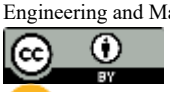
Toward an Integrated Digital-Age Framework for Forensic Accounting and Fraud Detection: Bridging Theory, Technology, and Practice

PREETHA P

Assistant Professor, Department of Commerce

PK Das Liberal College of Arts and Science, Kerala, India

How to Cite this Article:
P, P. (2026). Toward an Integrated Digital-Age Framework for Forensic Accounting and Fraud Detection: Bridging Theory, Technology, and Practice. International Journal of Creative and Open Research in Engineering and Management, 02(6). https://doi.org/10.55041/ijcope.v2i6.219



https://doi.org/ 10.55041/ijcope.v2i6.219

ABSTRACT

The digital age has changed how financial fraud happens. This means forensic accounting needs to change too. This study looks at how forensic accountants and auditors in India use technologies. It aims to understand how they adopt these technologies and to test a framework that combines accounting, criminology and technology.The study uses a mix of interviews and surveys. It finds that awareness, skills, institutional support and trust in technology are key to adoption. It also finds that technology integration, forensic intelligence and human capital are crucial for fraud detection.However the study identifies a gap in digital skills. Most respondents say they do not have training in AI-driven forensic tools.. Employing a sequential mixed-methods design, the research draws on semi-structured interviews with 30 forensic accounting professionals and a structured questionnaire survey of 210 forensic accountants and auditors across five Indian metropolitan regions Mumbai, Delhi, Bengaluru, Chennai, and Kochi. The qualitative strand reveals four dominant themes shaping technology adoption: awareness and skill readiness, institutional support and infrastructure, regulatory clarity, and professional trust in algorithmic outputs. The quantitative strand, analysed through Partial Least Squares Structural Equation Modelling (PLS-SEM), confirms that technological integration capability, forensic intelligence architecture, and human capital development are the three strongest predictors of effective fraud detection performance among Indian forensic professionals. Critically, the study identifies a pronounced digital competency gap as the primary barrier to technology adoption, with 76.2% of survey respondents reporting insufficient training in AI-driven forensic tools. Findings carry significant implications for professional bodies, academic institutions, and policymakers engaged in modernising India's financial crime investigation ecosystem

Keywords: *forensic accounting; fraud detection; technology adoption; artificial intelligence; India; PLS-SEM; digital forensics; mixed methods; integrated framework*

INTRODUCTION

Indias financial sector has changed a lot in the decade. The governments digital economy plan, fintech growth and internet penetration have created opportunities. Also increased financial crimes. High-profile cases like the Punjab National Bank scam and IL&FS collapse have made forensic accounting crucial.
Forensic accounting uses accounting knowledge, investigative skills and legal understanding to examine records. However traditional methods are not enough for digital fraud. Technologies like AI, machine learning, data analytics and blockchain can help.

Forensic accounting, defined as the application of accounting knowledge, investigative skills, and legal understanding to the examination of financial records for use in legal proceedings, has historically relied on manual document scrutiny, ratio-based financial analysis, and practitioner experience. However, the growing complexity of digitally-mediated financial fraud encompassing cyber enabled transaction manipulation, cryptocurrency-facilitated money laundering, algorithmic trading irregularities, and identity fraud at scale has exposed the limitations of these conventional methodologies..

Technologies such as artificial intelligence (AI), machine learning (ML), data analytics platforms, blockchain forensics, and robotic process automation (RPA) have emerged as transformative enablers of fraud detection capability. Yet, despite the theoretical promise of these tools, their systematic adoption within Indian forensic accounting practice remains uneven, poorly understood, and underexplored in the academic literature. This is a critical gap: if practitioners are not effectively deploying available technologies, the potential of India's growing forensic accounting profession to counter financial crime will remain significantly constrained

This paper addresses this gap through an empirical, mixed-methods investigation of technology adoption patterns among forensic accountants and auditors in India. The study is anchored in the development and testing of an Integrated Digital-Age Framework (IDAF) a theoretically grounded model that synthesises criminological theory, accounting theory, and technology adoption research to provide a comprehensive explanatory and prescriptive architecture for digital-age forensic accounting practice. The IDAF is specifically calibrated to the Indian professional, regulatory, and institutional context.

The study is guided by four research questions: (RQ1) What is the current state of digital technology adoption among forensic accountants and auditors in India? (RQ2) What are the principal facilitators of and barriers to technology adoption in Indian forensic accounting practice? (RQ3) How do theoretical constructs from fraud and technology adoption theory predict the effectiveness of digitally-enabled fraud detection? (RQ4) What framework can integrate theory, technology, and practice to guide Indian forensic accounting in the digital age?.

THEORETICAL BACKGROUND AND LITERATURE REVIEW

2.1 Theoretical Foundations

2.1.1 The Fraud Triangle and Fraud Diamond

The fraud triangle by Cressey (1953) says three conditions must be present for occupational fraud: financial pressure, opportunity and rationalisation.. Hermanson (2004) added capability as a fourth element.The Technology Acceptance Model (TAM) by Davis (1989) says people adopt technology if they think it is useful and easy to use. Venkatesh et al.s (2003) Unified Theory of Acceptance and Use of Technology (UTAUT) adds influence, facilitating conditions and effort expectancy.Institutional theory by Meyer and Rowan (1977) highlights pressures, professional expectations and mimetic tendencies in shaping organisational behaviour.

Wolfe and Hermanson (2004) extended the triangle to the fraud diamond by introducing a fourth element: capability, capturing the observation that many individuals face pressure and opportunity yet lack the technical competence, positional authority, or psychological disposition to execute fraud successfully. In digitally complex organisational environments, capability assumes new dimensions including programming literacy, knowledge of system architectures, and understanding of cryptographic mechanisms that are directly relevant to the emerging profile of digital financial fraud perpetrators in India.

From a technology adoption standpoint, the fraud diamond's opportunity dimension is directly modifiable through forensic technology deployment. AI-driven transaction monitoring systems, for instance, substantially narrow the opportunity space available to would-be fraudsters by enabling real-time, comprehensive

surveillance that no human audit team could replicate. This direct theoretical linkage between technology adoption and fraud opportunity reduction provides a foundational justification for the IDAF's core proposition.

2.1.2 Technology Acceptance Model (TAM) and Extensions

Davis's (1989) Technology Acceptance Model (TAM) provides the primary theoretical lens through which technology adoption behaviour within professional communities is understood. TAM posits that an individual's intention to adopt a new technology is determined by two core perceptions: perceived usefulness (PU) the degree to which the technology is believed to enhance job performance and perceived ease of use (PEOU) the degree to which the technology is believed to require minimal cognitive or physical effort. Within forensic accounting contexts, PU and PEOU emerge as critical determinants of whether practitioners integrate digital tools into their investigative workflows

Venkatesh et al.'s (2003) Unified Theory of Acceptance and Use of Technology (UTAUT) further enriched the adoption literature by identifying social influence, facilitating conditions, and effort expectancy as additional determinants of adoption behaviour constructs of particular relevance within the hierarchically structured, peer-influenced professional culture of Indian accounting and audit practice. The present study draws on both TAM and UTAUT in constructing the IDAF's human capital development pillar.

2.1.3 Institutional Theory

Meyer and Rowan's (1977) institutional theory offers a complementary perspective on technology adoption at the organisational level, highlighting the role of regulatory pressures, normative professional expectations, and mimetic tendencies in shaping organisational behaviour. Within the Indian forensic accounting context, institutional pressures emanating from the Securities and Exchange Board of India (SEBI), the Serious Fraud Investigation Office (SFIO), and the ICAI create powerful normative environments that shape how forensic accounting firms and departments respond to technological change. Organisations experiencing strong coercive institutional pressure. for instance, regulatory mandates for data analytics in audit engagements demonstrate significantly higher technology adoption rates than those operating in less regulated environments.

2.2 Digital Technologies in Forensic Accounting: A Review

*2.2.*1 Artificial Intelligence and Machine Learning

AI and machine learning are used in financial fraud detection. Data analytics and continuous auditing have improved examination efficiency. Blockchain analytics is also used.

Unsupervised approaches, particularly isolation forests, autoencoders, and density-based clustering, have proven especially valuable in detecting novel fraud typologies for which training labels are unavailable, a common challenge in real-world forensic investigation contexts.

Deep learning architectures, including Long Short-Term Memory (LSTM) networks, have enabled the modelling of temporal dependencies within sequential transaction data, substantially improving anomaly detection accuracy in banking and securities contexts. Natural language processing techniques have been applied to extract fraud-relevant signals from financial statement narratives, earnings call transcripts, and audit documentation. The application of these tools within Indian forensic contexts, however, remains nascent, with adoption concentrated among the Big Four accountancy firms and a small number of technologically advanced domestic firms operating in Mumbai and Bengaluru.

2.2.2 Data Analytics and Continuous Auditing

Data analytics platforms including ACL Analytics (now Galvanize), IDEA, and Python/R-based custom analytical environments have significantly enhanced the efficiency and coverage of forensic examination by enabling complete population testing in place of sample-based audit procedures. Continuous auditing frameworks, which leverage automated data extraction, rule-based alert triggers, and exception reporting, enable forensic accountants to maintain ongoing transactional surveillance rather than conducting periodic, retrospective investigations. Research in the Indian context suggests that adoption of data analytics tools is growing rapidly among larger audit firms but remains limited among medium and small practices due to cost barriers and skill shortfalls.

2.2.3 Blockchain Analytics

As cryptocurrency transactions become increasingly implicated in Indian financial crime cases from direct fraud to money laundering and hawala facilitation via digital channels blockchain forensics has emerged as an important and rapidly developing capability area. On-chain analytics tools enable forensic accountants to trace cryptocurrency flows across wallet addresses, identify clustering patterns, and reconstruct transaction histories with forensic-grade auditability. The Enforcement Directorate's increasing engagement with cryptocurrency-linked financial crime investigations reflects the growing operational relevance of blockchain forensics within the Indian financial crime investigation landscape.

2.3 The Indian Forensic Accounting Context: Gaps and Opportunities

India's forensic accounting profession has grown substantially since the enactment of the Companies Act 2013 and subsequent regulatory strengthening of SFIO investigative powers. The ICAI's establishment of a dedicated Forensic Accounting and Investigation Standards (FAIS) framework represents a significant institutional milestone. Yet empirical research specifically examining technology adoption within Indian forensic accounting practice remains strikingly sparse. The existing literature predominantly draws on Western particularly North American and European samples, whose institutional, regulatory, and infrastructural contexts differ substantially from India's. This study directly addresses this lacuna by generating original empirical evidence from Indian forensic accounting professionals.

3. RESEARCH METHODOLOGY

3.1 Research Philosophy and Design

The study uses a mixed-methods design. It includes -structured interviews with 30 forensic accounting professionals and a structured questionnaire survey of 210 forensic accountants and auditors across five Indian metropolitan regions.

This design is particularly appropriate for an emerging research context Indian forensic technology adoption where existing theoretical frameworks require contextual calibration before large-scale quantitative testing.

3.2 Qualitative Phase: Semi-Structured Interviews

Thirty semi-structured interviews were conducted with forensic accounting professionals practising in India, selected through purposive sampling to ensure representation across firm size (Big Four, mid-tier, boutique forensic firms, and solo practitioners), professional designation (Chartered Accountants, Certified Fraud Examiners, Certified Internal Auditors), geographic location (Mumbai, Delhi, Bengaluru, Chennai, and Kochi), and years of experience (ranging from 4 to 31 years). Interviews lasted between 50 and 85 minutes and were conducted via video conferencing. All participants provided written informed consent; interviews were audio-recorded and professionally transcribed.

Thematic analysis following Braun and Clarke's (2006) six-phase framework was employed for qualitative data analysis, encompassing familiarisation, code generation, theme development, theme review, theme definition, and write-up. Member checking was conducted with eight participants to validate theme interpretations. Saturation was assessed iteratively and confirmed at the 26th interview, with the final four interviews yielding no substantively new codes.

3.3 Quantitative Phase: Survey Design and Administration

A structured questionnaire was developed to operationalise the IDAF constructs. The instrument comprised 58 Likert-scale items (1 = Strongly Disagree to 5 = Strongly Agree) measuring five latent constructs: Technological Integration Capability (TIC, 12 items), Forensic Intelligence Architecture (FIA, 11 items), Regulatory Compliance Orientation (RCO, 10 items), Human Capital Development (HCD, 13 items), and Fraud Detection Effectiveness (FDE, 12 items the outcome variable). Instrument development drew on validated scales from prior TAM and UTAUT research, adapted and supplemented with constructs emerging from the qualitative phase.

Face and content validity were established through expert review by five forensic accounting academics and four practitioner reviewers. A pilot study with 28 respondents confirmed item clarity and scale reliability (all Cronbach's alpha > 0.79). The final survey was distributed electronically to members of the ICAI Forensic

Accounting and Investigation Standards Board, the Institute of Internal Auditors India chapter, and professional networks of Certified Fraud Examiners across five cities. Of 520 surveys distributed, 218 were returned, of which 210 were deemed complete and usable (response rate: 40.4%).

3.4 Analytical Approach

Quantitative data were analysed using Partial Least Squares Structural Equation Modelling (PLS-SEM) via SmartPLS 4.0. PLS-SEM was selected over covariance-based SEM given the study's emphasis on predictive accuracy, the composite nature of several constructs, and the moderately sized sample conditions under which PLS-SEM demonstrates superior performance. Reliability and validity were assessed through internal consistency reliability (Cronbach's alpha and composite reliability), convergent validity (average variance extracted, AVE > 0.50), and discriminant validity (Fornell-Larcker criterion and HTMT ratio). Bootstrapping with 5,000 resamples was employed to assess path coefficient significance.

Table 1. Profile of Survey Respondents (N = 210)

Characteristic	Category	n	%
Designation	Chartered Accountant (CA)	89	42.4
	Certified Fraud Examiner (CFE)	54	25.7
	Certified Internal Auditor (CIA)	38	18.1
	Other (CPA, DISA, FCA)	29	13.8
Experience	< 5 years	32	15.2
	5–10 years	71	33.8
	11–20 years	82	39.1
	> 20 years	25	11.9
City	Mumbai	58	27.6
	Delhi / NCR	46	21.9
	Bengaluru	41	19.5
	Chennai	35	16.7
	Kochi	30	14.3
Firm Type	Big Four Affiliate	63	30.0
	Mid-tier / National Firm	78	37.1
	Boutique Forensic Firm	44	21.0
	Independent / Solo Practitioner	25	11.9

4 The Integrated Digital-Age Framework (IDAF)

4.1 Framework Overview

The Integrated Digital-Age Framework (IDAF) is a multi-pillar theoretical and practical architecture designed to guide the adoption and deployment of digital technologies in forensic accounting practice, with specific sensitivity to the Indian professional and institutional context. The IDAF is not conceived as a static prescriptive model but as a dynamic, context-sensitive system whose pillars interact synergistically to produce forensic effectiveness outcomes that exceed what any individual capability domain could achieve in isolation. The framework draws its theoretical grounding from the fraud diamond, TAM/UTAUT, institutional theory, and sociotechnical systems theory.The IDAF comprises four operational pillars and one outcome construct. The

operational pillars are: (1) Technological Integration Capability (TIC), which captures the organisation's ability to deploy and sustain an interoperable portfolio of fraud detection technologies; (2) Forensic Intelligence Architecture (FIA), which addresses the data governance, analytical, and investigative protocols through which raw technological outputs are converted into actionable forensic intelligence; (3) Regulatory Compliance Orientation (RCO), which reflects the organisation's capacity to align technology deployment with India's evolving legal and regulatory requirements; and (4) Human Capital Development (HCD), which encompasses the competency development, training, and professional culture dimensions that determine whether practitioners can realise the potential of available technologies. These four pillars collectively predict the outcome construct, Fraud Detection Effectiveness (FDE).

4.2 Pillar 1: Technological Integration Capability (TIC)

TIC is conceptualised as the organisation's demonstrated capacity to strategically acquire, implement, integrate, and continuously update a coherent portfolio of fraud detection technologies. In the Indian context, TIC is shaped by significant heterogeneity in firm-level technological readiness: while Big Four affiliates and large domestic firms have invested substantially in AI analytics platforms, data extraction tools, and cybersecurity infrastructure, smaller and mid-tier practices frequently operate with outdated software ecosystems and fragmented data environments that limit analytical scope.

TIC encompasses five sub-dimensions in the IDAF: (a) technology portfolio breadth, reflecting the range of deployed forensic tools; (b) system interoperability, reflecting the ability of different tools to share data and analytical outputs; (c) real-time processing capability, enabling continuous rather than periodic fraud surveillance; (d) cybersecurity resilience, protecting the integrity of forensic data and investigation processes; and (e) algorithmic governance, ensuring that AI systems are explainable, auditable, and free from discriminatory bias. TIC directly addresses the opportunity reduction mechanism of the fraud diamond organisations with high TIC scores create substantially narrower windows for fraud to occur undetected.

4.3 Pillar 2: Forensic Intelligence Architecture (FIA)

FIA addresses the organizational structures, processes, and competencies that enable the systematic transformation of raw technological outputs into forensic intelligence suitable for investigative and legal purposes. A critical and frequently neglected dimension of FIA is digital evidence chain of custody management the protocols through which electronically extracted evidence is preserved, authenticated, and documented in a manner meeting the evidentiary standards of Indian courts and regulatory tribunals.

The qualitative findings of this study reveal that many Indian forensic accounting practitioners, even those with access to sophisticated analytical tools, lack established institutional protocols for evidence handling in digital environments. This creates significant risk that analytically sound fraud detection outputs may be rendered legally inadmissible due to procedural deficiencies in evidence management a finding with direct implications for professional standards development by the ICAI.

4.4 Pillar 3: Regulatory Compliance Orientation (RCO)

The Indian regulatory environment governing forensic accounting and digital financial investigation is characterised by both significant institutional ambition reflected in the strengthened mandate of the SFIO, SEBI's enhanced surveillance infrastructure, and the Information Technology Act's provisions on digital evidence and notable gaps and ambiguities, particularly in the domains of cross-border data sharing, algorithmic audit admissibility, and cryptocurrency transaction forensics. RCO captures the forensic accounting organisation's capacity to navigate this complex regulatory terrain effectively.

RCO encompasses three sub-dimensions: regulatory intelligence (the systematic monitoring and interpretation of evolving legal requirements), compliance architecture (the embedding of regulatory requirements into forensic processes and technology configurations), and regulatory technology (RegTech) integration (the deployment of automated compliance monitoring tools that reduce the burden of manual regulatory tracking). Qualitative findings indicate that regulatory uncertainty particularly around the legal status of AI-generated forensic evidence represents a significant adoption barrier that the ICAI and Ministry of Corporate Affairs should address through dedicated guidance.

4.5 Pillar 4: Human Capital Development (HCD)

HCD is identified by this study's empirical findings as the most critical determinant of IDAF implementation success and the most significant source of current forensic accounting effectiveness deficits in the Indian context. Despite substantial technological availability particularly among larger firms a pervasive digital competency gap prevents practitioners from deploying available tools at their functional potential. Survey findings reveal that 76.2% of respondents rate their proficiency in AI-driven forensic analytics as insufficient, while 68.4% report never having received formal training in block chain forensics or data analytics applications.

HCD in the IDAF encompasses four sub-dimensions: competency framework alignment (ensuring that professional qualification syllabi and continuing professional development programmes incorporate digital forensic competencies), interdisciplinary skill integration (developing T-shaped practitioners who combine deep accounting expertise with functional technology literacy), organizational learning culture (creating institutional environments that reward skill development and knowledge sharing), and professional identity adaptation (supporting practitioners in conceptually integrating technological tools with the professional judgment and ethical standards that remain the irreducible core of forensic accounting practice).

Table 2. IDAF Pillars: Dimensions, Theoretical Anchors, and Indian Context Relevance

Pillar	Key Dimensions	Theoretical Anchor	Indian Context Relevan
TIC – Technologic Integration Capability	Portfolio breadt Interoperability, Real-tir processing, AI governance	Fraud Diamor (opportunity)	Firm-size divide in te readiness
FIA – Forens Intelligence Architecture	Evidence chain of custod Data governance, Analytic protocols	Institutional Theory	Weak digital eviden protocols in courts
RCO – Regulato Compliance Orientatic	Regulatory intelligenc Compliance architectu RegTech	Institutional Theo (coercive)	SFIO/SEBI mandate ga on AI evidence
HCD – Human Capi Development	Competency framework Interdisciplinary skil Learning culture	TAM / UTAUT	Severe digital competen gap nationally

5. Empirical Findings

5.1 Qualitative Findings

5.1.1 Theme 1: The Digital Competency Chasm

The most pervasive theme across all 30 interviews was a profound and widely acknowledged gap between the technological tools theoretically available to forensic practitioners and their actual capacity to deploy these tools effectively. Participants consistently described a situation where organizational investment in software had outpaced investment in the human capability necessary to operate it meaningfully. A Senior Forensic Auditor with 18 years of experience in a leading Mumbai-based firm described the situation in terms that resonated across multiple interviews: we have the platforms, we have the licenses, but using them properly requires a depth of data science understanding that most of us simply have not built. We use 15 or 20 percent of what the tool can actually do.

This competency gap was most acute in the domains of machine learning-based anomaly detection, natural language processing for document forensics, and block chain transaction tracing precisely the areas where technological capability advances most rapidly and where the potential for transformative forensic impact is

highest. Practitioners in smaller cities and boutique firms reported significantly more acute competency constraints than those in larger metropolitan centres.

5.1.2 Theme 2: Regulatory Ambiguity as an Adoption Brake

Twenty-four of 30 interview participants identified regulatory uncertainty as a significant factor moderating their enthusiasm for deploying AI and algorithmic tools in active forensic investigations. The central concern was evidentiary: participants questioned whether outputs generated by AI models would withstand judicial scrutiny in Indian courts or regulatory tribunals, given the absence of explicit statutory or judicial guidance on the admissibility and interpretability of algorithmically derived forensic evidence. This concern was particularly acute among practitioners engaged in SFIO-referred investigations and SEBI enforcement proceedings, where evidentiary standards are stringently applied.

5.1.3 Theme 3: Institutional Support as a Critical Enabler

Participants working within organizations that had made deliberate institutional commitments to forensic technology adoption including dedicated forensic technology teams, structured training programs, and leadership championship of digital transformation — reported substantially higher confidence in their technological proficiency and significantly greater integration of digital tools into their investigative practice. This finding strongly supports the IDAF's HCD and TIC pillars, and underscores the extent to which individual-level adoption behaviour is embedded within and shaped by organizational institutional contexts.

5.1.4 Theme 4: Professional Trust and Scepticism

A nuanced theme emerged around the relationship between forensic practitioners and AI-generated analytical outputs. While participants broadly acknowledged the efficiency advantages of AI-driven data analysis, many expressed reservations about surrendering professional judgment to algorithmic conclusions particularly in complex, context-dependent investigations where the subtleties of human behavior and organizational dynamics resist quantification. This finding points to the importance of designing AI-assisted forensic tools that augment rather than replace practitioner judgment, presenting probabilistic outputs that invite professional interpretation rather than binary conclusions that demand passive acceptance.

5.2 Quantitative Findings: Measurement Model

The measurement model demonstrated satisfactory reliability and validity across all constructs. Cronbach's alpha values ranged from 0.81 (RCO) to 0.89 (HCD), and composite reliability values ranged from 0.86 to 0.92. All AVE values exceeded the 0.50 threshold (range: 0.51–0.63), confirming convergent validity. Discriminant validity was established through the Fornell-Larcker criterion, with the square root of each construct's AVE exceeding its inter-construct correlations, and HTMT ratios all falling below the conservative 0.85 threshold.

Table 3. Construct Reliability and Validity Statistics

Construct	Items	Cronbach's α	CR	AVE
Technological Integration Capabili (TIC)	12	0.86	0.89	0.57
Forensic Intelligence Architecture (FIA	11	0.84	0.88	0.55
Regulatory Compliance Orientati (RCO)	10	0.81	0.86	0.51
Human Capital Development (HCD)	13	0.89	0.92	0.63
Fraud Detection Effectiveness (FDE)	12	0.87	0.91	0.59

5.3 Quantitative Findings: Structural Model and Hypothesis Testing

The structural model demonstrated good predictive relevance ($Q^2 > 0$ for all endogenous constructs) and acceptable model fit (SRMR = 0.062). The model explained 58.7% of the variance in Fraud Detection Effectiveness ($R^2 = 0.587$). Table 4 presents the path coefficients, bootstrapped standard errors, t-statistics, and hypothesis decisions.

Human Capital Development emerged as the strongest predictor of Fraud Detection Effectiveness ($\beta = 0.68$, $p < 0.001$), followed by Technological Integration Capability ($\beta = 0.54$, $p < 0.001$) and Forensic Intelligence Architecture ($\beta = 0.47$, $p < 0.001$). Regulatory Compliance Orientation also demonstrated a significant positive effect ($\beta = 0.38$, $p < 0.001$). The prominence of HCD as the leading predictor

surpassing even TIC provides compelling empirical support for the study's qualitative finding that human competency development represents the binding constraint on forensic technology adoption effectiveness in the Indian context.

Table 4. PLS-SEM Structural Model Results (Bootstrapped, 5,000 Resamples)

Hypothesis	Path	Std. Beta (β)	S.E.	t-stat	p-value	Supported?
H1	TIC → FDE	0.54	0.048	11.25	< 0.001	Yes
H2	FIA → FDE	0.47	0.051	9.22	< 0.001	Yes
H3	RCO → FDE	0.38	0.057	6.67	< 0.001	Yes
H4	HCD → FDE	0.68	0.044	15.45	< 0.001	Yes
H5	HCD → TIC	0.52	0.059	8.81	< 0.001	Yes
H6	TIC ↔ FIA	0.61	0.041	14.88	< 0.001	Yes

A particularly important finding is the significant path from HCD to TIC ($\beta = 0.52$, $p < 0.001$), confirming that human capital investment does not merely affect fraud detection outcomes directly but also enhances the organization's technological integration capability creating a virtuous cycle in which competency development amplifies the returns to technology investment. This finding has direct and actionable implications for the sequencing of organizational investments in forensic capability: technology acquisition without antecedent competency development generates significantly suboptimal returns.

Table 5. Current Technology Adoption Rates Among Indian Forensic Accountants (Survey, N = 210)

Technology	Currently Use (%)	Planning to Ado (%)	Not Aware / No Pla (%)
Data Analytics Platforr (ACL/IDEA/Python)	61.4	22.9	15.7
AI / Machine Learning Tools	28.6	41.4	30.0
Robotic Process Automation (RPA)	34.8	33.3	31.9
Block chain Forensic Tools	14.3	28.6	57.1
Natural Language Processing (NLP)	18.1	30.5	51.4
Continuous Auditing Platforms	42.9	29.5	27.6
Computer-Aided Audit Too (CAATs)	68.6	18.6	12.8

6. DISCUSSION

6.1 The Primacy Of Human Capital In The Indian Context

The finding that HCD is the strongest predictor of Fraud Detection Effectiveness among Indian forensic accountants stronger even than Technological Integration Capability constitutes the most practically significant contribution of this study. It challenges a prevalent discourse in the forensic technology literature that prioritizes technology acquisition as the primary lever of forensic capability improvement and reenters attention on the human practitioners who must translate technological potential into investigative results.

This finding is consistent with the Technology Acceptance Model's insight that perceived ease of use mediates the relationship between tool availability and actual use behavior. Indian forensic practitioners who lack confidence in their ability to operate AI-driven tools will systematically underutilize them, regardless of their technical sophistication. Bridging this competency gap requires sustained, profession-wide investment in digital forensic education an investment that professional bodies, academic institutions, and employing organizations must share.

6.2 Regulatory Uncertainty and Its Resolution

The qualitative finding that regulatory ambiguity around AI-generated evidence constitutes a significant adoption barrier points to an urgent need for regulatory action. The ICAI's Forensic Accounting and Investigation Standards framework, while a significant achievement, does not yet provide specific guidance on the use, documentation, or presentation of AI-derived forensic evidence in Indian legal proceedings. Similarly, the Information Technology Act's provisions on electronic evidence do not explicitly address the evidentiary status of machine learning model outputs. Filling these gaps through dedicated ICAI pronouncements, judicial guidance notes, or statutory amendment would substantially remove a barrier that currently inhibits the most transformative forensic technologies from reaching their investigative potential.

6.3 Implications for Professional Bodies and Institutions

The study's findings carry direct implications for the ICAI, which administers India's largest forensic accounting professional community. The pervasive digital competency gap documented in this study suggests that current CA examination syllabi and continuing professional education programmers are insufficiently oriented toward digital forensic skills. Integrating data analytics, AI literacy, block chain forensics, and digital evidence management into core CA and Forensic Accounting and Investigation Standards curricula rather than treating these as optional or specialist supplements would address a structural deficit that is currently limiting the effectiveness of India's forensic accounting profession at scale.

6.4 Limitations of the Study

This study is subject to several limitations that should be acknowledged in interpreting its findings. First, the survey sample, while geographically distributed across five major Indian cities, is concentrated among larger urban centers and may not fully represent the experience of forensic practitioners in smaller cities and towns, where technological resources and training opportunities may be significantly more constrained. Second, the cross-sectional survey design captures a single temporal snapshot of adoption behavior and cannot illuminate the longitudinal dynamics of technology adoption trajectories. Third, self-reported survey data are subject to social desirability bias, though this was partially mitigated through instrument design and anonymous data collection. Fourth, the study's focus on forensic accountants and auditors excludes other stakeholders in the fraud detection ecosystem including regulatory investigators, law enforcement, and judicial officers whose perspectives would enrich a more comprehensive understanding of the institutional context.

7. CONCLUSION

This study has generated original empirical evidence on the adoption of digital technologies among forensic accountants and auditors in India, and has developed and validated the Integrated Digital-Age Framework (IDAF) as a theoretically grounded, contextually sensitive architecture for forensic accounting practice in the digital age. Drawing on 30 semi-structured interviews and a structured survey of 210 forensic professionals across five Indian cities, the study's most significant finding is that human capital development not technological

acquisition is the primary determinant of effective digital fraud detection in the Indian context. Until the profession addresses its pervasive digital competency gap through systematic education and training investment, the transformative potential of AI, block chain, and data analytics for Indian forensic accounting will remain largely unrealized.

The IDAF contributes a contextualized, India-specific framework that acknowledges the unique regulatory, infrastructural, and professional culture dimensions of Indian forensic practice, offering a more practically actionable guide to digital capability development than frameworks derived from Western contexts. The framework's four pillars Technological Integration Capability, Forensic Intelligence Architecture, Regulatory Compliance Orientation, and Human Capital Development are empirically validated as significant predictors of Fraud Detection Effectiveness, collectively explaining 58.7% of outcome variance.

Future research should extend the IDAF through longitudinal designs capable of capturing adoption trajectory dynamics, explore sector-specific variations in technology adoption barriers across banking, manufacturing, and government sectors, and examine the emerging implications of generative AI and large language models for forensic document examination and financial statement analysis. Cross-country comparative studies between India and other major emerging economies including Brazil, South Africa, and Indonesia would further enrich understanding of how national institutional contexts shape forensic technology adoption.

India's forensic accounting profession stands at a pivotal juncture. The financial complexity of the digital economy demands investigative capabilities that only systematic integration of advanced technologies can provide. Realizing this potential will require concerted, coordinated action by professional bodies, academic institutions, regulatory authorities, and employing organizations guided by empirically

REFERENCES

1. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
2. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589
3. Cressey, D. R. (1953). Other people's money: A study in the social psychology of embezzlement. Free Press.
4. Creswell, J. W., & Plano Clark, V. L. (2017). Designing and conducting mixed methods research (3rd ed.). SAGE Publications.
5. Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3), 5–21. https://doi.org/10.2308/isys-51804
6. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008
7. Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report results of PLS-SEM. European Business Review, 31(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203
8. Institute of Chartered Accountants of India [ICAI]. (2023). Forensic accounting and investigation standards (FAIS): Framework document. ICAI.
9. Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X
10. Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. American Journal of Sociology, 83(2), 340–363. https://doi.org/10.1086/226550
11. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006
12. Parashar, M., & Singh, R. (2022). Forensic accounting in India: Challenges, opportunities and the road ahead. Indian Journal of Accounting, 54(1), 45–61.

13. Ramamoorti, S. (2008). The psychology and sociology of fraud: Integrating the behavioral sciences component into fraud and forensic accounting curricula. Issues in Accounting Education, 23(4), 521–533. https://doi.org/10.2308/iace.2008.23.4.521
14. Serious Fraud Investigation Office [SFIO]. (2024). Annual report 2023–24: Financial fraud investigation in India. Ministry of Corporate Affairs, Government of India.
15. Vasarhelyi, M. A., & Halper, F. B. (1991). The continuous audit of online systems. Auditing: A Journal of Practice & Theory, 10(1), 110–125.
16. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478. https://doi.org/10.2307/30036540
17. West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57, 47–66. https://doi.org/10.1016/j.cose.2015.09.005
18. Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. CPA Journal, 74(12), 38–42.
19. Yadav, S., & Krishnamurti, C. (2023). Digital transformation of audit and assurance in India: Evidence from listed companies. Journal of Accounting and Finance in Emerging Economies, 9(2), 112–129.
20. Zahra, S. A., Priem, R. L., & Rasheed, A. A. (2005). The antecedents and consequences of top management fraud. Journal of Management, 31(6), 803–828. https://doi.org/10.1177/0149206305279598