International Journal of Accounting and Economics Studies, 12 (8) (2025) 219-231

International Journal of Accounting and Economics Studies

Website: www.sciencepubco.com/index.php/IJAES
https://doi.org/10.14419/3q97j527
Research paper

Accounting and Corporate Deception: A Global and Indian Perspective on Forensic Accounting Interventions

Dr. Barkha Rani [1], Suman Das [2], Dr. Saurabh Rana [3], Dr. Narender Kumar Bishnoi [3]*, Mahaveer Prasad [4]

[1] Assistant Professor, Department of ABST, University of Rajasthan, Jaipur, India
[2] Assistant Professor, Department of Geography, Kirori Mal College, University of Delhi, New Delhi, India
[3] Assistant Professor Senior Scale, Faculty of Law, University of Delhi, New Delhi, India
[4] Research Scholar, Department of ABST, University of Rajasthan, Jaipur, India
**Corresponding author E-mail: n.bishnoi84@gmail.com*

Received: October 1, 2025, Accepted: November 19, 2025, Published: December 8, 2025

Abstract

Over the past decade, financial fraud has transformed from isolated misconduct to intricate, cross-border networks exploiting systemic weaknesses in governance, technology, and regulation. Traditional audit and compliance solutions, which are reactive and compartmentalized, are falling behind the adaptive and scalable nature of fraud. It is challenging to discern between deliberate fraud and legitimate transactions due to sophisticated tactics like smart contract attacks and synthetic identities. As a front-line defence, forensic accounting necessitates a proactive, intelligence-driven strategy that combines knowledge of finance, cyber, regulations, and risk. Despite legislative improvements, India's system is reactive rather than preventive due to large gaps in enforcement, coordination, and specialized capability. Closing this gap requires incorporating forensic methods into corporate governance and encouraging shareholder participation. Advanced technologies like blockchain traceability and real-time surveillance are essential to this evolution. The future of fraud prevention depends on institutions' capacity to promptly identify and eradicate emerging risks. Forensic accounting must evolve into a core pillar of financial oversight to safeguard systemic integrity in an era of engineered deception.

Keywords: *Forensic Accounting; Frauds; India.*

1. Introduction

In today's financial world, when dishonest methods like creative accounting and window dressing have gotten more sophisticated and common, the old belief that "an auditor is a watchdog, not a bloodhound" has become increasingly outdated (Abou-Zeid, El-Mousawi, & Younis, 2020). These manipulations usually conceal financial deficiencies by misleading stakeholders with the inherent flaws of traditional rule-based and sampling-focused audits (Elumilade et al., 2021; Kaminski, Wetzel, & Guan, 2004). According to Schipper (1989), creative accounting is the intentional involvement of management in the financial reporting process by manipulating estimates and accounting decisions that are permitted by existing rules. Even while these actions are frequently lawful, they have the potential to misrepresent the financial health and performance of an organization.

In addition to undermining investor confidence and regulatory monitoring, accounting fraud is a dynamic and secretive phenomenon that also fuels wider economic instability (Black, 2010). It puts international financial systems at risk by raising capital market volatility and unpredictability. One well-known example of how fraud can be included in reporting that seems to be compliant on the surface is the infamous practice of "cooking the books," in which companies overstate earnings or conceal costs. Typical auditing is insufficient to detect tiny errors because of the complexity of these systems. As Baesens, Vlasselaer, and Verbeke (2015) argue, a data-driven and expert-based approach—grounded in historical fraud patterns and predictive indicators—is essential to identifying and mitigating emerging financial misconduct.

Forensic accounting has consequently emerged as a critical discipline in modern fraud detection, offering tools and methodologies far beyond the purview of traditional audit functions. Forensic accounting employs machine learning techniques, data mining, and network analysis to examine complete datasets in order to identify abnormalities and early fraud indications, in contrast to audits that depend on samples (Elumilade et al., 2021). In order to find trends of creative accounting and deliberate misrepresentation, it looks into both quantitative measures and qualitative disclosures (Özkul & Pamukçu, 2012). According to Crumbley (2009), forensic accounting operates at the intersection of auditing, economics, finance, law, and information systems—requiring multidisciplinary proficiency to tackle increasingly intricate schemes.

The scope of forensic accounting has been further expanded by natural language processing and text analytics, which make it possible to examine narrative financial statements for linguistic indicators of dishonesty (Goel, Gangolly, Faerman, & Uzuner, 2010; Honigsberg, 2020). The evidential value of financial communications in legal and regulatory investigations is strengthened by these technologies' ability

Copyright © Dr. Barkha Rani et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

to identify minute changes in tone or structure that can point to fraudulent intent. To settle economic and financial conflicts, forensic accounting is a multidisciplinary profession and industry that integrates theories and methods from law, psychology, sociology, criminology, and finance, according to Huber and DiGabriele (2014). Forensic accounting is a specialist profession that includes the identification, investigation, and analysis of financial data relevant to fraud and legal inquiries, according to the American Institute of Certified Public Accountants (AICPA).

A paradigm shift in fraud detection methods is represented by the use of big data analytics in forensic procedures. The period between the discovery of fraudulent activity and its detection can be greatly reduced by quickly identifying deviations from expected norms through the real-time analysis of enormous amounts of both structured and unstructured data (Shalhoob et al., 2024; Mittal, Kaur, & Gupta, 2021). Tools like anomaly detection, predictive modeling, and data visualization are increasingly vital in unearthing complex, hidden fraud schemes before they escalate. Moreover, forensic accounting strengthens corporate governance by addressing the audit expectation gap—the difference between public expectations of audits and the limited scope of what audits typically deliver. Without the limitations that frequently impede statutory auditors, forensic accountants use their legal knowledge and specialized investigative abilities to more precisely identify financial misstatements (Gray & Debreceny, 2014; Adejumo & Ogburie, 2025) (Altaf, 2025). This paper is an attempt to analyze how, with the growth of technological advancement, new forms of fraud are emerging—and how forensic accounting techniques are evolving in response. It evaluates the changing environment of forensic accounting in the context of digital innovation and assesses the discipline's adaptability to combat modern fraud threats. Furthermore, by examining significant fraud cases at the national and international levels, this paper investigates the state of forensic accounting in India and draws attention to the scope and character of possible financial malfeasance in both situations. Fraud detection procedures need to be redefined in light of the changing financial world. As corporate fraud becomes more widespread and intricate, our tactics must adapt as well. The shift from traditional audits to forensic accounting is a required strategic realignment as well as a methodological advancement. Forensic accounting provides a strong framework to identify, stop, and address fraudulent financial activity by utilizing big data, artificial intelligence, and multidisciplinary approaches. This protects transparency and confidence in capital markets (Vijayalakshmi & Jeevan, 2024; Özkul & Pamukçu, 2012; Elumilade et al., 2021).

2. Review of Literature

Forensic accounting has long existed across various cultures, with its roots traced to Kautilya's ancient Indian documentation of embezzlement techniques and the crime-solving practices of figures like Birbal (Okpako, 2013; Alabdullah, 2014). Forensic accounting is a specialist area that aims to detect fraud and resolve legal problems, while being frequently confused with auditing (Bhasin, 2007; Shah, 2014; Ocansey, 2017; Joseph, 2016). Major scandals like Enron and WorldCom, which revealed the shortcomings of conventional auditing techniques, gave the discipline a huge boost in popularity around the world (Anghel & Poenaru, 2023a). By identifying systemic vulnerabilities, forensic accounting has a preventive function in addition to detecting financial crimes (Lamba & Jain, 2020). By tracking down illegal activities and providing expert testimony, the forensic accountant serves as a financial investigator (Lamba & Jain, 2020). Numerous investigations conducted worldwide have confirmed its efficacy in fraud detection (Capraş & Achim, 2023; Ratzinger-Sakel et al., 2022). Although nations like Australia, New Zealand, and South Africa exhibit strong research participation, awareness, and implementation are still unequal, especially in areas like Jordan (Alharasis et al., 2023) (Botes & Saadeh, 2018). Forensic accounting is still not well studied in India, despite the country's increasing demand for openness due to corporate fraud (Chetry et al., 2025). Strong financial accountability is essential for drawing in investment and winning over investors, as the nation now ranks fourth in the world in terms of GDP. Regulatory barriers and a lack of understanding persist despite ICAI's efforts to set standards (ICAI, 2020). The importance of improving forensic processes is demonstrated by notable fraud cases such as Satyam, PNB, and IndusInd Bank (Reuters, 2025).

The COVID-19 pandemic further underscored the importance of the field as cybercrime surged and regulatory shortcomings were exposed (Jamil et al., 2022). While Faizah et al. (2020) concentrated on employing big data analytics to detect healthcare fraud, Mehta et al. (2022) emphasized how artificial intelligence might enhance forensic capabilities. Merigó (2017) highlighted how the global discourse on forensic accounting has been dominated by American research. Furthermore, theoretical works present forensic accounting as a proactive and reactive instrument to counteract financial fraud (Ozili, 2020; DiGabriele & Huber, 2013). Recent bibliometric reviews (Merigó, 2017; Ratzinger-Sakel & Tiedemann, 2022) indicate that nearly 65% of published research on forensic accounting between 2010 and 2024 originates from the United States and Europe, reflecting a Western dominance in the field. In contrast, contributions from emerging economies—particularly India, the Middle East, and parts of Africa—account for less than 20% of total output. Within this body of literature, approximately 40% of studies emphasize digital and AI-enabled fraud detection, while research addressing educational frameworks, regulatory systems, and localized applications remains limited. This uneven distribution highlights the continuing need for region-specific investigations and applied research in developing economies such as India. The discipline's multidisciplinary component, which combines legal, auditing, and financial skills, is receiving more attention (Yadav & Yadav, 2013). Although adoption obstacles like organizational reluctance and a lack of infrastructure still exist, technological advancements like artificial intelligence (AI) and data mining have revolutionized its application (Akinbowale et al., 2023; Sánchez-Aguayo et al., 2021; Nickell et al., 2023). Studies show a variety of implementation issues at the regional level. In Saudi Arabia and India, cultural and legislative constraints impede development (Wadhwa & Pal, 2012; Oraby, 2023), whereas developed regions enjoy greater institutional support (Guellim, N. et al., 2024). The importance of forensic accounting in corporate governance is becoming more widely acknowledged, and strong systems are associated with lower fraud risks (Mousavi et al., 2022; Blanco et al., 2023). Professional and educational gaps are still quite important. In nations such as Australia and India, growth is impeded by inadequate curriculum coverage and a lack of industry participation (Al-Shurafat et al., 2024; Ismail et al., 2022). Most people agree that standardized terminology and training are necessary (Botes & Saadeh, 2018). Supported by real-world case studies like the Satyam and Saradha scams (Almeida, 2024; GN, 2022), recent trends emphasize new objectives, including digital forensics and regulatory technologies (Ellili et al., 2024; Afriyie et al., 2023). The research consistently highlights the growing importance of forensic accounting in safeguarding financial integrity and calls for enhanced regulatory frameworks, technological flexibility, and international cooperation (Curtis, 2008; Nasrallah et al., 2022; Ozili, 2023).

3. Objectives of The Study

The idea of forensic accounting is still intricate and multidimensional, especially when viewed in light of accounting procedures and financial records. In order to properly utilize this field's potential in addressing financial irregularities, it is necessary to increase comprehension, given the low level of awareness surrounding it. This study employs a qualitative and interpretive review method to analyze how forensic accounting has evolved as a response to financial misconduct across jurisdictions. Scholarly articles and regulatory documents

were retrieved from Scopus, Web of Science, SSRN, and ResearchGate, focusing on studies published between 2010 and 2025. Sources were screened for conceptual depth, empirical relevance, and policy orientation toward fraud detection and governance reform. The selected literature and case materials were thematically coded under categories such as fraud typologies, regulatory responses, and forensic interventions. Comparative analysis between global and Indian contexts was undertaken to identify emerging trends, structural gaps, and policy lessons shaping forensic accounting's contemporary role. The present study aims to achieve the following objectives:

1) Investigate major financial fraud cases.
2) Analyze the techniques and methodologies utilized in fraud.
3) The nature of newly emerging financial frauds and manipulative accounting practices
4) Assess the role of forensic accounting in detecting and preventing fraudulent activities.
5) Evaluate the prospects of forensic accounting in India in light of the increasing incidence of financial fraud.

By highlighting the importance of forensic accounting in preventing and detecting fraud, especially in the Indian financial sector, this study adds to the larger conversation on the subject. This research is organized into five thorough sections. Major worldwide fraud episodes over the last ten years are examined in the first section, along with their scope, the parties involved, and the type of misbehaviour. The methods employed in these frauds are examined in the second section, which also shows patterns and how fraudulent activity has changed over time. Emerging frauds fuelled by technology developments, particularly some that are expected to occur soon, are the subject of the third section. The function of forensic accountants in identifying, stopping, and lessening such frauds is assessed in the fourth section. The fifth and last section evaluates the state, difficulties, and advancements of forensic accounting in India.

3.1. Decade of deception: a global review of major financial frauds

Over the past decade, there has been a dramatic growth in fraudulent activity in the global financial sector, marked not just by an increase in frequency but also by an increase in complexity and breadth. From traditional Ponzi schemes and accounting frauds to sophisticated cyber heists and crypto-related scams, financial crimes have outpaced many of the regulatory and institutional safeguards meant to prevent them. This section presents a global review of major financial frauds that occurred during the last decade. The comprehensive table included herein catalogues high-profile fraud cases across regions and sectors, detailing the methods used, financial losses incurred, and broader socio-economic consequences. These cases are not isolated events; they reflect deeper systemic vulnerabilities—ranging from regulatory failures and weak corporate governance to technological loopholes and transnational legal blind spots. Together, the data and analysis in this report aim to identify recurring themes, root causes, and emerging risks in the world of financial fraud. By examining the largest frauds of the previous decade, this study seeks to strengthen institutional resilience, direct future regulatory efforts, and aid in the development of more adaptable financial supervision structures.

Table 1: Major Fraudulent Cases Over the Last Decade: Comparative Summary of Major Global Frauds Based on Regulatory and Media Sources, Outlining Each Case's Year, Nature, Scale, and Impact

Sr. No	Name of Fraud Case	Year	Nature of Fraud	Magnitude of Fraud	Parties Affected
1	Adani-Hindenburg	2023	Stock manipulation and accounting fraud schemes, as alleged by Hindenburg Research.	USD 218 billion (market loss as claimed)	Investors, Govt. tax revenues
2	FTX Cryptocurrency Exchange (USA)	2022	Misuse of customer funds, lack of internal controls, and fraudulent asset handling.	$8-10 billion	Investors, crypto clients, and creditors
3	Greensill Capital (UK)	2021	Misleading financial reporting and high-risk lending through supply-chain finance.	$10+ billion	Credit Suisse, UK Govt, SMEs
4	Wirecard AG (Germany)	2020	Falsified bank balances and accounting fraud. Claimed €1.9B that didn't exist.	€1.9 billion	Investors, German regulators, global partners
5	Luckin Coffee (China)	2020	Inflated revenues by booking fake sales to meet growth expectations.	$310 million	Nasdaq, investors, shareholders
6	PNB-Nirav Modi Scam	2018	Nirav Modi and associates colluded with PNB officials to obtain fraudulent Letters of Undertaking (LoUs) and Letters of Credit (LoCs) via SWIFT without collateral.	Fraudulent LoUs worth 13,000 Cr	Punjab National Bank, Correspondent Banks
7	IL&FS Crisis	2018	Financial mismanagement, misreporting, and concealment of true financial health; defaulted on multiple debt obligations due to excessive leverage and NPAs.	Exposure over 191,000 Cr	Stock market, bond market, credit markets
8	Steinhoff International (South Africa)	2017	Falsified accounts, hidden debts, and inflated asset values to hide losses.	$7.4 billion	Shareholders, auditors, EU regulators
9	Theranos (USA)	2016	Misrepresentation of blood testing tech; deceived investors and regulators.	$700 million	Investors, Patients, FDA, Media
10	Volkswagen Emissions Scandal (Germany)	2015	Installed 'defeat devices' to cheat on emissions tests.	$33 billion in fines	Consumers, Regulators, Auto Industry
11	Saradha Group	2013	A Ponzi scheme promising high returns using funds from new investors to pay earlier ones.	Thousands of crores (estimated)	Retail investors, political stakeholders
12	Kingfisher Airlines	2012	Accumulation of debt due to high operational costs and aggressive expansion; defaulted on loans.	Loan default of 29,000 Cr	Employees, Banks, Investors
13	Satyam Computer Services	2009	The founder inflated financial statements (revenues, assets, cash) using fake invoices, fabricated bank statements, and inflated employee/salary figures.	Overstated cash: 5,040 Cr; Liabilities: 1,230 Cr; Debtors: 490 Cr	Shareholders, 53,000 employees

The techniques used by scammers have drastically changed over the last ten years, showing growing complexity, digital manipulation, and systemic abuse. Cases like Luckin Coffee (2020), which started with classic revenue inflation, demonstrated how inflated coupon-based transactions and fraudulent sales entries were utilized to inflate financial performance and deceive investors. In Wirecard AG (2020), executives crafted a complex web of deception by falsifying bank balances, inventing escrow accounts, and exploiting regulatory blind spots across jurisdictions—highlighting the growing difficulty of cross-border financial oversight. Another manipulation came to light with Greensill Capital (2021), where credit risk was concealed through aggressive off-balance-sheet financing and opaque supply chain finance

structures. This raised more general concerns about disclosure transparency in fintech lending. The collapse of the FTX cryptocurrency exchange in 2022 opened a new chapter in wrongdoing in the digital age by exposing intentional circumvention of internal safeguards, user fund mixing, and a near-complete lack of corporate governance in decentralized finance (DeFi) systems. The use of offshore shell companies, related-party transactions, and purported stock manipulation were also highlighted by Adani-Hindenburg (2023) as ways to maintain the appearance of financial health and boost share values. These examples, which come from a variety of industries and regions, highlight how complicated and widespread financial fraud has become over the last ten years. By analyzing each case in detail and highlighting the strategies used, the financial impact, and any systemic repercussions, the accompanying table provides a clear picture of how deceit has developed and thrived in a rapidly shifting financial climate.

3.2. Evolving schemes: techniques, patterns, and the growth of financial misconduct

The nature of financial fraud has clearly changed during the last ten years. The field has changed from being dominated by human manipulation and simple internal deceit to highly sophisticated methods that take advantage of digital systems, disjointed regulations, and global financial interconnectedness. Fraud increasingly occurs across platforms, assets, and borders and is no longer limited to balance sheets. The accompanying diagram shows how fraud strategies have changed over the last ten years to put these trends in perspective. It draws attention to the ways that global connectedness, digitalization, and a greater dependence on virtual assets have changed the nature of financial fraud. What emerges is a clear trajectory: fraud has become more scalable, less detectable, and more global in its execution.

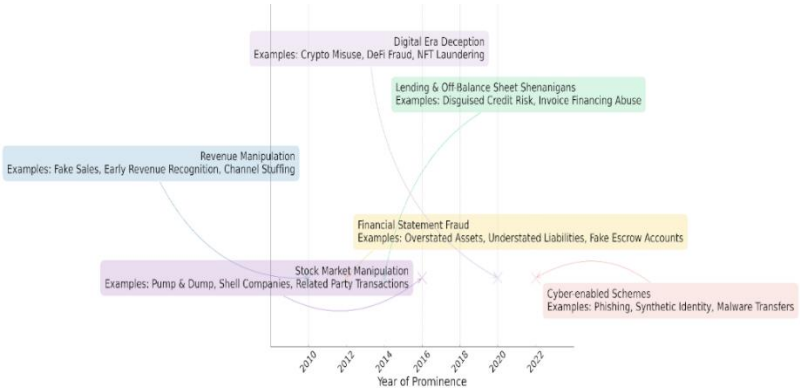

Fig. 1: Bubble Timeline: Evolution of Financial Fraud Methods; Illustrates the Progression of Global Financial Fraud Techniques Over Time, Highlighting the Transition from Traditional Accounting Manipulation to Digitally Enabled, Cross-Border Schemes.

The chronological heatmap (2014–2024) offers a visual trajectory of this shift. While asset misappropriation remains the most reported fraud category, its gradual decline—from 80 recorded cases in 2014 to 55 in 2024—suggests a redistribution of effort toward harder-to-detect, more scalable techniques. On the other hand, the rise of phishing tactics, malware attacks, payment gateway breaches, and illegal access to financial systems has caused cybercrime to surge sevenfold. This increase is not just quantitative; it signifies a qualitative change from internal wrongdoing to globally distributed crimes that are digitally coordinated.

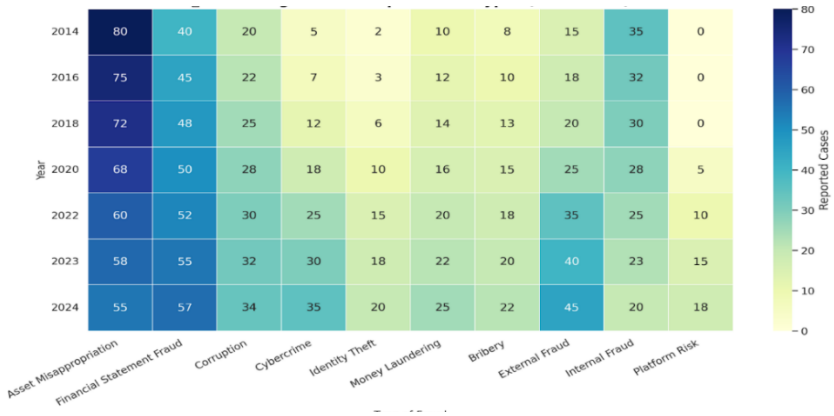

Fig. 2: Chronological Heat Map of Fraud Types (2014-2024); Visual Comparison of Dominant Fraud Types Over a Decade, Showing the Shift from Asset Misappropriation Toward Cyber-Enabled and Technology-Driven Financial Crimes.

Other fraud types previously viewed as secondary—such as identity theft, platform risk, and digital money laundering—have also gained significant ground. Their rise is a reflection of the rise of multi-layered fraud operations that take advantage of decentralized platforms, digital supply chains, and weak identity protocols. The heat map also reveals a notable reversal in the origin of fraud: external actors now perpetrate a greater proportion of financial misconduct than internal employees, underscoring the growing threat of third-party exploitation as companies rely more on digital vendors and outsourced services.

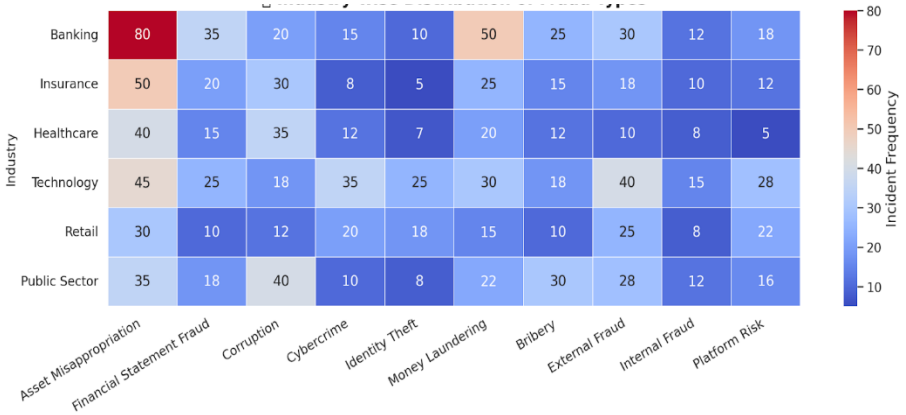

Fig. 3: Industry-Wise Distribution of Fraud Types: Visual Comparison of Dominant Fraud Types (Industry), Showing the Shift from Asset Misappropriation Toward Cyber-Enabled and Technology-Driven Financial Crimes

The unequal manifestation of this progression across industries is further revealed by the industry-wise heatmap. Banking has traditionally been a prime target since it has direct access to financial movements, but it still faces a lot of risks from both old (asset theft) and contemporary (external fraud, cybercrime) sources. The insurance industry is particularly vulnerable to financial statement fraud and corruption, which suggests structural deficiencies in transparency and regulatory compliance. A hotbed for procurement corruption and cybercrime, the healthcare industry is especially vulnerable during global crises and exposes supply networks and data abuse. Because of the fragility brought forth by increasing digitization and software dependency, technology organizations are particularly vulnerable to platform manipulation, API breaches, and external fraud. Meanwhile, retail and public sector entities, though reporting fewer incidents, show diverse exposures ranging from bribery and identity theft to internal collusion, reflecting underdeveloped internal controls and complex operational ecosystems. Drawing on data from ACFE's Report to the Nations (2014–2024), KPMG's Fraud Barometer, PwC's Economic Crime Survey, and RBI's annual reports, several dominant fraud techniques have emerged across sectors.

a) Financial Statement Manipulation: Digital Amplification of Classic Tactics

The largest losses are still caused by financial statement fraud, which averages $1.5 million each case (ACFE). It now uses digital billing systems, AI-enabled accounting tools, and ERP automation, which were previously restricted to human accounting entries. Among the noteworthy instances are 2020, Luckin Coffee (inflated coupons and fake transactions to commit fraudulent sales), Byju's (2021) (Deferred liabilities and aggressive early revenue recognition) and Heinz (2021), and Steinhoff (2017) (Fabricated earnings using cost manipulation and off-balance-sheet vehicles). These cases reveal how automation conceals manipulation within data architecture, challenging conventional audit trails.

b) Market Manipulation: Synthetic Valuation and Structural Opacity

Capital markets have become breeding grounds for engineered fraud, with increased use of related-party layering, offshore entities, and algorithmic distortion. Among the noteworthy instances are Adani–Hindenburg 2023(Alleged market inflation via circular trading and hidden ownership structures), FTX 2022 (token-based asset inflation, co-mingled client funds, and concealed risk through financial engineering). These strategies demonstrate a move away from misreporting and toward the creation of synthetic value, which makes it more difficult to discern between innovation and manipulation.

c) Banking and Lending Fraud: Algorithmic Loopholes in Fintech Ecosystems

RBI reports (2020–2023) highlight the persistence of credit-related fraud in public sector banks, now intensified by digital finance like PNB–Nirav Modi 2018 (Fraudulent LoUs used to obtain unauthorized credit), IL&FS 2018 (Circular lending and concealed liabilities). With fintech platforms automating loan origination and disbursement, fraud now exploits fake KYC data, synthetic borrowers, and app-based layering—making fraud scalable and harder to trace.

d) Operational Distortion: Internal Deception Disguised as Efficiency

Operational fraud includes less evident but equally important tactics like channel stuffing and procurement collusion, like Asian Paints 2022 (Unusual receivables revealed suspected revenue inflation from overstocking during a period of low demand). Such schemes are difficult to uncover without forensic analytics or insider disclosures.

e) Systemic Fraud: Cross-Border, Multi-Layered, and Embedded

The defining trend is integration—fraud today spans legal, cyber, financial, and behavioral dimensions. It is often orchestrated by networks of insiders, external enablers, and shell entities. The magnitude and sophistication of fraud have changed from Satyam (2009) to FTX (2022) and Adani–Hindenburg (2023), demonstrating how fraud has become entrenched, flexible, and challenging to identify with fragmented compliance systems.

3.3. Frontiers of fraud: emerging threats in a tech-driven era

As global financial systems digitize, fraud has entered a new frontier—one that is real-time, algorithmic, and increasingly difficult to detect.

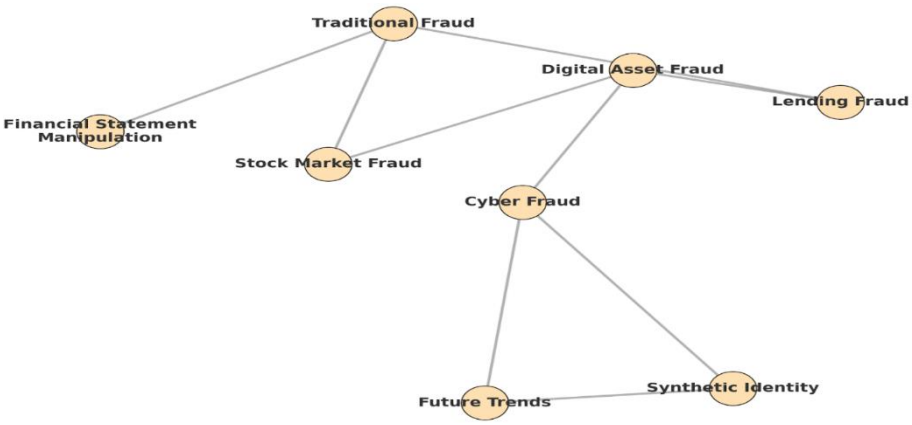

Fig. 4: Evolution of Financial Fraud Methods: from Traditional to Tech Enabled.

The diagram provides a conceptual journey through the transformation of financial misconduct over time. It begins with Traditional Fraud, such as basic revenue manipulation and accounting misstatements, which historically relied on manual deceit—like inflated sales figures or understated liabilities—to mislead investors and regulators. From this base, the diagram branches into Financial Statement Manipulation, Stock Market Fraud, and Lending Fraud—three methods that became more structured and systemic over time. These methods evolved to include shell companies, related-party transactions, off-balance-sheet lending, and earnings engineering. The fraud landscape evolved into Digital Asset Fraud, which includes cryptocurrency scams, NFT laundering, and DeFi misuse, as financial systems adopted digital assets and platforms. Cyber Fraud, a crucial node in the picture that symbolizes a significant change in the methods of committing fraud—through phishing, malware, QR code manipulation, and fake identities—was made possible by this digital advancement. These cyber tactics now enable real-time, personalized deception that's harder to trace and more damaging.

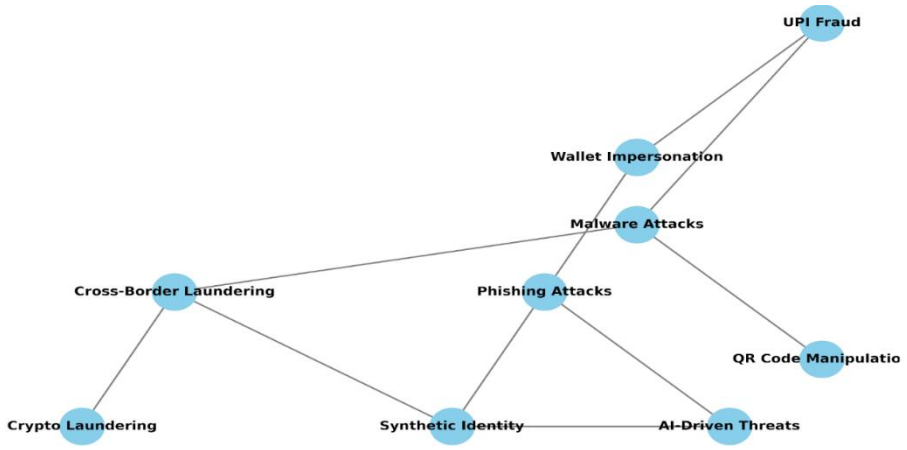

Fig. 5: Interlinking Network of Cyber-Enabled Financial Fraud Categories.

The networked nature of these frauds is visually represented in the accompanying diagram, illustrating how individual techniques—phishing, wallet impersonation, UPI scams, or synthetic identity creation—are interlinked. One technique often enables or amplifies another. For example, a phishing effort could result in credentials being taken, which could then be used for identity theft or to tamper with QR-based payments. These days, fraud operates as a self-reinforcing ecosystem that can scale swiftly and change in real time. Fraud enhanced by AI is at the heart of this development. According to INTERPOL and IFCACC (2023), artificial intelligence is being used in more than 40% of fraud efforts worldwide. Traditional frauds are being replaced with deepfake audio, synthetic voice cloning, and customized spear-phishing attacks. Social engineering is now hyper-personalized, automated, and delivered across multiple vectors—WhatsApp, fake UPI requests, spoofed customer service calls, and even real-time "receive money" frauds. Malware disguised as financial or utility apps allows fraudsters remote access to banking apps, while "man-in-the-browser" bots hijack transactions silently.

Another crucial area is the fraud of synthetic identities. In order to construct identities that pass digital KYC and AML checks, fraudsters now combine authentic data—such as Aadhaar, PAN, and biometrics—with fictitious credentials. These hybrid profiles evade compliance systems and create disjointed audit trails when they are used to open bank accounts, request credit, or launder money.

Digital asset fraud—through cryptocurrencies, NFTs, and DeFi platforms—adds another dimension. The systemic opacity of decentralized systems was revealed by the FTX collapse: ownership and intent are obscured by uncontrolled exchanges, cross-chain transactions, and anonymous wallets. Although INTERPOL's IFCACC task force (2023) has started focusing on these crimes, forensic tracing tools are still lacking.

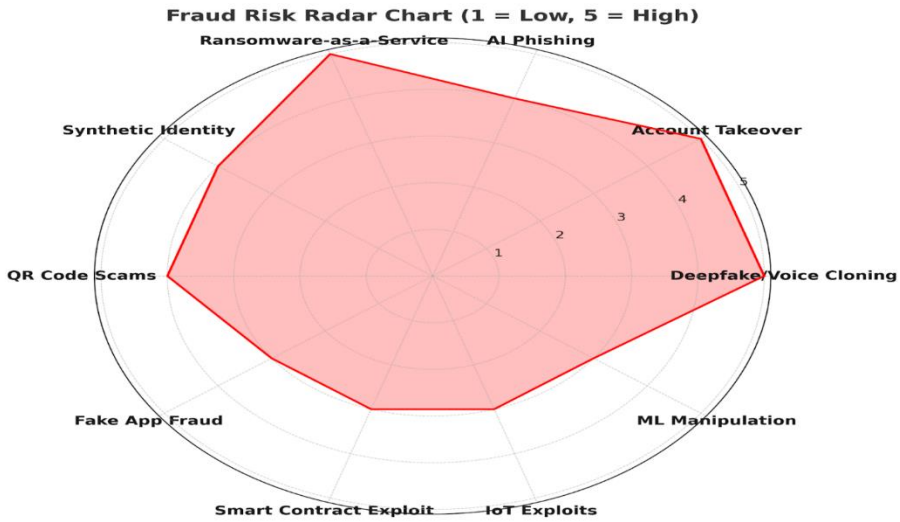

Fig. 6: Fraud Risk Radar Chart of Emerging Digital and Cyber-Enabled Fraud Types.

The Fraud Risk Radar Chart highlights the rising complexity of technology-enabled financial crimes, drawing on intelligence from INTERPOL's IFCACC alerts, PwC's 2023 Global Economic Crime Survey, and ACFE's Emerging Fraud Risks reports. At the highest risk level (5), threats such as deepfake voice impersonation, ransomware-as-a-service (RaaS), and account takeovers mark a shift toward real-time exploitation and the use of anonymized digital infrastructures. Deepfake voice fraud has been used to impersonate executives for unauthorized transfers, while RaaS enables cyber extortion by distributing ready-to-use malware kits to non-technical offenders. Account takeovers through stolen credentials or hijacked sessions compromise both personal and enterprise-level financial security. Close behind are advanced phishing campaigns, synthetic identity fraud, and QR code scams, all exploiting mobile payment systems, social engineering, and digital wallets. RBI data from 2021–2024 shows a steady rise in UPI-related frauds and QR manipulation, disproportionately affecting small businesses and low-awareness users. Lower on the risk scale but still critical are fake app frauds and smart contract exploits targeting unregulated DeFi platforms. These crimes unfold in milliseconds within encrypted or blockchain-based systems, leaving fragmented evidence and challenging conventional audits. Hybrid identity data, manipulated invoices, and interconnected fraud chains—where one attack fuels another—further erode traditional verification methods. This evolving fraudscape demands multidisciplinary countermeasures that merge data-driven analytics, cyber forensics, and advanced investigative techniques to keep pace with its speed, scale, and global reach.

3.4. Guardians of integrity: forensic accountants and the fight against financial crime

In a world increasingly governed by digital transactions and algorithmic decisions, the boundary between legitimate finance and fraud has become dangerously porous. Forensic accountants, experts who combine financial knowledge with meticulous investigation to unearth wrongdoing hidden behind intricate accounting, shell companies, and cyber-enabled schemes, are at the vanguard of preserving financial integrity. They are now essential in negotiating the intricacies of contemporary fraud since their function has changed from traditional audits to comprehensive financial investigation. Forensic accountants have played a crucial role in resolving some of the biggest financial scandals of the past ten years. In India, the ₹13,000 crore PNB–Nirav Modi scandal in 2018 was exposed when forensic experts traced fraudulent Letters of Undertaking and collusion between insiders and external parties, revealing systematic abuse of SWIFT controls. The same year, the IL&FS collapse exposed over ₹91,000 crore in concealed liabilities and opaque intercompany loans, identified through in-depth forensic analysis. Global examples of how financial crimes can go unnoticed until forensic experts step in include the 2020 Wirecard collapse, which involved manufactured subsidiaries and fake bank balances, and the 2022 FTX scandal, in which billions of consumer cryptocurrency holdings vanished. In each of these cases, forensic accountants played a pivotal role in decoding revenue fabrication, tracing complex fund flows, and exposing exploitation of digital loopholes.

Forensic accountants use a variety of specialized instruments to conduct these kinds of investigations. Software like as ACL (Audit Command Language) and IDEA are used in traditional ledger analysis to find hidden patterns, abnormalities, and outliers in large financial datasets. For use in court or law enforcement, visualization technologies like Tableau and Power BI assist in transforming raw data into understandable, interpretable evidence. Programs like FTK (Forensic Toolkit) and EnCase are used to recover deleted data, examine email communications, and identify document-level changes when digital evidence recovery is required. This was essential in exposing the fraudulent transactions that were the root cause of the accounting crisis at Luckin Coffee. Blockchain analysis tools like CipherTrace, Elliptic, and Chainalysis were used to track money transferred between anonymous wallets and shell companies in crypto-related scams like FTX. Similarly, forensic investigators used ownership records, stock exchange data, and offshore filings to investigate claims of stock inflation and opaque related-party arrangements in the Adani–Hindenburg (2023) case. As financial crime becomes more sophisticated, forensic accountants are using cutting-edge and new technologies more and more. Artificial intelligence is used by programs like MindBridge AI and Darktrace for Finance to track financial activity in real time and identify odd trends that could indicate fraud. Natural Language Processing (NLP) algorithms are now being used to scan contracts, emails, and disclosures for signs of misleading intent—essential in detecting discrepancies like those found in the Greensill Capital case. Additionally, blockchain-based forensic explorers are emerging as tools not only for tracking immutable financial data but also for simulating and stress-testing fraud scenarios. Behavioral biometrics—which monitor typing rhythm, login behavior, and device interaction patterns—are being integrated into fraud detection systems to combat threats like mobile wallet impersonation and synthetic identities.

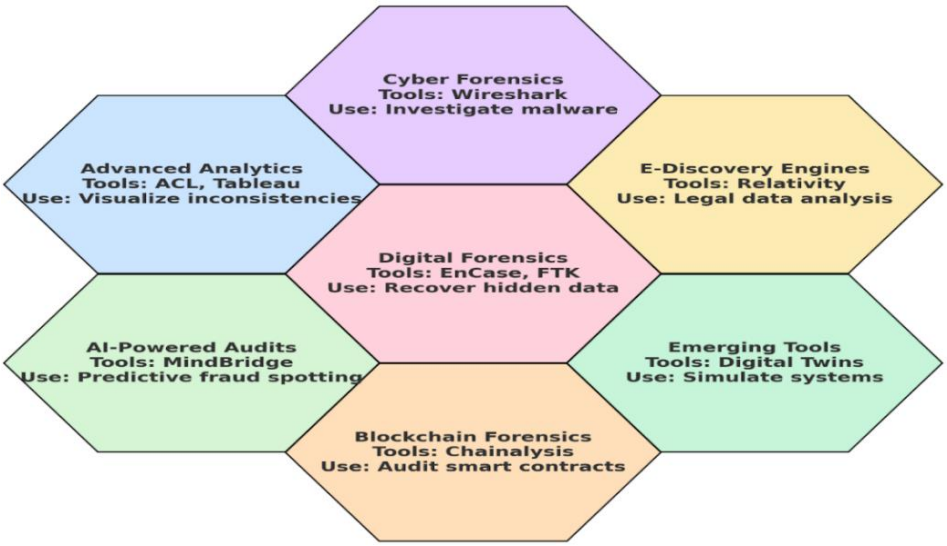

Fig. 7: Strategic Tools and Technologies Used by Forensic Accountants – Hexagonal Grid.

This expanding toolkit reflects the need for forensic accountants to operate not only as financial analysts but as cyber investigators and data scientists. These days, they are involved in court proceedings, mergers and acquisitions, internal control designs, and insolvency investigations. They are also essential in spotting systemic problems and preventing further misconduct because of their advisory and risk assessment responsibilities. In order to provide a globally coordinated response to financial crime, organizations like ACFE, ICAI, ICAEW, AICPA, CIMA, and others in countries including South Africa, the US, the UK, and India are providing professionals with certificates like CFE, CFF, and FAFD. While there are different professional institutes or organizations under which forensic accountant professionals are made to perform various duties relating to combating financial fraud in books & accounts. An illustrative list of these organisations can be defined as under:

Region	Organization	Certification / Focus
Australia	CPA Australia	Forensic Module
Australia	ICFA	CrFA
Canada	CAFI	Membership Programs
Canada	CPA Canada	IFA
Global	ACFE	CFE
Global	IIA	CIA
Global	IAFA	Cr.FA
India	ICAI	FAFD
India	ACFAP	CFAP
India	IIFA	Courses
Malaysia	MIA	Forensic Modules
Nigeria	IFAN	IFAN Certs
South Africa	SAICA	Electives
South Africa	ACFE SA Chapter	CFE
UAE	ACFE UAE Chapter	Arabic CFE
UK	ICAEW	Forensic Accreditation
UK	CIMA	Forensic Training
USA	AICPA	CFF
USA	NAFA	Training Resources

Regions
Global
USA
UK
Canada
Australia
India
South Africa
Nigeria
Malaysia
UAE

Fig. 8: Professional Organizations and Certification Bodies for Forensic Accounting Professionals Worldwide.

The obstacles that lie ahead are tremendous, though. In order to evade traditional detection methods, modern fraud uses artificial intelligence (AI), spoofing communications, creating false identities, and manipulating QR codes. Credential theft brought on by phishing allows account takeovers, which in turn make it easier to launder money through DeFi platforms. Often, these attacks are piled and combined. This webbed structure of fraud, often crossing jurisdictions and technical infrastructures, demands a new investigative approach. Traditional forensic models that treat fraud as discrete events are no longer adequate. Today's forensic accountants must decode real-time, AI-orchestrated deception that leaves minimal audit trails and thrives on system fragmentation. Looking ahead, the profession faces a critical inflection point. The field of forensic accounting needs to change from a reactive post-fraud investigation strategy to a proactive, intelligence-driven one. Cross-border intelligence sharing, real-time surveillance systems, and integration with RegTech will become essential. In addition to providing a visual depiction of the threat, the radar chart that highlights frontier fraud risks—from deepfakes and synthetic identities to smart contract exploits—also acts as a call to action. The trust of international financial systems may be permanently jeopardized if forensic accountants, regulators, and institutions are unable to keep up with the speed and complexity of fraudsters. The speed and effectiveness of forensic accounting's adaptation will determine the future of financial integrity in this arms race between deception and detection.

3.5. India's forensic frontier: progress, gaps, and the road ahead

India's battle against financial fraud is at a critical crossroads—marked by both progress and persistent vulnerabilities. As the financial system becomes more digitized and interconnected, fraud schemes have grown more complex, high-value, and tech-driven. In FY25, reported bank frauds surged to ₹36,014 crore, nearly triple the previous year's losses, despite fewer overall cases—highlighting a shift toward larger, more sophisticated crimes. Public Sector Banks remain disproportionately impacted, while procurement fraud and cybercrime continue to rise sharply. On the positive side, forensic accounting is gaining prominence, supported by digital tools, tighter regulatory oversight, FATF compliance efforts, and expanding training programs. However, India still lacks a cohesive forensic and legal framework, and investigations are often reactive and delayed. The shortage of skilled forensic professionals, overlapping jurisdictions, and underutilization of AI further limit proactive fraud detection. These dynamics expose the systemic cracks even as reform efforts accelerate. India's evolving fraud landscape demands faster institutional response, smarter analytics, and deeper integration of forensic audits into mainstream financial governance.

Examining the well-known scams that have put India's institutional resilience to the test is essential to gaining a greater understanding of the country's forensic frontier. India has seen a variety of financial scams, from massive Ponzi schemes to stock manipulation, which have revealed serious weaknesses in oversight and governance. The table below chronicles some of the most significant financial frauds in recent Indian history, spanning from the Saradha Chit Fund scandal in the 2010s to the more recent allegations involving Jai Corporation Limited and Anil Ambani's Reliance Communications in 2025. These cases highlight how financial crime in India is changing and how urgently we need to update our forensic response framework to make it more deterrent-driven, predictive, and flexible.

Table 2: Major Financial Frauds in India During the Last Decades (2010–2025)

Name of Fraud	Year	Nature of Fraud	Magnitude of Fraud	Parties Affected
Jai Corporation Limited	2025	Alleged ₹22,434 crore fraud	₹22,434 crore	Likely banks or financial institutions
Anil Ambani's SBI Fraud Case	2025	Classified as 'fraud' by SBI, potential bank fraud amounting to over ₹20,000 crore, according to India Today, Reliance Communications	Potentially over ₹20,000 crore	State Bank of India, potentially other lenders, and Reliance Communications
Adani Group Scandal	2023	Allegations of stock manipulation, accounting fraud, and bribery	Varies, which led to a significant decline in share prices	Investors, the stock market, the company's reputation, and stakeholders
Yes Bank Scandal	2020	Irregularities and fraudulent activities, including granting loans for bribes	₹600 crores given by DHFL	Yes Bank itself, investors, and the Indian banking sector
DHFL Scam	2019	Fraudulent transactions, financial mismanagement, loan default, and alleged adverse takeover	Over ₹34,000 crores ($13.93 billion)	Investors, lenders (including banks), and the company itself
CG Power and Industrial Solutions	2019	Overstatement of profits, understatement of liabilities, siphoning off funds	Not explicitly stated, but led to significant financial irregularities	Company, investors, and stakeholders, according to Legal Mantra
Punjab & Maharashtra Co-operative (PMC) Bank Scam	2019	Creation of fictitious accounts to hide loans made to the Housing Development and Infrastructure Limited (HDIL) group, which were not repaid	Over ₹6,500 crores ($900 million)	PMC Bank depositors and the bank itself
Nirav Modi-PNB Scam	2018	Fraudulent issuance of Letters of Undertaking (LoUs) from PNB to obtain funds without collateral	Over $2 billion (₹13,000 crore)	Punjab National Bank, other banks involved, and the Indian banking sector
IL&FS Financial Scandal	2018	Concealment of financial stress and defaults on debt obligations, liquidity crisis	Over $12 billion	IL&FS itself, investors, creditors, and the Indian financial system
Vijay Mallya Loan Default Scam	2012-2016	Financial mismanagement and loan default, according to The420.in	Around ₹10,000 crore ($500 crores)	Banks (including SBI), Kingfisher Airlines employees, and the company itself
Saradha Chit Fund Fraud	2010s	Ponzi scheme, collecting money from investors with promises of high returns, using funds from new investors to pay older ones	Over ₹2,500 crore	Millions of investors in West Bengal and Assam

Summary of significant Indian financial frauds highlighting their year, nature, magnitude, and affected parties, reflecting the growing complexity and scale of economic crimes in the country.

The table's compilation of financial frauds is a sobering reminder of how varied and enduring white-collar crime is in India. Sorted chronologically from the most current to the earliest cases, it shows the increasing complexity and systemic consequences of financial wrongdoing in addition to their growing magnitude. One of the most evident patterns is the size of the losses, with some frauds exceeding the ₹10,000 crore mark. As demonstrated by the 2025 cases involving Jai Corporation Limited and Anil Ambani's SBI Fraud Case alone, fraudsters are still exploiting institutional flaws and regulatory shortcomings at startling rates. Notably, public sector organizations like SBI and PNB are still affected in spite of earlier lessons learned.

The nature of fraud has also evolved—from basic loan defaults and misrepresentation of liabilities to intricate scams involving stock manipulation, fictitious accounts, and cyber-fraud tactics. While older scams like the Saradha Chit Fund fraud were rooted in traditional Ponzi models, newer ones, such as the Adani Group allegations and DHFL scam, involve layered corporate structures and financial misreporting, requiring advanced forensic scrutiny. From huge national banks and corporate stakeholders to small investors in regional chit funds, the parties impacted are diverse. The table serves as a call to action and a mirror of India's present vulnerabilities, in addition to listing past occurrences. The recurrence of trends over time indicates that fraud innovation has outpaced reforms.

The methods used in financial frauds across India reveal how some schemes have persisted over decades while others have evolved to match the sophistication of modern financial systems. Traditional fraud techniques, such as fraudulent discounting or kite flying, involved exploiting delays in the banking system to draw unauthorized credit. Likewise, companies often engaged in stock manipulation and loan fraud by inflating asset values or secretly disposing of collateral, actions explicitly noted by the RBI as common offenses. Diversion of funds, embezzlement, and financial misstatement have also been mainstays—ranging from siphoning money away from core operations to falsifying books through ghost employees, fake expenses, or premature revenue recognition. Corruption and insider trading further compound the issue, with illegal payments and confidential information routinely abused for personal gain. These legacy tactics remain the foundation for many large-scale frauds even today. When viewed alongside the modern scams in the table, these traditional methods show how deep-rooted and adaptable financial crime in India is—constantly shifting in form but consistent in objective: exploiting systemic gaps for personal or corporate profit.

The onset of the digital age has not only modernized India's financial landscape but also opened new frontiers for fraud. With the widespread use of online transactions and fintech platforms, digital payment fraud has surged, ranging from credit card scams and phishing schemes to fake job offers targeting unsuspecting users. FY24 saw a sharp spike in such fraud cases, with Grip Invest noting card and internet fraud as major contributors. Alongside this, cybercrime has emerged as a serious threat, with data breaches, malware attacks, and the theft of intellectual property affecting both corporations and consumers. Fraudsters are also exploiting vulnerabilities in digital platforms, a trend intensified during the pandemic's push toward online services. Even legacy scams like billing and procurement fraud have evolved, now leveraging digital tools to fabricate invoices, create phantom vendors, and reroute company funds. These developments reflect not just a change in tactics, but a growing sophistication that mirrors the pace of India's digital transformation—revealing that as technology advances, so too does the ambition and adaptability of financial fraud.

Status of Forensic Accounting in India

Forensic accounting in India, though a relatively nascent discipline, is experiencing rapid growth and gaining increasing recognition due to several interconnected factors. Inspired by global trends and significant financial scandals, the field has moved beyond its initial niche status to become a vital component of corporate governance and fraud deterrence. The dominance of the "Big Four" consulting firms (Deloitte, KPMG, PricewaterhouseCoopers, and EY) in the Indian market, according to ResearchGate, reflects the growing corporate demand for specialized fraud investigation and litigation support services, even though there were initially few chartered accounting firms that focused on this area. Growing awareness of the terrible effects of financial crimes on business reputations, investor confidence, and the economy as a whole is another factor driving this demand.

The Institute of Chartered Accountants of India's (ICAI) proactive engagement is a significant milestone in bolstering the forensic accounting scene. Acknowledging the rising tide of financial and cyber frauds, the ICAI's Committee on Information Technology initiated a Certificate Course on Forensic Accounting and Fraud Detection (FAFD) for practicing CAs. Professionals who complete this course will have the investigative skills they need to identify fraud, calculate damages, and offer vital litigation support by applying accounting and auditing concepts. The ICAI has also actively worked with law enforcement and regulatory agencies like the Enforcement Directorate and the Serious Fraud Investigation Office (SFIO) to enhance its investigative capabilities and digital resilience. Furthermore, the Forensic Accounting and Investigation Standards (FAIS), which were introduced by the ICAI on July 1, 2023, provide a clear framework for experts performing forensic engagements, raising the standard and legitimacy of their work.

The intricacy of financial crimes and the growing demand for fraud detection experts have put forensic accounting at the center of India's academic and professional landscape. The "Forensic Accounting Courses in India – A Landscape Overview" diagram offers a thorough overview of the many educational options offered in the nation. It highlights a range of programs from highly regarded Indian colleges and institutes' specialized postgraduate degrees and certificates to globally renowned certifications like the Certified Fraud Examiner (CFE). This overview summarizes the variety of educational options designed to provide aspiring forensic accountants with the conceptual knowledge and hands-on skills necessary to tackle intricate financial frauds. By categorizing these courses into certificates, diplomas, postgraduate degrees, and international certifications, the figure offers crucial insights into the availability and structure of forensic accounting education across India.

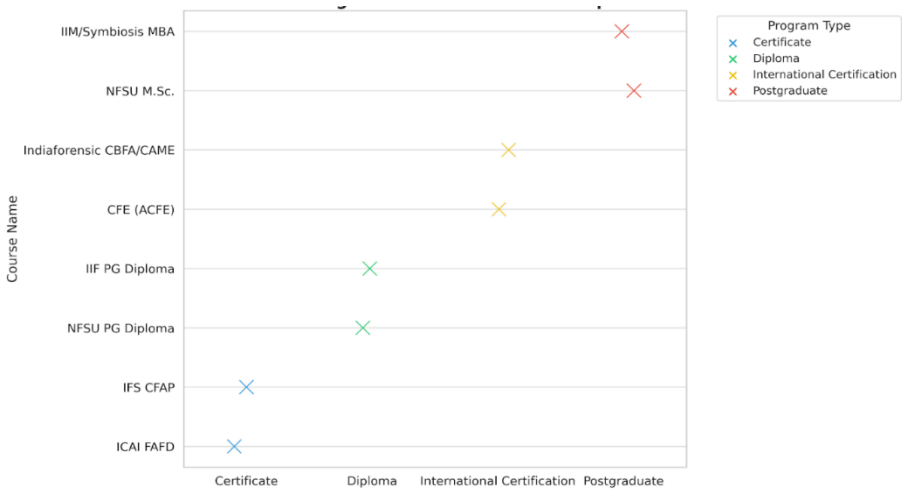

Fig. 9: Landscape Overview of Forensic Accounting Courses and Certifications in India.

This chart provides a well-organized summary of the many educational options for prospective forensic accountants in India, broken down by certification level. Certificate courses at the foundational level, including India Forensic's short-term modules and ICAI's Forensic Accounting and Fraud Detection (FAFD), are intended to give professionals the fundamental investigative abilities and hands-on experience in digital fraud analysis. Moving further, more in-depth instruction is offered via diploma programs from organizations such as the Indian Institute of Finance and the National Forensic Sciences University (NFSU), which frequently combine the legal, technological, and financial facets of fraud examination. Professionals seeking academic rigor and leadership positions in the sector are catered to by postgraduate degrees, such as the M.Sc. in Forensic Accounting or MBA concentrations in financial crime. International Certifications like the Certified Fraud Examiner (CFE), which is widely acknowledged for its legitimacy and extensive reach in fraud prevention, detection, and investigation, are also highlighted in the diagram. These programs collectively demonstrate the rising need for qualified forensic specialists in India's quickly evolving financial sector, where interdisciplinary knowledge and tech-enabled competence are essential in the fight against complex financial crimes.

4. Conclusion

The trajectory of financial fraud prevention will increasingly depend on how quickly institutions can adapt to emerging threats rather than on lessons from past crises. Modern fraud is no longer confined to isolated incidents; it operates through adaptive, cross-border networks that exploit governance gaps, technological vulnerabilities, and regulatory blind spots. This evolution demands a shift from reactive investigations to intelligence-led, preventive strategies. Forensic accounting must position itself as a core, forward-looking pillar of financial governance, integrating traditional investigative expertise with advanced capabilities in blockchain tracing, behavioural analytics, and real-time surveillance. Its role now extends beyond uncovering fraud after the fact—it must anticipate risks, map systemic weaknesses, and neutralize threats before they mature. In India, the convergence of digital transformation, regulatory tightening, and institutional initiatives—particularly from ICAI and academic partnerships—provides a strong foundation for such progress. Yet, persistent gaps remain: a shortage of skilled specialists, delays in legal processes, and the absence of a unified forensic framework continue to limit impact. Addressing these weaknesses will require embedding forensic practices into corporate governance structures, enhancing inter-agency collaboration, and fostering deeper public–private–academic partnerships. Crucially, investment in capacity building and the adoption of cutting-edge tools must be accelerated to match the pace of fraud innovation. If these measures are pursued decisively, forensic accounting in India will not only strengthen fraud detection and prevention but also reinforce trust, transparency, and resilience across the financial ecosystem. In a world where fraud is engineered to evade detection, only a proactive, multidisciplinary, and technology-enabled approach can safeguard institutional integrity and protect economic stability.

During the preparation of this work, the author(s) used ChatGPT and Grammarly in order to refine the language. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the published article.

References

[1] Advanced Analytics. Library Progress International, Vol.44 No.3, Jul-Dec 2024: P. 22014-22024

[2] Adejumo, Adetunji & Ogburie, Chinonso. (2025). Forensic accounting in financial fraud detection: Trends and challenges. International Journal of Science and Research Archive. 14. 1219-1232. https://doi.org/10.30574/ijsra.2025.14.3.0815.

[3] Akinbowale OE, Mashigo P, Zerihun MF. The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry. Cogent Bus Manag. 2023. https://doi.org/10.1080/23311975.2022.2163560.

[4] Alabdullah, T. T. Y. (2014). Are forensic accountants needed in the Middle East?. International Journal of Business and Management, 9(1), 101–106. https://doi.org/10.5539/ijbm.v9n1p101.

[5] Alharasis, E.E., Haddad, H., Alhadab, M., Shehadeh, M. and Hasan, E.F., 2023. Integrating forensic accounting in education and practices to detect and prevent fraud and misstatement: case study of Jordanian public sector. Journal of Financial Reporting and Accounting. https://doi.org/10.1108/JFRA-04-2023-0177.

[6] Almeida, A. (2024, July 11). Satyam Scam- Case study of India's Biggest Corporate Fraud. Retrieved August 10, 2024, from tradebrains: https://tradebrains.in/satyam-scam/

[7] Al-Shurafat, H., Sands, J., Jones, G. & Beattie, C., (2024) "Obstacles Facing the Development of Forensic Accounting Curricula within Australian Universities: Exploring Perspectives of Practitioners and Educators", *Australasian Accounting, Business and Finance Journal* 18(2), 188-195. https://doi.org/10.14453/aabfj.v18i2.12.

[8] Altaf, O. M. (2025). *Forensic accounting: Uncovering fraud with advanced analytics. Center for Management Science Research*, 3(3). ISSN 3006-5291, 3006-5283.

[9] Anghel, G., & Poenaru, C.-E. (2023a). Forensic Accounting, a Tool for Detecting and Preventing the Economic Fraud. Valahian Journal of Economic Studies, 14(2), 87–100. https://doi.org/10.2478/vjes-2023-0018.

[10] Baesens, Bart & Van Vlasselaer, Véronique & Verbeke, Wouter. (2015). Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection. https://onlinelibrary.wiley.com/doi/book/10.1002/9781119146841. https://doi.org/10.1002/9781119146841.

[11] Baljinder Kaur & Kiran Sood & Simon Grima, 2022. "A systematic review on forensic accounting and its contribution towards fraud detection and prevention," Journal of Financial Regulation and Compliance, Emerald Group Publishing Limited, vol. 31(1), pages 60-95, June. https://doi.org/10.1108/JFRC-02-2022-0015.

[12] Bhasin, Madan Lal, Forensic Accounting: A New Paradigm for Niche Consulting (2007). The Chartered Accountant, January 2007, Available at SSRN: https://ssrn.com/abstract=2703647.

[13] Black, W. K. (2010). The great American stickup: How Reagan Republicans and Clinton Democrats enriched Wall Street while mugging Main Street. https://www.abebooks.com/9781568584348/Great-American-Stickup-Reagan-Republicans-1568584342/plp.

[14] Blanco B, Dhole S, Gul FA. Financial statement comparability and accounting fraud. J Bus Financ Acc. 2023;50(7–8):1166–205. https://doi.org/10.1111/jbfa.12652.

[15] Botes, V. and Saadeh, A. (2018), "Exploring evidence to develop a nomenclature for forensic accounting", Pacific Accounting Review, Vol. 30 No. 2, pp. 135-154. https://doi.org/10.1108/PAR-12-2016-0117.

[16] https://doi.org/10.1108/PAR-12-2016-0117

[17] Capraş, I.L., Achim, M.V. (2023). An Overview of Forensic Accounting and Its Effectiveness in the Detection and Prevention of Fraud. In: Achim, M.V. (eds) Economic and Financial Crime, Sustainability and Good Governance. Contributions to Finance and Accounting. Springer, Cham. https://doi.org/10.1007/978-3-031-34082-6_13.

[18] Chetry, P., Tiwari, R. K., Baxi, J., & Shekar, M. C. (2025). Student Perspectives on Forensic Accounting in Indian Higher Education. Vision, 0(0). https://doi.org/10.1177/09722629241307135.

[19] Chiu, Victoria & Liu, Qi & Muehlmann, Brigitte & Baldwin, Amelia Annette, 2019. "A bibliometric analysis of accounting information systems journals and their emerging technologies contributions," International Journal of Accounting Information Systems, Elsevier, vol. 32(C), pages 24-43. https://doi.org/10.1016/j.accinf.2018.11.003.

[20] Chung, E. (2021, August 27). Luckin Cofee Accounting Fraud. Retrieved August 13, 2024, from sevenpillarsinstitute: https://sevenpillarsinstitute.org/case-study-luckin-coffee-accounting-fraud/.

[21] Commission, S. a. (2021, September 3). SEC Charges the Kraft Heinz Company and Two Former Executives for Engaging in Years long Accounting Scheme. Retrieved August 13, 2024, from sec.gov: https://www.sec.gov/newsroom/press-releases/2021-174.

[22] Crumbley D. L., Heitger L. E. & Smith G. S. (2009). Forensic and investigative accounting. Chicago: CCH. https://opac.ueab.ac.ke/cgi-bin/koha/opac-detail.pl?biblionumber=17971&shelfbrowse_itemnumber=41646.

[23] D. Vijayalakshmi , Jala Jeevan (2024) Forensic Accounting: Uncovering Fraud with Advanced Analytics. Library Progress International, Vol.44 No.3, Jul-Dec 2024: P. 22014-22024

[24] Deb, S. (2022, May 12). All you need to Know About the Nirav Modi scam. Retrieved August 10, 2024, from ipleaders: https://blog.ipleaders.in/all-you-need-to-know-about-the-nirav-modi-scam/.

[25] DiGabriele, James A. and Huber, Wm. Dennis, Topics and Methods in Forensic Accounting Research (December 1, 2013). Accounting Research Journal, 28(1), 98-114., Available at SSRN: https://ssrn.com/abstract=2361944 or https://doi.org/10.2139/ssrn.2361944.

[26] Ellili N, Nobanee H, Haddad A, Alodat AY, AlShalloudi M. Emerging trends in forensic accounting research: bridging research gaps and prioritizing new frontiers. Journal of Economic Criminology,Volume 4,2024,100065,ISSN 2949-7914,. https://doi.org/10.1016/j.jeconc.2024.100065.

[27] Ellili, N., Nobanee, H., Alodat, A.Y. et al. Mapping marine insurance: a bibliometric review: a taxonomical study using bibliometric visualization and systematic analysis. J Financ Serv Mark 29, 745–762 (2024). https://doi.org/10.1057/s41264-023-00232-w.

[28] Elumilade, O. O., Ogundeji, I. A., Achumie, G. O., Omokhoa, H. E., & Omowole, B. M. (2021). Enhancing fraud detection and forensic auditing through data-driven techniques for financial integrity and security. Journal of Advanced Education and Sciences, 1(2), 55–63. https://doi.org/10.54660/.JAES.2021.1.2.55-63.

[29] Faizah, Y. N., Musyarofah, S., & Anggono, A. (2020, December). Fraud detection in healthcare organization: A bibliometric analysis approach. In International Colloquium Forensics Accounting and Governance (ICFAG) (Vol. 1, No. 1, pp. 96-103). https://conference.trunojoyo.ac.id/pub/icfag/article/view/15.

[30] George E. Curtis; Legal and Regulatory Environments and Ethics: Essential Components of a Fraud and Forensic Accounting Curriculum. Issues in Accounting Education 1 November 2008; 23 (4): 535–543. https://doi.org/10.2308/iace.2008.23.4.535.

[31] Goel, Sunita & Gangolly, Jagdish & Faerman, Sue. (2010). Can Linguistic Predictors Detect Fraudulent Financial Filings?. Journal of Emerging Technologies in Accounting. 7. 10.2308/jeta.2010.7.1.25. https://doi.org/10.2308/jeta.2010.7.1.25.

[32] Gray, G. L., & Debreceny, R. S. (2014, December). A taxonomy to guide research on the application of data mining to fraud detection in financial statement audits. International Journal of Accounting Information Systems, 15,No. 4:pp 357-380. https://doi.org/10.1016/j.accinf.2014.05.006.

[33] Guellim, N., Yami, N., Freihat, A.F. et al. Evaluating the perceived value of forensic accounting: a systematic review method. Discov Sustain 5, 351 (2024). https://doi.org/10.1007/s43621-024-00431-y.

[34] Honigsberg, Colleen, Forensic Accounting (October 2020). Annual Review of Law and Social Science, Vol. 16, pp. 147-164, 2020, Available at SSRN: https://ssrn.com/abstract=3711272 or https://doi.org/10.1146/annurev-lawsocsci-020320-022159.

[35] Imoniana, J. O., Antunes, M. T. P., & Formigoni, H. (2013). The Forensic Accounting and Corporate Fraud. Journal of Information Systems and Technology Management, 10(1), 119–144. https://doi.org/10.4301/s1807-17752013000100007.

[36] Institute of Chartered Accountants of India. (2020). Forensic Accounting and Investigation Standards. ICAI.

[37] Ismail, S., Al-zoubi, A. B., Dahmash, F. N., Ahmad, S., & Mahmoud, M. (2022). A Review on Forensic Accounting Profession and Education: Global Context. Preprints. https://doi.org/10.20944/preprints202211.0369.v1.

[38] Jain, D.E. and Lamba, J. (2020) "FORENSIC ACCOUNTING: A WAY TO FIGHT, DETER AND DETECT FRAUD", *IARS' International Research Journal*, 10(1). https://doi.org/10.51611/iars.irj.v10i1.2020.106.

[39] https://www.redalyc.org/journal/6638/663873428002/html.

[40] Jain, y. (2022, May 19). Sebi vs Urja Global: The strange Case of a non-existent element and a market scam. Retrieved August 13, 2024, from cnbctv18: www.cnbctv18.com/market/stocks/sebi-zacobite-scam-urja-global-nippon-shinyaku-65-million-dollars-13533672.htm.

[41] Jamil, A.H., Mohd Sanusi, Z., Yaacob, N.M., Mat Isa, Y. and Tarjo, T. (2022), "The Covid-19 impact on financial crime and regulatory compliance in Malaysia", Journal of Financial Crime, Vol. 29 No. 2, pp. 491-505. https://doi.org/10.1108/JFC-05-2021-0107.

[42] JOFRE, M. (July 2017). Fighting Accounting Fraud Through Forensic Analytics. Sydney: University of Sydney. Journal of Accounting and Taxation, Vol. 12 No. 4, pp. 118-125.

[43] Joseph, F. A., Okike, B. M., & Yoko, V. E. (2016). The impact of forensic accounting in fraud detection and prevention evidence from Nigerian public sector. International Journal of Business Marketing and Management, 1(5), 34-40.

[44] Kaminski, K. A., Wetzel, T. S., & Guan, L. (2004). Can financial ratios detect fraudulent financial reporting? Managerial Auditing Journal, 19(1), 15–28. https://doi.org/10.1108/02686900410509802.

[45] Madan Lal Bhasin , 2016. Contribution of Forensic Accounting to Corporate Governance: An Exploratory Study of an Asian Country. Retrieved from http://medwelljournals.com/abstract/?doi=ibm.2016.479.492. https://doi.org/10.2139/ssrn.2676488.

[46] Mehta, Kamakshi & Mittal, Prabhat & Gu, Pa & Tandon, J.. (2022). Analyzing the Impact of Forensic Accounting in the Detection of Financial Fraud: The Mediating Role of Artificial Intelligence.

[47] Mittal, Prabhat & Kaur, Amrita & Gu, Pa. (2021). The Mediating Role of Big Data to Influence Practitioners to Use Forensic Accounting for Fraud Detection. European Journal of Business Science and Technology. 7. 47-58. https://doi.org/10.11118/ejobsat.2021.009.

[48] Mousavi, M., Zimon, G., Salehi, M., & Stępnicka, N. (2022). The Effect of Corporate Governance Structure on Fraud and Money Laundering. Risks, 10(9), 176. https://doi.org/10.3390/risks10090176.

[49] Nader and El-Mousawi, Hasan and Younis, Joumana (2020): Role of Forensic Accounting in Curbing Creative Accounting Practices—An Empirical Study. Published in: scholink inc, Vol. 5, No. 3 (June 2020): pp. 28-46. https://doi.org/10.22158/rem.v5n3p28.

[50] Nasrallah, N. H., El Khoury, R., & Harb, E. (2022). Forensic accounting in a digital environment: a new proposed model. In Handbook of research on the significance of forensic accounting techniques in corporate governance (pp. 128-149). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-7998-8754-6.ch007.

[51] Nickell, Erin and Schwebke, Jason and Goldwater, Paul, an introductory audit data analytics case study: Using Microsoft Power BI and Benford's Law to detect accounting irregularities (September 1, 2023). Journal of Accounting Education, Forthcoming, Available at SSRN: https://ssrn.com/abstract=4653324. https://doi.org/10.1016/j.jaccedu.2023.100855.

[52] Ocansey, E. O. N. D. (2017). Forensic Accounting and the Combating of Economic and Financial Crimes in Ghana. European Scientific Journal, ESJ, 13(31), 379. https://doi.org/10.19044/esj.2017.v13n31p379.

[53] Okpako, A. E. P., & Atube, E. N. (2013). The impact of forensic accounting on fraud detection. European Journal of Business and Management, Vol.5, No.26, 2013, 61-70. ISSN (Paper)2222-1905 ISSN (Online)2222-2839. https://www.iiste.org/Journals/index.php/EJBM/article/view/8063/8602.

[54] Oraby SA. The forensic accounting and the financial fraud detection: the case of Saudi Arabia. Glob J Arts Hum Soc Sci ISSN. 2023;2583:2034. https://doi.org/10.4236/ojacct.2024.133008.

[55] Ozili PK. Forensic accounting research around the world. Journal of Financial Reporting and Accounting. 2023. https://doi.org/10.1108/JFRA-02-2023-0106.

[56] Ozili, Peterson K, Forensic Accounting Theory (January 1, 2020). Finance, Insurance and Risk Management Theory and Practices, Vol. 1, Emerald, 2020, Available at SSRN: https://ssrn.com/abstract=3525672.

[57] Özkul, F.U., Pamukçu, A. (2012). Fraud Detection and Forensic Accounting. In: Çaliyurt, K., Idowu, S. (eds) Emerging Fraud. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-20826-3_2.
[58] Ratzinger-Sakel, N. V. S., & Tiedemann, T. (2022). Fraud in accounting and audit research (1926–2019) – a bibliometric analysis. Accounting History Review, 32(2–3), 97–143. https://doi.org/10.1080/21552851.2022.2143827.
[59] Reuters. (2025, May 8). Forensic review finds India's IndusInd Bank executives traded shares before accounting disclosure. https://www.reuters.com/sustainability/boards-policy-regulation/forensic-review-found-indias-indusind-bank-executives-traded-shares-before-2025-05-08/.
[60] Sánchez-Aguayo, M., Urquiza-Aguiar, L., & Estrada-Jiménez, J. (2021). Fraud Detection Using the Fraud Triangle Theory and Data Mining Techniques: A Literature Review. Computers, 10(10), 121. https://doi.org/10.3390/computers10100121.
[61] Schipper, K. (1989) Commentary on Earnings Management. Accounting Horizons, 3, 91-102. Open Journal of Business and Management, Vol.7 No.1. https://www.scirp.org/reference/referencespapers?referenceid=2440010
[62] Shah, Manoj. (2014). Practical Approach for Requirement of Forensic Accounting in India. 2. 32-37. Midas Touch International Journal of Commerce, Management and Technology Volume 2, No. 10, October- 2014, ISSN: 2320 -778; https://www.researchgate.net/publication/355162436_Practical_Approach_for_Requirement_of_Forensic_Accounting_in_India.
[63] Shalhoob, H., Halawani, B., Alharbi, M., & Babiker, I. (2024). The Impact of Big Data Analytics on The Detection of Errors and Fraud in Accounting Processes. Revista De Gestão Social E Ambiental, 18(1), e06115. https://doi.org/10.24857/rgsa.v18n1-121.
[64] Stephen Owusu Afriyie & Michael Owusu Akomeah & Gertrude Amoakohene & Benjamin Chris Ampimah & Chosniel Elikem Ocloo & Michael Owusu Kyei, 2023. "Forensic Accounting: A Novel Paradigm and Relevant Knowledge in Fraud Detection and Prevention," International Journal of Public Administration, Taylor & Francis Journals, vol. 46(9), pages 615-624, July. https://doi.org/10.1080/01900692.2021.2009855.
[65] Wadhwa, L. & Pal, Vikash. (2012). Forensic accounting and fraud examination in India. 7. 2006-2009. https://www.researchgate.net/publication/298171818_Forensic_accounting_and_fraud_examination_in_India.
[66] Yadav, S., & Yadav, S. (2013). Forensic Accounting: A New Dynamic Approach to Investigate Fraud Cases. EXCEL International Journal of Multidisciplinary management Studies, 3 (7). http://www.zenithresearch.org.in/images/stories/pdf/2013/JULY/EIJMMS/1_EIJMMS_VOL3_ISSUE7_JULY2013.pdf.