ROLE OF ARTIFICIAL INTELLIGENCE AND DATA ANALYTICS IN FORENSIC AUDITING: REDUCING FINANCIAL FRAUD

Dr. Jai Tater*
Dr. Umaid Raj Tater**

ABSTRACT:

Financial fraud is not a new problem — but what has changed dramatically over the past two decades is both the scale at which it occurs and the ingenuity with which it is concealed. Traditional forensic auditing, for all its strengths, was built around a world of paper trails and periodic reviews. That world no longer exists. Today, transactions move in milliseconds, financial instruments span multiple jurisdictions, and the gap between when fraud is committed and when it is discovered can stretch into years. Against this backdrop, the question of whether Artificial Intelligence and Data Analytics can meaningfully strengthen forensic auditing is not merely academic — it has real consequences for investors, regulators, and the public. This paper takes up that question directly. Drawing on primary survey data collected from 187 audit professionals across India, complemented by a systematic review of published literature spanning 2015 to 2024, the study examines how machine learning, anomaly detection, natural language processing, robotic process automation, and blockchain analytics are reshaping forensic audit practice. The findings are encouraging but not uncritical: organisations that have integrated AI into their audit frameworks report substantially better fraud detection outcomes, but the barriers to adoption — particularly around data quality, skilled personnel, and regulatory clarity — remain formidable. The paper concludes by proposing the Intelligent Forensic Audit System (IFAS), a six-dimensional framework intended to guide organisations and regulators in navigating these challenges. Keywords: Forensic Auditing, Artificial Intelligence, Data Analytics, Financial Fraud, Machine Learning, Anomaly Detection, Blockchain, Fraud Prevention, Regulatory Compliance, India

INTRODUCTION

Background and Context

There is something almost paradoxical about the current state of corporate financial oversight. On one hand, the sheer volume and granularity of financial data available to auditors today would have been unimaginable to their predecessors two or three decades ago. On the other hand, the frequency and cost of financial fraud has not decreased — if anything, it has grown more severe. The Association of Certified Fraud Examiners estimated in its 2024 Report to the Nations that organisations globally lose roughly five per cent of annual revenues to occupational fraud each year, amounting to losses exceeding four point seven trillion US dollars. Cases like the Satyam Computers scandal in India and the Wirecard collapse in Germany are not isolated anomalies; they reflect systemic vulnerabilities that conventional audit methods have repeatedly failed to catch. Forensic auditing is a field that combines accounting know-how with investigative skills, and it's been the main way to protect against financial fraud. But the methods used in most forensic audits were created when data was simpler and easier to handle. These methods, like manually checking samples, testing transactions based on rules, and reconciling at the end of a period, are basically looking back at what's already happened and only checking certain things. When someone trying to commit fraud understands how these systems work, they can set up their transactions in a way that helps them avoid getting caught. This is a problem because it means the current methods might not be good enough to catch all fraud. It is in this context that the emergence of Artificial Intelligence and advanced data analytics represents something genuinely significant. The capacity to monitor entire

* Guest Faculty, Department of Accounting, Jai Narain Vyas University, Jodhpur
** Assistant Professor, Department of Business Administration, Jai Narain Vyas University, Jodhpur

transaction populations continuously, to detect subtle multivariate patterns that no human reviewer could identify, and to generate predictive risk flags before fraud crystallises into loss — these are not marginal improvements. They represent a different philosophy of fraud prevention altogether. Whether and how this potential is being realised in practice, particularly within the Indian corporate and regulatory environment, is the central concern of this study.

STATEMENT OF THE PROBLEM

The promise of AI in forensic auditing is well established in theory; the practice, however, is considerably messier. Adoption is concentrated among large organisations with the resources to invest in complex technology infrastructure. Smaller firms and public sector entities — which are often the most vulnerable to fraud — continue to depend on methods that have not fundamentally changed in decades. Meanwhile, the academic literature on this topic, while growing, tends to treat technological, organisational, and regulatory dimensions in isolation, offering limited guidance to practitioners who must manage all three simultaneously. This study is an attempt to address that gap.

OBJECTIVES OF THE STUDY

1. To examine the current landscape of AI and data analytics tools deployed in forensic auditing, both globally and within India.

2. To assess empirically how effective AI-driven approaches are in detecting and preventing financial fraud.

3. To identify the key challenges and institutional barriers that impede wider adoption.
4. To propose a structured framework — the IFAS — for integrating AI and data analytics into forensic auditing practice in a sustainable and contextually appropriate way. To provide audit professionals, organizations, and regulatory bodies in India with recommendations that are backed by solid evidence.

SIGNIFICANCE OF THE STUDY

India occupies a somewhat unusual position in this discussion. Its digital financial infrastructure has advanced with remarkable speed — the Unified Payments Interface alone now processes billions of transactions monthly — yet forensic audit capabilities have not kept pace. Regulatory bodies including SEBI, MCA, and ICAI are increasingly aware of the need for AI governance frameworks in auditing, but actionable guidance remains limited. This study speaks directly to that need, offering both empirical evidence and a structured framework grounded in the Indian context.

SCOPE AND LIMITATIONS

The study covers peer-reviewed academic literature, industry reports, and documented case studies published or conducted between 2015 and 2024. Sectors included in the analysis are banking, insurance, listed corporate entities, public sector undertakings, and manufacturing. Several limitations deserve acknowledgement. AI technologies are evolving at a pace that inevitably outstrips any single study's capacity to capture; what is current practice today may be obsolete within a few years. Access to proprietary organisational data was restricted, which constrains the depth of case analysis possible. Finally, the available empirical literature remains disproportionately concentrated in developed country contexts, which limits the generalisability of some findings to the Indian setting.

REVIEW OF LITERATURE

The Evolution of Forensic Auditing

Forensic auditing didn't just appear out of nowhere. It has a history that starts with accountants who worked with courts and lawyers to look at financial records that were in dispute. Over time, it became a more organized and proactive field, especially after the big corporate scandals in the early 2000s. Researchers like Singleton and Singleton point out that forensic auditing really became a profession after the Enron scandal, when the Sarbanes-Oxley Act was passed. This law required companies to have better internal controls and independent auditing, which meant that auditors had to be more thorough in their investigations.

The 1990s and early 2000s saw a major change in auditing with the introduction of Computer-Assisted Audit Techniques. This allowed auditors to work with large amounts of electronic data using tools like ACL and IDEA. However, as Wells pointed out in 2017, these tools were still pretty basic. They were good at finding things that auditors already knew to look for, but they weren't very good at finding new and unusual fraud schemes that didn't fit into the predefined categories. In other words, they were great at identifying patterns they were programmed to recognize, but not so great at discovering completely new ones. This limitation made it difficult for auditors to stay one step ahead of fraudsters who were constantly coming up with new ways to cheat the system. As a result, auditors needed to find new and better ways to use technology to fight fraud.

ARTIFICIAL INTELLIGENCE AND ITS ENTRY INTO AUDITING

The scholarly conversation about AI in auditing began in earnest around the mid-2010s. Kokina and Davenport (2017) produced what became a widely cited study examining how cognitive technologies and machine learning were beginning to reshape audit functions at the major accounting firms. Their central finding — that AI tools could automate roughly 40 per cent of routine audit tasks — was striking not so much for the number itself as for what it implied: that auditors freed from mechanical work might redirect their attention towards judgement-intensive investigation.

Sun and Vasarhelyi (2018) demonstrated in a subsequent study that deep learning neural networks could detect fraudulent financial statements with accuracy rates above 90 per cent, a performance level that substantially exceeded conventional logistic regression models. Around the same time, the U.S. Securities and Exchange Commission was quietly deploying natural language processing tools to screen earnings call transcripts and management discussion sections for linguistic patterns associated with deliberate misrepresentation — work documented by Bauguess (2017) that showed recall rates well above what manual review could achieve.

DATA ANALYTICS AND THE TRANSFORMATION OF FRAUD INVESTIGATION

Data analytics has changed things in a big way. Even though AI gets a lot of attention, the basic work of using all transaction data instead of just samples to make audit conclusions has been just as important. The idea of continuous auditing was first thought of by Vasarhelyi and Halper back in 1991, but it took a while for computers to be powerful enough and for data storage to be big enough to make it actually work. This new way of auditing has been a game-changer, and it's interesting to see how it's developed over time. With more power and storage, auditors can now look at all the data, not just a small part of it, which makes their conclusions more accurate. This has been a big shift in the way audits are done, and it's had a big impact on the field.

Nigrini's (2012) work on Benford's Law is worth noting here as an example of how a fairly simple analytical technique, properly applied to large datasets, can expose manipulation that human reviewers would never detect. Similarly, Coderre (2009) documented how digital root tests and stratified sampling applied to transaction datasets could surface statistical anomalies with reasonably high precision. Appelbaum, Kogan, and Vasarhelyi (2017) extended this line of thinking to what they called 'big data auditing' — the integration of unstructured external data such as social media sentiment, regulatory filings, and news sources into fraud risk profiling. The enrichment of forensic analysis through these additional data streams represents a genuine qualitative advance over purely internal transaction review.

AI-SPECIFIC APPLICATIONS IN FORENSIC CONTEXTS

Several studies have examined particular AI tools within forensic auditing contexts with some precision. Jans, Alles, and Vasarhelyi (2014) used process mining on accounts payable transaction logs to identify instances of fraudulent vendor creation and duplicate payment schemes — finding not just that the technique worked, but that it surfaced patterns that had been invisible to the existing internal controls. Gepp et al. (2018) compared the performance of different machine learning classifiers — decision trees, support vector machines, and neural networks — in predicting fraudulent financial statements and found that ensemble methods combining multiple models consistently outperformed any individual algorithm.

In India, researchers like Majithia and Patel, and Sharma and Dubey, took a closer look at how AI is being used in banking and insurance. What they found was pretty interesting - when banks and insurance companies used AI to monitor transactions, they were able to catch fraud happening in real time, and that's a big deal. But here's the thing: even though AI was helping to detect fraud, the way it was being used varied a lot from one institution to another. Some were doing a great job, while others were struggling to get it right. This just goes to show that introducing new technology isn't always a straightforward process, and there's still a lot to learn about how to make it work effectively.

WHAT THE LITERATURE LEAVES UNADDRESSED

For all its richness, the literature has some conspicuous gaps. Most empirical studies focus on a single technology or sector in isolation, making it difficult to develop integrated guidance for organisations that must make decisions across multiple dimensions simultaneously. The developing country context — and India in particular — remains underrepresented in quantitative empirical work. And the interaction between technological capability and organisational readiness (human capital, data governance, internal culture) has received less systematic attention than it deserves. These are the gaps this study tries, in part, to fill.

RESEARCH METHODOLOGY

RESEARCH DESIGN

The study is using a combination of methods to get a better understanding of the issue. It's looking at numbers from a survey, which gives a broad view and allows for generalizations, but it's also examining specific cases and reviewing existing literature to add depth and context. This approach is intentional, as using just one method wouldn't have been enough to answer the questions being asked. By combining these methods, the study can interpret the numbers in a more meaningful way. The survey data provides a wide view, while the case studies and literature review help to explain what the numbers really mean.

PHILOSOPHICAL ORIENTATION

In terms of research philosophy, the study sits in what might loosely be described as the interpretivist-positivist middle ground — not an unusual position for applied social science research. Positivist assumptions underpin the quantitative analysis: the expectation that survey responses, properly collected and coded, can yield generalisable conclusions about patterns and relationships. Interpretivist sensibilities inform the case analysis: the recognition that context matters enormously in understanding why organisations behave the way they do with respect to technology adoption.

DATA COLLECTION

We collected our main information using a set of questions that we gave to experts in forensic auditing, accounting, and internal auditing all over India. This happened between July and October 2024. We sent these questions through local groups of accountants, companies that do audits, and universities. Out of 214 question sets that we sent out, 187 were completed and useful - that's about 87.4 percent, which is a good response for a survey like this that targets professionals.

We got our secondary data from a variety of places. This included academic journals like Scopus, Web of Science, and JSTOR. We also looked at reports from big companies like ACFE, Deloitte, PwC, EY, and KPMG. Additionally, we checked out publications from regulatory bodies such as SEBI, RBI, ICAI, and MCA. And finally, we examined documented cases of corporate fraud from both Indian and international sources.

SAMPLING STRATEGY

To get a good understanding of the people working in auditing, fraud investigation, and accounting with technology, a special kind of survey was done. This survey focused on three main groups of people: those who work as forensic auditors or accountants, people who do internal audits for companies, and researchers who study accounting and finance. There were 78 forensic auditors and accountants, which is about 41.7% of the total people surveyed. Then, there were 62 internal audit professionals, making up about 33.2%. Lastly, 47 researchers in accounting and finance were part of the survey, which is about 25.1%.

Category	Sample Size	Percentage
Practising Forensic Auditors / CAs	78	41.7%
Corporate Internal Audit Professionals	62	33.2%
Academic Researchers (Commerce / Accounting)	47	25.1%
Total	187	100%

Table 1: Distribution of Survey Respondents by Professional Category

ANALYTICAL APPROACH

To understand the results, we looked at the numbers - how often things happened, what percentage of people agreed, and the average score people gave. We also checked if the questions we asked were reliable by using a special test called Cronbach's Alpha. Then, we compared the answers from different groups of people to see if there were any differences. For the written answers, we used a method called thematic coding to find common themes. We also did a big review of what other people have written about the topic, looking at 312 papers and choosing 94 that were relevant, well-researched, and recent.

ETHICAL CONSIDERATIONS

People took part in the main survey by choice and were promised that their answers would be kept secret. We didn't ask for any personal details that could identify them. All the other information used in the study came from public sources and we gave credit where it was due. The way we designed the study and collected the data followed the rules set by the Indian Council of Social Science Research, which makes sure research is done in an ethical way.

AI AND DATA ANALYTICS TOOLS IN FORENSIC AUDITING

MACHINE LEARNING AND PREDICTIVE ANALYTICS

Machine learning occupies a central position in the AI-driven forensic audit toolkit, and for good reason. Supervised learning models, trained on historical fraud data, can classify transactions and financial entries as normal or anomalous with a speed and consistency that no team of human auditors can match. Unsupervised methods — particularly clustering algorithms — go a step further, identifying unusual groupings of activity without needing labelled training data. This matters because genuinely novel fraud schemes, by definition, do not match historical patterns, and a system that can only find what it has been taught to look for will always lag behind a creative fraudster. Reinforcement learning is the next big thing. It's a way to make detection models better over time. Here's how it works: the model gets updated based on how well it does - whether it gets things right or wrong. This means it can learn from its mistakes and get better without needing to be retrained all the time. Some banks in India and around the world are starting to use this approach, but it's still not very common to see it used on a large scale. As time goes on, we can expect to see more of this type of learning, where machines get smarter and more accurate, just like we do when we learn from our experiences.

ANOMALY DETECTION SYSTEMS

Anomaly detection is one of the most established and widely used applications of artificial intelligence in forensic auditing. It uses a range of methods, from simple statistical approaches like z-score analysis and interquartile range testing, to more complex multivariate AI systems. These systems can detect unusual patterns across thousands of data dimensions at the same time. Some commercial platforms, such as SAS Fraud Management, IBM Safer Payments, and Oracle's OFSAA suite, have made this capability a part of daily operations at large financial institutions. They can flag suspicious transactions, anomalies in authorization, and unusual relationships with vendors in real-time. This helps institutions to identify and prevent fraudulent activities more effectively. By using AI in this way, financial institutions can stay one step ahead of potential threats and protect their assets. The use of anomaly detection has become a crucial tool in the fight against fraud and financial crime.

NATURAL LANGUAGE PROCESSING

The potential of NLP in forensic auditing is somewhat less intuitive than transaction analytics but no less significant. A large fraction of the most consequential information about an organisation's financial position and management behaviour lives not in structured data tables but in text: board minutes, audit committee correspondence, management commentaries, contract terms, emails, and regulatory filings. NLP tools that can parse this material at scale — extracting entities, identifying sentiment shifts, and flagging linguistic markers associated with deception — give auditors access to a dimension of evidence that was previously available only through labour-intensive manual review. The SEC's use of NLP to screen earnings call transcripts and MD&A sections for deceptive language patterns, as described by Bauguess (2017), offers perhaps the clearest demonstration of this capability. Detection rates achieved through automated text analysis substantially exceeded those from comparable manual review processes.

ROBOTIC PROCESS AUTOMATION

RPA automates the repetitive, rule-governed components of the audit process — journal entry testing, account reconciliation, vendor master validation, and similar tasks that require accuracy and consistency but not judgement. When combined with AI capabilities (a combination sometimes called intelligent process automation or IPA), these systems can handle exceptions and learn from outcomes rather than breaking down when they encounter inputs outside their original programming. Major firms including Deloitte and KPMG have publicly described IPA deployments that reduce forensic audit cycle times by substantial margins while eliminating the data entry errors that periodically compromise manual processes.

BLOCKCHAIN ANALYTICS

As more people buy and sell digital assets, it's becoming really important to look at how blockchain affects audits. There are special tools like Chainalysis and Elliptic that help track digital assets as they move through the blockchain system. They can show how transactions are connected and find wallet addresses that might be involved in illegal activities. One of the best things about blockchain is that its records can't be changed once they're made. This makes it really useful for audits because it creates a clear and trustworthy trail of transactions. This has already been really helpful in investigating things like cryptocurrency fraud, money laundering, and ransomware payments.

Tool / Technique	Primary Application	Adoption Level (India)	Key Limitation
Machine Learning (Supervised)	Transaction fraud classification	Moderate–High (large firms)	Requires substantial labelled training data
Anomaly Detection	Real-time transaction monitoring	High (banking sector)	High false positive rates if poorly calibrated
Natural Language Processing	Document and disclosure analysis	Moderate	Context sensitivity; language nuance
Robotic Process Automation	Audit task automation	High	Limited to rule-based tasks
Blockchain Analytics	Digital asset tracing	Growing	Requires specialist knowledge
Predictive Analytics	Fraud risk scoring	Moderate	Model interpretability challenges

Table 2: Summary of AI and Analytics Tools in Forensic Auditing

Indian Journal of Business Administration (IJBA)
(A National Peer Reviewed Refereed Journal)
ISSN: 0975-6825, Volume 18, Issue 2, July-December 2025, pp. 46-59

DATA ANALYSIS AND FINDINGS

AI AWARENESS AND ADOPTION LEVELS

The survey data reveal a pattern of adoption that is both more extensive than might have been expected and more uneven than is comfortable. Among respondents from large organisations — those with annual turnover exceeding Rs. 500 crores — 73.4 per cent reported active use of at least one AI-driven audit tool. Among respondents from small and medium enterprises, that figure drops to 18.6 per cent. The size differential is not surprising in itself, but its magnitude suggests that the gap in fraud detection capability between large and small organisations is substantially wider than is generally acknowledged in regulatory or professional discourse. Sectoral variation is similarly pronounced. Banking and financial services respondents reported the highest awareness levels (88.5%), followed by insurance (76.3%) and listed corporates (69.4%). Public sector undertakings registered the lowest awareness scores (44.7%), which is concerning given the scale of public funds at stake in this sector.

Sector	AI Awareness (%)	Active AI Adoption (%)	Fraud Reduction Observed (%)
Banking & Financial Services	88.5%	71.2%	62.4%
Insurance	76.3%	58.9%	54.7%
Listed Corporates (BSE/NSE)	69.4%	53.1%	48.3%
Public Sector Undertakings	44.7%	29.8%	31.6%
Manufacturing	52.3%	34.6%	37.2%
SMEs	31.8%	18.6%	22.1%

Table 3: AI Awareness, Adoption and Observed Fraud Reduction by Sector

EFFECTIVENESS IN FRAUD DETECTION

Many companies have started using AI to help with auditing, and they're really happy with the results. When asked to rate how well it works, they gave it very high scores. For example, a tool that uses AI to find unusual activity got a score of 4.31 out of 5, and a tool that uses predictions to help with auditing got a score of 4.08. Overall, the average score was 4.17, which is very good. This suggests that the companies are consistent in their opinions about how well the AI tools work.

Here's what we can learn from a real-life example. A bank in northern India used a new system to monitor transactions and it worked really well. Within six months, it found over 1,200 suspicious transactions that were linked to a big loan fraud. This fraud had been going on for over three years without being detected by the bank's old audit system. This shows that these systems can be very effective when they are used correctly. However, it's not always possible to get the same results everywhere - a lot depends on how well the system is set up and used. But this example does show what can be achieved when everything works as it should.

Efficiency Gains

Beyond fraud detection per se, AI adoption was associated with significant improvements in audit process efficiency. Respondents from AI-adopting organisations reported average reductions of 48.2 per cent in journal entry testing time, 63.7 per cent in data extraction and cleansing time, and 41.3 per cent in overall forensic audit cycle duration. These figures should be treated as indicative rather than definitive — they are self-reported and likely subject to some optimistic bias — but the direction is consistent across respondent categories and corroborated by published case study evidence.

Barriers to Adoption

The study's findings on adoption challenges are perhaps the most practically significant part of the analysis. Data quality and availability emerged as the most commonly cited barrier, raised by 68.4 per cent of respondents with a severity rating of 4.3 out of 5. High implementation costs came second (61.2 per cent, severity 4.1), followed closely by shortage of AI-skilled audit professionals (58.7 per cent, severity 4.2). Concerns about algorithmic transparency and explainability were flagged by 47.3 per cent of respondents — a finding that has particular relevance in forensic contexts, where audit conclusions may need to withstand legal scrutiny.

Challenge	Frequency (%)	Severity Rating (1–5)
Data Quality and Availability Issues	68.4%	4.3
High Implementation and Licensing Costs	61.2%	4.1
Shortage of AI-Skilled Audit Professionals	58.7%	4.2
Algorithmic Bias and Explainability Concerns	47.3%	3.9
Regulatory and Legal Uncertainty	42.8%	3.8
Cybersecurity and Data Privacy Risks	39.6%	4.0
Resistance to Change in Audit Culture	35.2%	3.5

Table 4: Barriers to AI Adoption in Forensic Auditing — Frequency and Severit

PROPOSED FRAMEWORK: THE INTELLIGENT FORENSIC AUDIT SYSTEM (IFAS)

The empirical findings described above, combined with the review of existing literature and case evidence, point towards a common conclusion: that effective AI-driven forensic auditing is not primarily a technology problem. It is an organisational and governance problem for which technology is a necessary but insufficient solution. The Intelligent Forensic Audit System (IFAS) proposed here is an attempt to capture this multi-dimensional reality in a structured, actionable framework. It comprises six interconnected dimensions, each addressing a distinct but interdependent aspect of the adoption challenge.

ISSN: 0975-6825, Volume 18, Issue 2, July-December 2025, pp. 46-59

DIMENSION 1: DATA INFRASTRUCTURE AND GOVERNANCE

No AI system performs well on poor data. Before any organisation invests in sophisticated AI tools for fraud detection, it needs to be confident that the underlying data — transaction records, master data, external feeds — meet minimum standards of completeness, accuracy, and timeliness. This means establishing data governance frameworks that assign clear ownership and accountability for data quality, and investing in the integration infrastructure needed to bring together data from disparate source systems into a coherent analytical environment. Cloud-based data warehouses and structured data lake architectures have made this considerably more affordable than it once was, even for mid-sized organisations.

DIMENSION 2: APPROPRIATE TECHNOLOGY SELECTION

There is a real risk of organisations adopting AI tools that are either too complex for their current data and human capital situation or too narrow to address their most significant fraud risks. A modular approach — deploying targeted solutions for well-defined fraud risk areas such as procurement fraud, revenue recognition manipulation, or cyber-enabled financial crime — tends to produce better outcomes than attempting comprehensive transformation in a single step. Tool selection should be driven by a rigorous assessment of the organisation's specific fraud risk profile and regulatory environment, not by vendor marketing.

DIMENSION 3: HUMAN CAPITAL DEVELOPMENT

This dimension is, in many ways, the most important and the most neglected. AI systems in forensic auditing need professionals who understand both what the technology is doing and what it cannot do — who can interpret model outputs critically, design appropriate validation tests, and communicate findings in a way that meets evidentiary standards. This skill set does not currently exist at scale in the Indian audit profession. Building it requires changes to CA and CMA curricula, expansion of specialised certification programmes, and sustained investment in continuing professional development. ICAI's Data Analytics Certificate Programme is a step in the right direction, but considerably more is needed.

DIMENSION 4: REGULATORY AND ETHICAL FRAMEWORK

The legal and regulatory status of AI-generated findings in forensic audit contexts is, in most jurisdictions, not yet clearly defined. In India, there is no specific guidance from SEBI, MCA, or ICAI on how AI tools should be governed in statutory or forensic auditing, what disclosure obligations apply, or how evidentiary questions around algorithmic outputs should be handled. This regulatory gap creates uncertainty for practitioners and may be deterring adoption. Developing clear, principles-based guidance — drawing on international models such as the OECD AI Principles and emerging IAASB thinking on technology-enabled auditing — should be a near-term priority.

DIMENSION 5: CONTINUOUS MONITORING AND MODEL GOVERNANCE

AI models for fraud detection are not set-and-forget systems. Fraud patterns evolve as fraudsters learn to evade detection algorithms — a dynamic sometimes described as 'adversarial adaptation.' Keeping AI systems effective over time requires ongoing model performance monitoring, regular recalibration using updated training data, and systematic tracking of false positive and false negative rates. Organisations serious about AI-driven forensic auditing need to establish model risk management functions within their internal audit or risk departments, with clear lines of accountability for model performance.

DIMENSION 6: CROSS-INSTITUTIONAL COLLABORATION

Individual organisations, however well-resourced, are working with a limited view of the fraud landscape. The intelligence needed to train and update fraud detection models improves substantially when it draws on experience across multiple institutions. This points towards the value of cross-institutional fraud intelligence sharing — anonymised and properly governed — between financial institutions, regulators, and law enforcement. Initiatives like the RBI's Project Pravaah and the FATF's existing financial intelligence sharing architecture offer templates that India could develop further. The barrier is less technical than political: institutions are often reluctant to share data that might reveal weaknesses in their own controls.

DISCUSSION

So, what did we learn from this study? A few things stand out. First, the question of whether AI is useful in forensic auditing is a good one. And the answer is, yes, it can be - but only if certain conditions are met. It seems to work better in some areas than others, and in bigger organizations rather than smaller ones. Also, it's really important to have good data governance and human experts involved, or it just won't be as effective. For example, banks that used AI saw a big reduction in fraud - 62.4 per cent, which is a pretty impressive number. But, if you look closer, you'll see that some banks did much better than that, while others didn't see much of a benefit at all. This is because the conditions for success, like good data and human expertise, weren't in place. Some key points to take away from this are: - AI can be really useful in forensic auditing, but it's not a magic solution that works everywhere. - It's more effective in some sectors and organizations than others. - Having good data governance and human experts is crucial for getting the most out of AI. - Even with AI, there's no one-size-fits-all solution - what works for one organization might not work for another. Overall, the study shows that AI can be a powerful tool in forensic auditing, but it needs to be used thoughtfully and with careful consideration of the underlying conditions.

The thing is, when it comes to adopting new technology, there are some big hurdles to overcome. And these hurdles aren't just going to disappear on their own - they need to be tackled head-on by lots of different people and groups working together. This can be a bit of a challenge for a system that's used to just letting the market sort things out, but it's the way it has to be. You see, problems like making sure data is good quality, getting professionals the skills they need, and figuring out all the regulatory stuff - these aren't things that can just be left to sort themselves out over time. They need a deliberate and coordinated effort from everyone involved. It's not always easy, but it's the only way to really make progress and get past these adoption barriers.

A third, more cautionary thread concerns the limits of AI itself. Machine learning models trained on historical fraud patterns will, by construction, be less effective at detecting genuinely novel schemes. Algorithmic bias — the risk that models perform differently for different types of transactions, sectors, or demographic groups — is a real problem that the forensic audit community has not yet grappled with systematically. And the 'black box' quality of deep learning models creates genuine difficulties in legal and regulatory proceedings where the basis for a finding needs to be explained and defended. These are not arguments against AI adoption; they are arguments for adopting it with clear eyes and appropriate safeguards.

It's clear that the challenges we're facing don't make it any less important to start using AI in forensic auditing in India. In fact, with the amount of financial fraud happening now, not doing anything is a big risk. The real question is, how can we use AI in a way that actually makes a difference in catching fraud, rather than just looking like we're using the latest technology? We need to make sure that any changes we make are lasting and effective, not just for show.

CONCLUSION

This study has examined, from multiple angles, the role of Artificial Intelligence and Data Analytics in transforming forensic auditing and reducing financial fraud. The evidence is consistent: organisations that have meaningfully integrated AI into their forensic audit frameworks detect fraud earlier, more accurately, and at lower marginal cost per investigation than those relying on traditional methods. The performance differentials are not small — they are large enough to represent a qualitative difference in the level of financial governance protection available.

The advantages of technology are not being shared equally among all organizations. There's a big difference in how well large companies that are good at using technology can protect themselves compared to smaller businesses and government groups. This difference creates a big weakness in the system that dishonest people can take advantage of. When some organizations have strong defenses using artificial intelligence and others have very little protection, it makes it more likely that the dishonest people will target the weaker ones, which are also the hardest to help.

The IFAS framework is a plan to help bridge the gap between where we are and where we need to be with AI. It's not about relying too much on technology to solve everything, but rather about paying attention to several key areas at the same time. These areas include making sure we have the right data infrastructure in place, choosing the best tools for the job, building the professional skills we need, having clear rules and regulations, keeping a close eye on how our models are working, and working together across different institutions. The thing is, we can't just focus on one or two of these areas and expect everything to fall into place - we need to be working on all of them simultaneously.

For India, the timing of this challenge is particularly acute. The country's digital financial infrastructure is advancing rapidly, creating both new opportunities for economic inclusion and new surface area for financial fraud. The accounting profession, regulatory institutions, and academic community have a shared responsibility — and, frankly, a narrow window — to build the ecosystem needed to ensure that AI's potential in forensic auditing is realised in practice and not just in conference proceedings.

RECOMMENDATIONS

For Forensic Audit Professionals

The first obligation for practising forensic auditors is to close their own knowledge gap. AI literacy — understanding what machine learning models can and cannot do, how anomaly detection algorithms work, what NLP tools are and are not good at — is becoming a core professional competency, not an optional specialisation. ICAI, ACFE, and global bodies offer programmes that provide starting points;

the challenge is making participation a professional norm rather than an individual choice. Beyond awareness, practitioners should develop the ability to document and defend AI-generated findings in ways that meet evidentiary standards. A fraud detection flag from an AI system is not itself evidence; it is the beginning of an investigation, and that distinction matters enormously in legal proceedings

FOR ORGANISATIONS

Organisations — particularly those in sectors with significant fraud exposure — should treat AI adoption in forensic auditing as a strategic priority rather than a technology infrastructure decision. This means board-level engagement with fraud risk management, not just delegation to the internal audit function. It means investing in data governance as a foundational capability before expecting AI tools to deliver on their promise. And it means being realistic about timelines: the benefits of AI in forensic auditing tend to accumulate gradually as models are trained, validated, and refined, not arrive immediately after system deployment.

FOR REGULATORY BODIES

SEBI, MCA, ICAI, and RBI have a big role to play in creating a good environment for high-quality AI-driven forensic auditing to grow. They need to make clear rules on how AI should be used in auditing, and make sure companies tell everyone about how they use AI tools and how well they work in detecting fraud. They should also help set up a system where different institutions can share information about fraud. In the long run, it's a good idea to include AI and data analysis in the basic education and training for accountants, rather than just making it an extra option. This will help them do their jobs better and keep up with the latest technology. By working together, these organizations can help make sure that AI-driven forensic auditing is used in a way that is fair, transparent, and effective.

REFERENCES

- Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. Auditing: A Journal of Practice & Theory, 36(4), 1–27.
- Association of Certified Fraud Examiners (ACFE). (2024). Report to the Nations: 2024 Global Study on Occupational Fraud and Abuse. Austin, TX: ACFE.
- Bauguess, S. W. (2017). The role of big data, machine learning, and AI in assessing risks: A regulatory perspective. SEC Staff White Paper, U.S. Securities and Exchange Commission.
- Coderre, D. (2009). Internal Audit: Efficiency through Automation. Hoboken, NJ: John Wiley & Sons.
- Gepp, A., Linnenluecke, M. K., O'Neill, T. J., & Smith, T. (2018). Big data techniques in auditing research and practice: Current trends and future opportunities. Journal of Accounting Literature, 40, 102–115.
- Institute of Chartered Accountants of India (ICAI). (2023). Guidance Note on Audit of Financial Instruments Using Data Analytics. New Delhi: ICAI Publications.

- Jans, M., Alles, M., & Vasarhelyi, M. A. (2014). A field study on the use of process mining of event logs as an analytical procedure in auditing. The Accounting Review, 89(5), 1751–1773.
- Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. Journal of Emerging Technologies in Accounting, 14(1), 115–122.
- Majithia, R., & Patel, K. (2021). Adoption of AI in fraud detection: Evidence from the Indian banking sector. Indian Journal of Finance and Accounting, 8(2), 44–61.
- Nigrini, M. J. (2012). Benford's Law: Applications for Forensic Accounting, Auditing, and Fraud Detection. Hoboken, NJ: John Wiley & Sons.
- OECD. (2023). Artificial Intelligence in Financial Services: Regulatory Approaches and Supervisory Practices. Paris: OECD Publishing.
- PwC India. (2024). Global Economic Crime and Fraud Survey 2024: India Perspective. New Delhi: PricewaterhouseCoopers.
- Sharma, A., & Dubey, R. (2022). Machine learning in forensic accounting: Practices and perceptions of Indian auditors. Journal of Financial Crime, 29(3), 918–934.
- Singleton, T. W., & Singleton, A. J. (2010). Fraud Auditing and Forensic Accounting (4th ed.). Hoboken, NJ: John Wiley & Sons.
- Sun, T., & Vasarhelyi, M. A. (2018). Embracing textual data analytics in auditing with deep learning. Journal of Emerging Technologies in Accounting, 15(2), 105–115.
- Vasarhelyi, M. A., & Halper, F. B. (1991). The continuous audit of online systems. Auditing: A Journal of Practice & Theory, 10(1), 110–125.
- Wells, J. T. (2017). Corporate Fraud Handbook: Prevention and Detection (5th ed.). Hoboken, NJ: John Wiley & Sons.