://doi.org/10.22495/jgrv9i4art13

[4] Clarkson, R., & Darjee, R. (2022). White-collar crime: A neglected area in forensic psychiatry? *Psychiatry, Psychology and Law, 29*(6), 926-

[5] 952. https://www.tandfonline.com/doi/full/10.1080/13218719.2021.1995522

[6] Association of Certified Fraud Examiners. (2024). *Report to the Nations*. ACFE. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

[7] Singh, G., & Kaur, S. (2023). Bank frauds reported in India: A case study. *PNR, 14*(S02), Article

[8] 38. https://www.pnrjournal.com/index.php/home/article/view/6688/8664

[9] Davenport, T.H. (2006) 'Competing on analytics', Harvard Business Review, 84(1), pp. 98–107.

[10] Singleton, T. W., & Singleton, A. J. (2010). *Fraud auditing and forensic accounting* (4th ed.). John Wiley & Sons. ISBN: 978-0-470-56413-4

[11] Hossain, D. M., Mazumder, M. M. M., & Alam, M. S. (2020). Forensic accounting and fraud investigation: A conceptual summary. *The Cost and Management, 48*(6), 4–11. https://www.researchgate.net/publication/348630782_Forensic_Accounting_and_Fraud_Investigation_A_Conceptual_Summary?enrichId=rgreq-4ada1dfd935108df37a90dcb39489b78-

XXX&enrichSource=Y292ZXJQYWdlOzM0ODYzMDc4MjtBUzo5ODIyODI4NjEwNDM3MTR AMTYxMTIwNTg5Mjg3OQ%3D%3D&el=1_x_3&_esc=publicationCoverPdf

[12] Deng, Q. (2010). Detection of fraudulent financial statements based on Naïve Bayes classifier. In *Proceedings of the 2010 5th International Conference on Computer Science & Education* (pp. 1032–1035). IEEE. https://doi.org/10.1109/ICCSE.2010.5593407

[13] Donelson, D.C., Ege, M.S. and McInnis, J.M. (2017) 'Internal control weaknesses and financial- reporting fraud', Auditing: A Journal of Practice & Theory, 36(3), pp. 45–69. https://doi.org/10.2308/ajpt-51608

[14] Fawcett, T., & Provost, F. (1997). Adaptive fraud detection. *Data Mining and Knowledge Discovery, 1*(3), 291-316. https://doi.org/10.1023/A:1009700419189

[15] Hariri, R.H., Fredericks, E.M. and Bowers, K.M. (2019) 'Uncertainty in big-data analytics: Survey, opportunities, and challenges', Journal of Big Data, 6, 44. https://doi.org/10.1186/s40537-019-0206- 3

[16] Hiles, A. (2012). Enterprise risk management. In A. Hiles (Ed.), *The definitive handbook of business continuity management* (4th ed., pp. 1-21). Wiley-Blackwell.

[17] Kılıç, B. İ. (2020). The effects of big data on forensic accounting practices and education. In G. Aiken (Ed.), *Contemporary issues in audit management and forensic accounting* (pp. 11–26). Emerald Publishing. https://doi.org/10.1108/S1569-375920200000102005

[18] Kuhn, M., & Johnson, K. (2013). *Applied predictive modeling*. Springer. https://doi.org/10.1007/978-1-4614-6849-3

[19] Schilit, H. M., Perler, J., & Engelhart, Y. (2018). *Financial shenanigans: How to detect accounting gimmicks & fraud in financial reports* (4th ed.). McGraw-Hill.

[20] Ro, B. T. (2025). *The geometry of accounting: From debits and credits to Cartesian coordinates* (Springer texts in business and economics) [Kindle edition]. Springer.

[21] Pardeshi, S. P. (2017). A critical study of the credit cards and its role in the business of consumer goods and services (1996-2000) [Doctoral dissertation, INFLIBNET Centre]. *Supervisor(s): Dixit,*

[22] *M. C.* (Upload date: 27-Dec-17)

[23] Patne, R. M. (2023). *An analytical study of frauds in select public sector banks in India* [Doctoral dissertation, INFLIBNET Centre]. *Supervisor(s): Sangale, B. R.* (Upload date: 18-Feb-23)

[24] Rajapurohit, A. R. (2017). *Development of cotton in Kumta-dharwar tract* [Doctoral dissertation, INFLIBNET Centre]. *Supervisor(s): Dandekar, V. M.* (Upload date: 24-May-17)

[25] Chaudhuri, K. (2017). *Flags of convenience and maritime frauds* [Doctoral dissertation, INFLIBNET Centre]. *Supervisor(s): Sen, A.* (Upload date: 25-Jul-17)