Volume 10, Issue 9, September – 2025 International Journal of Innovative Science and Research Technology
ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

The Integration of Artificial Intelligence in Forensic Auditing and its Implications for Real-Time Fraud Detection in Global Financial Institutions

Esther Alaka[1]; Ayomikun Eunice Akindayo[2]; Oluwafeyisike Ilemore[3]; Igba Emmanuel[4]

[1]Applied Statistics and Decision Analytics, Western Illinois University, Macomb, Illinois, USA.
[2]Department of Accounting, Omega Healthcare Investors, Maryland, United States.
[3]Darden School of Business, University of Virginia, Charlottesville, Virginia, USA.
[4]Department of Human Resource, Secretary to the Commission, National Broadcasting Commission Headquarters, Aso-Villa, Abuja, Nigeria.

Publication Date: 2025/09/26

Abstract: The integration of Artificial Intelligence (AI) into forensic auditing has emerged as a transformative approach to strengthening fraud detection and risk management within global financial institutions. Traditional auditing methods, while effective in retrospective analysis, often lack the speed and adaptability required to detect increasingly complex financial crimes in real time. AI-driven technologies, including machine learning, natural language processing, and predictive analytics, offer advanced capabilities for analyzing large volumes of transactional data, identifying hidden patterns, and uncovering anomalies that may indicate fraudulent activity. This review paper explores the evolving role of AI in forensic auditing, emphasizing its potential to enhance accuracy, efficiency, and timeliness in fraud detection processes. It further examines the practical implications for financial institutions, including improved compliance with regulatory frameworks, enhanced transparency, and proactive risk mitigation. Additionally, the review highlights challenges such as algorithmic bias, data privacy concerns, and the need for skilled professionals to interpret AI-generated insights. By synthesizing current research and industry practices, this paper provides a comprehensive assessment of how AI-enabled forensic auditing can redefine fraud detection and strengthen the resilience of financial systems in an increasingly digitized global economy.

How to Cite: Esther Alaka; Ayomikun Eunice Akindayo; Oluwafeyisike Ilemore; Igba Emmanuel (2025) The Integration of Artificial Intelligence in Forensic Auditing and its Implications for Real-Time Fraud Detection in Global Financial Institutions. *International Journal of Innovative Science and Research Technology*, 10(9), 1688-1707. https://doi.org/10.38124/ijisrt/25sep1334

I. INTRODUCTION

- *Background and Significance of Forensic Auditing in Global Finance*

Forensic auditing has emerged as a critical discipline within global finance, as financial frauds, misstatements, and irregularities increasingly threaten the integrity of financial institutions and markets. Forensic auditing goes beyond traditional external or financial audits by combining investigative accounting, legal knowledge, and analytical tools to detect and prevent fraud, misrepresentation, and money laundering (Odeyemi et al., 2024). The financial performance and credibility of multinational banks, investment firms, and regulated entities hinge on reliable financial reporting and ethical compliance; forensic auditing contributes to this by reconstructing transaction flows, tracing hidden liabilities, and verifying asset existence in ways standard auditing may not (Atalor, et al., 2023). Moreover, as audit failures or restatements can lead to large losses, legal liabilities, and reputational damage, the significance of forensic auditing is underscored in its ability to provide evidential support for legal or regulatory proceedings (Is artificial intelligence improving the audit process?, 2022). For example, forensic audits have been used to uncover earnings manipulation in public companies by analyzing off-balance-sheet items, shell company transactions, or unusual accruals that traditional audit sampling techniques might miss. In global finance contexts—e.g., cross-border banking, complex derivatives, multisubsidiary conglomerates—these techniques are especially relevant, because conventional audits are often limited by scope, sampling, and reliance on management representations (Odeyemi et al., 2024).

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

Therefore, forensic auditing plays a dual role: it assists in retrospective fraud detection and also bolsters preventive controls and assurance in economic systems. It reinforces investor confidence, regulatory enforcement, and internal governance, making it integral to the stability and transparency of financial markets globally (Atalor, et al., 2023).

➢ *Rise of Digital Financial Crimes and the Need for Advanced Solutions*

Over the past decade, financial crimes have proliferated in frequency, scope, and sophistication, propelled by digitalization, online payments, mobile banking, and the expansion of fintech ecosystems. Traditional fraud mechanisms—such as identity theft, phishing, synthetic fraud, transaction laundering, and manipulation of digital payment systems—are increasingly executed via digital channels, making them difficult to detect using legacy controls and manual oversight. The study Digital payment fraud detection methods in digital ages and Industry 4.0 demonstrates that rule-based and sampling-based detection systems are insufficient in the face of massive real-time transaction volumes and rapidly evolving fraud tactics. Machine learning and deep learning models are required to detect subtle anomalies and adapt to changing attack vectors (Atalor, & Omachi,2025). Additionally, bibliometric investigations show that academic and industry attention to AI-driven fraud detection has sharply risen, indicating both recognition of the risk and the search for scalable, advanced solutions (AI and Financial Fraud Prevention: Mapping the Trends and Challenges Through a Bibliometric Lens, 2024). These works highlight that fraud now often involves cross-border transactions, cryptocurrencies, dark web facilitation, and automation, thereby demanding detection systems that operate in near real time, integrate large heterogeneous data sources, and generate actionable insights with low false positive rates. In practice, banks dealing with tens of millions of low-value transactions per day or fintechs processing micropayments cannot afford delays in fraud detection; computational analytics, continuous monitoring, and AI offer the promise of identifying fraud as it occurs rather than after substantial losses have accumulated (Atalor, & Omachi,2025).

Hence, the rise of digital financial crime compels institutions to adopt advanced detection architectures—incorporating machine learning, anomaly detection, graph analytics, and real-time monitoring—to protect assets, maintain compliance, and preserve trust (Atalor, 2019).

➢ *Rationale for Integrating AI into Forensic Auditing*

The integration of Artificial Intelligence (AI) into forensic auditing is motivated by the need for greater efficiency, scalability, precision, and adaptability in fraud detection and investigations (Atalor, 2019). AI methods—including supervised and unsupervised machine learning, natural language processing (NLP), anomaly detection, and predictive modelling—allow forensic auditors to analyse large volumes of structured and unstructured data (e.g., transaction logs, email/text communications, contracts) far beyond what human auditors could feasibly examine (Leocádio, Malheiro, & Reis, 2024). For instance, AI-based systems can flag anomalies in transactional flows or uncharacteristic vendor relationships, or detect suspicious clustering in communication patterns, which traditional audits relying on sampling might miss (Atalor, 2022). Moreover, empirical evidence shows that investments in AI correlate with measurable improvements in audit quality and reductions in audit restatements and fees. The study Is artificial intelligence improving the audit process? found that audit firms employing AI workers experienced a statistically significant decrease in restatement likelihood (by about 5%), lower audit fees, and an eventual reduction in traditional audit labour over time, reflecting how AI complements or subsumes certain audit tasks while allowing auditors to focus on judgement, investigation, and oversight (Review of Accounting Studies, 2022). Finally, the rationale includes regulatory and stakeholder demands: global standards (such as those from IFRS, PCAOB, IAASB) increasingly expect auditors and financial institutions to adopt risk-based, technology-enabled auditing practices. AI integration helps satisfy these expectations by improving evidence reliability, increasing transparency, and facilitating compliance (Atalor, 2022).

➢ *Objectives and Scope of the Review*

The primary objective of this review is to critically examine the integration of artificial intelligence (AI) into forensic auditing and to evaluate its implications for real-time fraud detection in global financial institutions. As forensic auditing assumes an increasingly central role in ensuring financial integrity, the scope of this paper extends to exploring how AI technologies reshape the detection, investigation, and prevention of financial crimes across borders. By synthesizing existing scholarship, the review aims to highlight both the transformative benefits and the inherent challenges of AI-enabled auditing systems, positioning the discourse within the broader framework of financial crime prevention and global regulatory compliance. The scope also encompasses an assessment of AI techniques—such as machine learning, anomaly detection, and natural language processing—applied within forensic auditing to detect fraudulent transactions, irregular reporting, and concealed financial activities. This review situates its analysis within the global financial ecosystem, addressing not only the technological but also the institutional and regulatory dimensions of AI adoption. The intention is to capture a comprehensive picture that includes the strengths of AI systems in improving audit accuracy, timeliness, and efficiency, as well as the risks associated with algorithmic opacity, data privacy, and workforce readiness. Ultimately, the objectives of this review align with providing insights that are valuable to auditors, regulators, policymakers, and financial institutions. By defining the scope to integrate both academic literature and practical industry perspectives, the review underscores the importance of AI in creating resilient, transparent, and fraud-resistant financial systems, while acknowledging the complexities that accompany its global application.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

➢ *Organization of the Paper*

This paper is organized into seven main sections to provide a comprehensive and systematic exploration of the integration of artificial intelligence (AI) in forensic auditing and its implications for real-time fraud detection in global financial institutions. Following the introduction, which establishes the background, significance, and objectives of the study, Section 2 outlines the theoretical foundations of forensic auditing and AI, setting the conceptual framework for the discussion. Section 3 examines specific AI techniques applied in forensic auditing, while Section 4 focuses on their practical applications in real-time fraud detection within financial institutions. Section 5 addresses the broader implications of AI adoption, including compliance, governance, and operational efficiency. Section 6 critically evaluates the challenges and limitations associated with AI-driven forensic auditing, such as ethical concerns, data privacy, and skill gaps. Finally, Section 7 discusses future directions and presents the concluding remarks, synthesizing key insights and offering recommendations for enhancing the resilience of financial systems through AI-enabled forensic auditing. This structure ensures a logical flow, guiding the reader from conceptual foundations to applied insights and future considerations.

II. THEORETICAL FOUNDATIONS OF FORENSIC AUDITING AND AI

➢ *Evolution of Forensic Auditing Methodologies*

Over time, forensic auditing methodologies have transformed from largely manual, sample-based inspections to data-intensive, computational techniques capable of real-time and predictive detection of financial irregularities (Atalor, et al., 2023) as represented in figure 1. Early forensic auditing methods emphasized post-mortem examination of financial statements, interviews, and document inspection using judgmental sampling (Cyuma, et al., 2025). However, growing literature in fraud detection illustrates a shift: studies like Ramzan and Lokanan (2024) demonstrate that the field has evolved by embracing machine learning (ML) algorithms to identify fraudulent signatures in financial statement data. These methods include decision trees, neural networks, support vector machines, and ensemble approaches which outperform traditional statistical tests and ratio analyses, especially when dealing with non-linear relationships among fraud indicators (Atalor, et al 2023). Ali et al. (2022) provide evidence that many recent methodologies rely on large datasets, feature engineering, class imbalance correction (e.g., Synthetic Minority Oversampling Technique), and cross-validation to train models robust to overfitting (Cyuma, et al., 2025). These computational techniques contrast with earlier forensic auditing that relied instead on rules of thumb, anomalous account balance thresholds, or red-flag checklists (Atalor, & Enyejo, 2025). The shift further includes use of text analytics and unstructured data mining (e.g. email, logs) as part of evidence gathering. The evolution is also chronological: papers post-2015 increasingly report implementations of ML and AI approaches; earlier methods centered on descriptive or explanatory regression models (Atalor, & Enyejo, 2025). In sum, the current evolution in forensic auditing methodologies emphasizes real-time data ingestion, algorithmic pattern recognition, model validation, anomaly detection via unsupervised learning, and ensemble techniques. This evolution addresses limitations of sample-based detection, enhances sensitivity to subtle fraudulent signals, and reduces lag between occurrence and detection of fraud, which is critical in global financial institutions with high transaction volumes (Atalor ,2022).

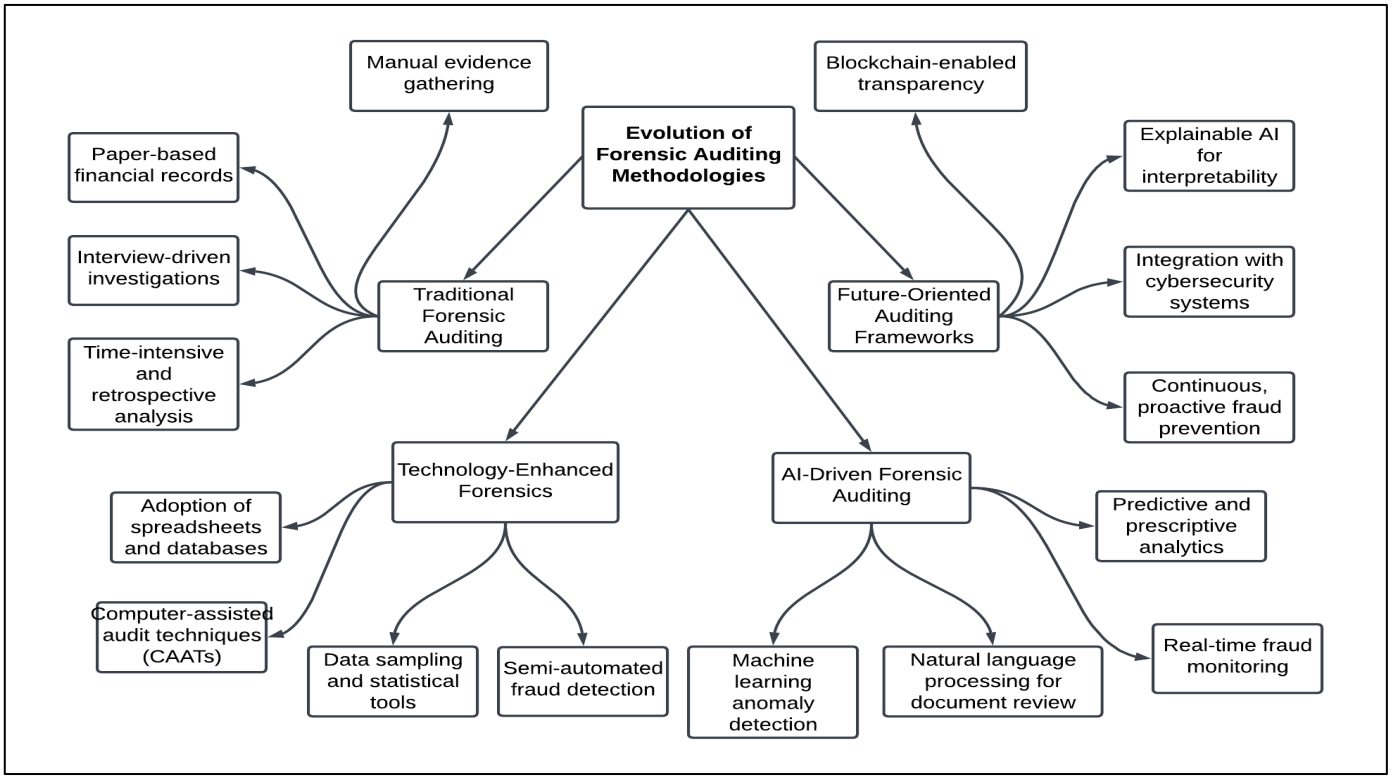

Fig 1 Evolution of Forensic Auditing Methodologies

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

Figure 1 illustrates the evolution of forensic auditing methodologies from traditional manual practices to advanced AI-driven frameworks, highlighting the paradigm shift in fraud detection. Initially, forensic auditing relied heavily on manual evidence gathering, paper-based records, and interview-driven inquiries, making the process retrospective and time-consuming. With the emergence of technology-enhanced methods, tools like spreadsheets, databases, and CAATs allowed auditors to leverage statistical sampling and semi-automated fraud detection. The transition to AI-driven forensic auditing marked a revolutionary step, where machine learning algorithms, natural language processing, and real-time predictive analytics significantly improved anomaly detection and fraud prevention efficiency. Looking ahead, future-oriented auditing frameworks are being shaped by blockchain's immutable ledger, explainable AI models, integrated cybersecurity measures, and continuous auditing systems, ensuring transparency, accountability, and proactive fraud prevention in global financial institutions.

- *Core Principles of Artificial Intelligence in Auditing*

The core principles underlying the use of artificial intelligence (AI) in auditing rest upon accuracy, transparency (or explainability), adaptability, and accountability (Atalor, & Enyejo, 2025). AI models employed in auditing must first deliver a high degree of predictive accuracy—correctly distinguishing between legitimate and illegitimate transactions, minimizing false positives and false negatives. Leocádio, Malheiro, and Reis (2024) emphasize validation techniques such as cross-validation, hold-out sample testing, and stress-testing under adversarial data to assure that models generalize across unseen datasets. Accuracy is essential for trust both within institutions and among regulators (Atalor, 2024). Transparency or explainability is a second principle: auditors, stakeholders, and regulators require models whose decision paths can be understood or interpreted (Atalor, 2024). Black-box models—e.g., deep neural networks or certain ensemble methods—must be supplemented with post-hoc interpretability tools (like SHAP, LIME) or inherently interpretable models when stakes are high (e.g., identifying fraud that may lead to legal processes). Leocádio et al. (2024) discuss that ethical principles such as fairness and non-maleficence become binding where model errors could lead to wrongful accusations or biased targeting (Atalor, & Enyejo, 2025). Adaptability is the third principle: fraud schemes evolve, so AI systems in auditing must be able to incorporate new patterns, novel data sources, streaming transaction flows, and concept drift. The Review of Accounting Studies article (2022) reveals how audit firms are investing in "AI workers" and centralized AI functions to continuously update and calibrate models in response to changing fraud risk landscapes (Imoh, & Idoko, 2022). Lastly, accountability demands clear responsibility for decisions made (or suggested) by AI-augmented systems. This includes robust governance, oversight, audit trails of AI generated decisions, alignment with regulatory compliance, and ability to challenge or explain outcomes (Imoh, & Idoko, 2022). The convergence of internal audit principles and AI best practices (e.g. transparency, fairness, and ethical accountability) is becoming more central in recent frameworks and audit firm practices (Imoh, & Idoko, 2023).

- *Intersection of AI, Data Analytics, and Fraud Detection*

At the intersection of AI, data analytics, and fraud detection lies the capacity to leverage advanced computational methods on large, heterogeneous data to reveal patterns and anomalies that would evade conventional audit procedures (Imoh, 2023). Data analytics provides the infrastructure—data cleaning, feature extraction, real-time streaming—that feeds into AI models; AI provides the pattern recognition, learning, and predictive capabilities. In the systematic review by Ali et al. (2022), numerous fraud detection efforts combine transactional data, financial ratios, governance indicators, non-financial metadata, and sometimes unstructured data to train machine learning models capable of flagging suspicious transactions or behavior (Imoh, 2023). ML classification models such as Random Forests, XGBoost, SVM, and neural networks are common, with ensemble methods being particularly effective in boosting predictive performance (Imoh, & Enyejo, 2025).

Ramzan and Lokanan (2024) emphasize this convergence further: their review reveals how accounting fraud detection literature is shifting from relying solely on statistical ratios and regression to computational methods, with ML/AI leveraging data analytics pipelines for preprocessing, dealing with class imbalance, cross-validation, and feature selection (Imoh, & Enyejo, 2025). These methods allow detection of not only known fraud types but emerging variants, such as collusive fraud, complex vendor anomalies, and digital payment fraud, where relational data and network analytics might reveal hidden links (Imoh, 2025). In practice, global financial institutions use AI-augmented data analytics to perform continuous auditing: real-time monitoring of transaction streams with anomaly detection alarms, graph analytics to detect suspicious relationships (vendor-customer, employee-supplier), and time-series models to detect sudden shifts in behavior (e.g., payment patterns) (Imoh, et al., 2025). The merging of streaming data infrastructure (big data architecture), AI model deployment, and alert generation is increasingly standard in sectors such as banking, payments, and insurance. This intersection enables not only detection but prevention and early warning, reducing lag between fraud occurrence and intervention, preserving both assets and reputation of institutions (Imoh, et al., 2025).

- *Conceptual Frameworks Guiding AI-Driven Auditing Practices*

Conceptual frameworks guiding AI-driven auditing practices serve to structure how AI is embedded in forensic auditing workflows, ensuring that technology implementation aligns with ethical, procedural, technical, and regulatory requirements as presented in table 1. One such comprehensive framework is offered by Leocádio, Malheiro, and Reis (2024) in their *Conceptual Framework for Auditing Practices*, which organizes auditing around four dimensions: real-time monitoring, risk assessment and scoring, evidence extraction from structured and unstructured data, and ethical-legal guardrails. In that framework, auditors' roles shift from purely retrospective examination to proactive oversight, leveraging continuous data flows, machine learning pipelines, and automated detection of anomalies or deviations

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

(Izundu, et al., 2025). Bias and ethics also feature centrally in frameworks. The systematic review *Bias and ethics of AI systems applied in auditing* (2024) highlights that any conceptual model must embed accountability, fairness, transparency, and data quality as core components. According to that study, conceptual models include processes for validating AI models, periodic audit of models themselves (model-audit), stakeholder engagement (including regulators, management, impacted parties), and mechanisms for explainability and oversight. These aspects are essential for ensuring that model outputs maintain credibility and defensibility, particularly in forensic contexts (Izundu, et al., 2025). These frameworks further allocate workflows for preprocessing, model training, validation, deployment, feedback loops (e.g. drift detection), and integration with legal and evidentiary standards. For instance, in an AI-driven auditing framework, after feature extraction and algorithm selection, there must be interpretability checks, performance monitoring under adversarial conditions, continuous updating of fraud risk profiles, and alignment with data protection regulations (Izundu, et al., 2025). By providing structure, these frameworks help financial institutions systematically address technical challenges (bias, overfitting, false positives), organizational challenges (skills, governance), and regulatory challenges (auditor responsibility, evidence admissibility) (Ononiwu, et al., 2023).

Table 1 Conceptual Frameworks Guiding AI-Driven Auditing Practices

Framework	Core Principles	Application in AI-Driven Auditing	Implications for Practice
Risk-Based Auditing (RBA)	Focuses on prioritizing audit resources toward areas of highest risk exposure.	AI models detect anomalies in high-risk financial transactions, automating the risk assessment process.	Enhances efficiency by targeting critical vulnerabilities, reducing false positives, and improving fraud detection accuracy.
Continuous Auditing (CA)	Promotes real-time or near-real-time monitoring of financial data flows.	Machine learning algorithms analyze streaming data to ensure timely identification of irregularities.	Enables proactive fraud detection, strengthens compliance, and supports adaptive governance.
Ethical & Accountability Frameworks	Emphasizes fairness, transparency, and explainability in AI systems.	Auditors integrate explainable AI (XAI) tools to validate decision-making processes in fraud detection.	Builds stakeholder trust, ensures regulatory compliance, and mitigates ethical risks associated with algorithmic bias.
Sociotechnical Systems Perspective	Considers the interaction between humans, technology, and organizational processes.	Human auditors collaborate with AI platforms, ensuring oversight and contextual interpretation of flagged anomalies.	Fosters balanced decision-making, bridges skills gaps, and aligns AI adoption with organizational culture.

III. AI TECHNIQUES IN FORENSIC AUDITING

➢ *Machine Learning Algorithms for Anomaly Detection*

Machine learning algorithms have become central in forensic auditing for spotting anomalous patterns and potential fraud, particularly in high-volume, high-velocity financial datasets such as general ledger (GL) entries as represented in figure 2 (Ononiwu, et al., 2023). Supervised learning models (e.g., Random Forest, Gradient Boosting Trees) have been trained on labelled examples of known fraud or misstatements, enabling auditors to classify journal entries or transactions automatically as high risk or low risk (Bakumenko & Tropmann-Frick, 2022). These models are especially useful for detecting known fraudulent schemes, but their performance depends heavily on the availability of high-quality labelled data, balanced classes, and robust cross-validation procedures to avoid overfitting (Ononiwu, et al., 2023). Unsupervised learning approaches (e.g., Isolation Forest, autoencoders) are particularly valuable where fraud patterns are unknown or evolving; they detect deviations from established norms without requiring labelled data (Schreyer, Sattarov, Borth, Dengel, & Reimer, 2017). For example, deep autoencoder networks have been applied to large-scale accounting data to reconstruct typical transaction patterns; journal entries with high reconstruction error (i.e. those which cannot be reconstructed well) are flagged as anomalies (Schreyer et al., 2017). Similarly, Bakumenko and Tropmann-Frick (2022) implement both supervised and unsupervised models on real GL datasets and show that unsupervised techniques like isolation forest or autoencoder catch anomalous entries not previously labelled (Ononiwu, et al., 2023). Beyond that, hybrid models that combine supervised and unsupervised components increase detection sensitivity and reduce false positives, by using unsupervised methods to surface candidates for investigation and supervised models to verify. Audit teams are moving toward more automated pipelines that include feature engineering (e.g., combining categorical and numerical features, transforming transaction metadata), model explainability (e.g. using SHAP or LIME) and continuous retraining to adapt to new types of fraud (Bakumenko & Tropmann-Frick, 2022).

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

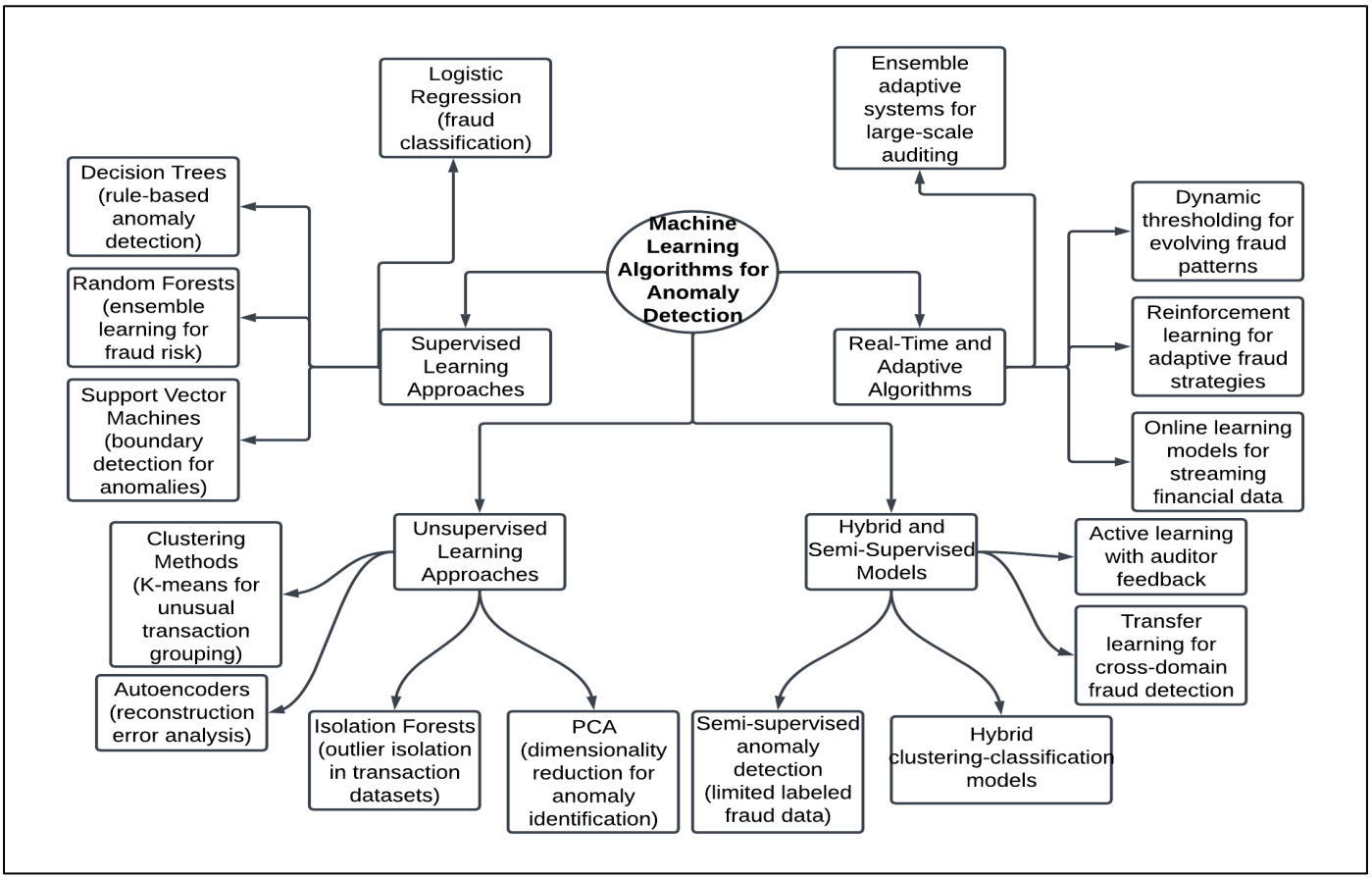

Fig 2 Machine Learning Algorithms for Anomaly Detection

Figure 2 demonstrates the taxonomy of machine learning algorithms applied in anomaly detection for forensic auditing, emphasizing their role in combating financial fraud. Supervised learning approaches rely on labeled data to build predictive fraud detection models, with algorithms like decision trees and support vector machines enabling interpretable classification. Unsupervised methods focus on detecting unknown fraud patterns, where clustering, autoencoders, and isolation forests are crucial in uncovering subtle anomalies in high-dimensional financial datasets. Hybrid and semi-supervised models bridge the gap between limited labeled fraud data and the vast amounts of unlabeled transactions, leveraging techniques such as transfer learning and active learning with human auditors to enhance detection accuracy. Finally, real-time and adaptive algorithms ensure continuous monitoring of financial systems, adjusting dynamically to evolving fraud strategies through reinforcement learning and streaming analytics. Together, these branches highlight a multi-layered AI-driven framework that improves anomaly detection robustness, transparency, and responsiveness in global financial auditing.

- *Natural Language Processing for Document and Communication Analysis*

Natural Language Processing (NLP) is increasingly leveraged in forensic auditing to process unstructured text—such as invoices, contracts, emails, internal memos, or chat logs—to detect indicators of fraud or misstatements. For instance, Boulieris, Symeonidis, and Sergiadis (2024) introduce *FraudNLP*, a public dataset of user actions and transactions, showing that online banking transaction sequences framed as natural language features can improve detection rates with lower custom feature-engineering effort (Ononiwu, et al., 2023). They demonstrate that features derived from pre-trained language models (e.g. embeddings capturing user behavior sequences) outperform many traditional engineered features in distinguishing fraudulent vs. non-fraudulent transactions (Ononiwu, et al., 2023). Similarly, (Jagdale& Deshmukh 2025) describe applications of NLP in financial text analytics, including named-entity recognition (NER) to identify parties, obligations, and unusual contract terms; sentiment analysis of communications; and topic modeling to cluster documents for anomalous themes (e.g. recurring references to high-risk terms such as “urgent payment,” “discount misclassification,” or “unapproved supplier”). They also discuss transformer models (BERT, RoBERTa) and domain adaptation, where financial-domain fine-tuning improves performance relative to general language models (Ononiwu, et al., 2023).

In forensic auditing practice, NLP helps auditors automate tedious document reviews, extract key risk indicators from text, detect inconsistent or conflicting information across documents (e.g., mismatched purchase orders vs. invoice descriptions), and flag suspicious internal communications. The combination of structured transaction data with unstructured text provides richer context for anomaly detection and can enable early detection of fraud schemes that rely on misleading narrative disclosures or

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

forged documents (Boulieris et al., 2024; Wibawa et al., 2024).

➢ *Predictive and Prescriptive Analytics for Fraud Risk Assessment*

Predictive analytics involves using historical and real-time data to forecast fraud risk, estimating probabilities of future fraud occurrences, whereas prescriptive analytics goes further to suggest actions to mitigate those risks (Ononiwu, et al., 2025). In auditing contexts, predictive models may forecast which vendors, transaction types, or client relationships are likely to yield unusual or fraudulent behavior—based on variables such as transaction size/frequency, account irregularities, temporal patterns, external economic indicators, or prior audit findings (Addy & Sanni, 2024). For example, credit risk models are being adapted to fraud risk: features indicating anomalous behavior are used alongside macroeconomic predictors to segment risk and allocate audit resources accordingly as presented in table 2 (Ononiwu, et al., 2025). Prescriptive analytics builds on such forecasts by recommending auditing strategies: which specific transactions to sample more heavily, what thresholds for alerts or red flags to set, and how to configure internal control responses. The study in (Javaid, 2024). shows financial service firms using predictive risk scores combined with scenario analysis and optimization techniques to decide optimal audit paths—choosing between manual review, automated flags, or escalations for high-risk cases (Javaid, 2024). A typical implementation pipeline involves data gathering (both structured transactional data and external data such as news or regulatory reports), feature engineering (temporal trends, behavior baselines), model training (supervised ML), validation (ROC, precision/recall, cost curves), predictive scoring, and then prescription: rules or decision support tools that suggest control actions, resource allocation, or automated responses (Ononiwu, et al., 2024). Real-time or near-real-time predictive scoring enables faster detection of fraud and helps reduce exposure. Financial institutions integrating prescriptive analytics report lowered response times, better prioritization of investigations, and improved ROI on forensic investigations because prescriptive guidance helps prevent fraudulent losses rather than merely detecting them after the fact (Addy & Sanni, 2024; JIER, 2024).

Table 2 Predictive and Prescriptive Analytics for Fraud Risk Assessment

Analytics Type	Core Principles	Application in Fraud Risk Assessment	Implications for Practice
Predictive Analytics	Uses historical data, statistical models, and machine learning to forecast potential fraud risks.	Identifies suspicious transaction patterns, unusual behavior, and high-risk entities before fraud occurs.	Improves proactive risk management and reduces financial losses by anticipating fraudulent activity.
Prescriptive Analytics	Goes beyond predictions by recommending optimal actions and decision pathways.	Suggests targeted interventions such as enhanced due diligence, transaction blocking, or adaptive monitoring rules.	Enables auditors and regulators to act decisively, improving fraud prevention strategies and compliance.
Hybrid Models (Predictive + Prescriptive)	Integrates forecasting with decision-making optimization for dynamic fraud management.	AI-driven tools simultaneously flag anomalies and recommend corrective actions tailored to risk levels.	Enhances real-time response capability and reduces reliance on manual auditing.
Organizational Implementation	Embeds predictive and prescriptive models into enterprise risk management systems.	Automated fraud dashboards, continuous monitoring tools, and scenario simulations guide strategic planning.	Strengthens governance, ensures regulatory compliance, and boosts resilience against evolving fraud schemes.

➢ *Intelligent Automation and Robotic Process Automation in Auditing*

Intelligent automation, including Robotic Process Automation (RPA), augments forensic auditing by automating repetitive, rules-based tasks, thereby freeing human auditors to focus on judgment, anomaly investigation, and complex decision making. Huang and Vasarhelyi (2019) articulate how RPA is being applied in auditing for tasks such as reconciling inventory, matching accounts, validating transactional consistency, and extracting data from fixed-format systems. These automation bots follow predefined rules but can be configured to trigger alerts when encountering exceptions—for instance, mismatched vendor names, unexpected account types, or deviations in totals—with audit logs preserved for evidence and traceability (Ononiwu, et al., 2024). (Perdana, et al., 2023) report on implementation in multiple audit firms: RPA was used to prototype and automate data extraction from various ERP systems, perform preliminary data cleansing, schedule repetitive audits, and generate standardized audit workpapers. Their findings indicate that using RPA reduces processing time by up to 40%, reduces manual error, and improves auditor satisfaction (Ononiwu, et al., 2025). However, they also note that RPA implementation requires careful oversight to ensure bots follow correct logic, maintain data security, integrate with AI models for risk scoring, and provide an audit trail such that outputs are defensible in regulatory inspections (Perdana, et al., 2023). In the context of fraud detection, intelligent automation complements AI-driven models by executing operational tasks: feeding data pipelines, monitoring flagged transactions, triggering initial investigations, ensuring compliance with prescribed

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

thresholds, and gathering evidence from multiple systems (Ononiwu, et al., 2025). When combined with ML anomaly detection and prescriptive analytics, RPA can operationalize fraud detection into continuous, near real-time monitoring, closing the gap between model detection and practical response (Ononiwu, et al., 2025).

IV. APPLICATIONS IN REAL-TIME FRAUD DETECTION

➢ *Transaction Monitoring and Anomaly Detection Systems*

Transaction monitoring systems enhanced with anomaly detection algorithms represent one of the frontline defenses in real-time fraud detection by global financial institutions (Ononiwu, et al., 2025). The hybrid framework proposed by Robu, Zhang, and Farkas (2023) illustrates how combining techniques such as SMOTEBoost for imbalance handling, adversarial training, FraudGAN for synthetic fraud generation, drift detection algorithms (e.g., DDM, ADWIN), and explainability tools (SHAP, LIME) can result in significantly improved recall rates and reduced false positives while maintaining low latency in production settings (Ononiwu, et al., 2023). Such systems continuously ingest transactional data streams (payments, transfers, account activity) and apply supervised or semi-supervised models to classify or score transactions for anomaly risk (Ononiwu, et al., 2025). Hemati, Schreyer, and Borth (2021) investigate unsupervised anomaly detection through continual learning on real journal entry data—financial accounting data that arrives in streaming form. Their work demonstrates that models which continuously update, rather than relying only on periodic batch processing, can adapt to shifting distributions, reduce both false positive and false negative rates, and better capture emerging fraud patterns. In practice, financial institutions deploy architectures with dual streams: a real-time detection stream that monitors incoming transactions, often with simpler and lower-latency models, and a batch retraining stream that updates models with accumulated data, feeding into the real-time pipeline (Ononiwu, et al., 2023). These systems also include risk thresholds, feedback loops, human-in-the-loop review for flagged anomalies, and model monitoring for concept drift or adversarial inputs (Azonuche et al., 2025). For example, in the GCC hybrid framework, adversarial robustness is tested via simulated attacks, and drift detection allows the system to adjust thresholding or retrain when behavior changes occur. Overall, transaction monitoring with anomaly detection draws on large-scale streaming architectures, continuous model training, and careful trade-offs among detection speed, accuracy, explainability, and operational cost (Robu et al., 2023; Hemati et al., 2021).

➢ *Continuous Auditing and Proactive Fraud Prevention*

Continuous auditing is increasingly adopted within global financial institutions as part of moving from retrospective fraud detection to proactive prevention as presented in table 3 (Azonuche et al., 2025). Javaid and Nobanee (2023) survey how blockchain data (immutable, append-only ledgers) combined with AI enables real-time accounting and auditing practices, making it possible to detect deviations almost as soon as they occur. The literature emphasizes themes like triple entry accounting and event-based recording that feed into continuous auditing systems, which monitor internal controls and transactions continuously rather than only at fixed periods (Azonuche et al., 2025). These systems allow earlier identification of irregularities, potential misstatements, unusual patterns of behavior, or control breakdowns (Azonuche, & Enyejo, 2024). The continual learning framework by Hemati, Schreyer, and Borth (2021) supports this shift: their model for unsupervised anomaly detection uses streaming journal entry data so that auditors can observe shifts in patterns across time, reducing delay between when fraud begins and when it is detected. This allows internal audit functions to move beyond scheduled or periodic sampling to dynamic risk estimation and more frequent, even near-real-time, checks. Proactive fraud prevention emerges through continuous risk scoring of accounts, vendors, or transaction channels; alerting when risk thresholds are breached; implementing automated or semi-automated control measures; and feeding these alerts back into internal risk governance (Azonuche, & Enyejo, 2024). Financial institutions implementing continuous auditing benefit from lower loss exposure, faster response time, and more efficient resource allocation: instead of waiting for end-of-period audits to detect fraud that may have gone unchecked for months, continuous auditing frameworks detect emerging threats early, enabling remediation before damage accumulates (Azonuche, & Enyejo, 2024). Key technical enablers include streaming data pipelines, automated monitoring of control metrics, continuous model retraining, and integration with governance and compliance processes (Javaid & Nobanee, 2023; Hemati et al., 2021).

Table 3 Continuous Auditing and Proactive Fraud Prevention

Key Aspect	AI-Driven Application	Impact on Auditing	Implications for Financial Institutions
Real-Time Monitoring	AI models continuously analyze transactions and financial records.	Enables early detection of suspicious activities before escalation.	Improves fraud resilience and reduces financial losses.
Risk-Based Alerts	Machine learning generates anomaly-based alerts for high-risk behaviors.	Auditors focus on critical cases instead of random sampling.	Enhances efficiency in fraud prevention strategies.
Predictive Analytics	Historical fraud patterns inform predictive models.	Supports proactive decision-making and risk mitigation.	Institutions anticipate and address vulnerabilities before exploitation.
Automated Compliance	AI automates compliance checks with regulatory frameworks.	Ensures consistent audit coverage with reduced human error.	Strengthens trust, accountability, and adherence to global standards.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

➢ *Integration of AI with Blockchain and Digital Ledgers*

The integration of AI with blockchain and digital ledger technologies offers powerful synergies for forensic auditing and real-time fraud detection. Javaid and Nobanee (2023) survey how blockchain's properties—immutability, consensus-driven verification, shared append-only ledgers—can undergird AI systems by supplying reliable, tamper-evident data streams for audit and anomaly detection (Azonuche, & Enyejo, 2024). This ensures that transaction data is less susceptible to manipulation, legitimizing the inputs to AI models. It enables real-time accounting and continuous auditing, as each transaction or event entered into the blockchain can be immediately ingested and assessed (Azonuche, & Enyejo, 2024). Louati et al. (2025) propose frameworks specifically for smart contracts: their AI-Based Anomaly Detection and Optimization Framework for Blockchain Smart Contracts detects deviations in contract states, gas usage, or transaction sequences within the blockchain environment. The framework uses both anomaly detection algorithms and optimization layers to correct or flag suspicious behaviors in smart contract execution (Azonuche, & Enyejo, 2024). Examples include detection of abnormal interactions with smart contract functions, abnormal patterns in asset transfers, or unexpected invocation sequences, especially on permissioned blockchain platforms where identity and access can be controlled (Azonuche, & Enyejo, 2024). In practice, financial institutions implementing the integration use permissioned blockchains for inter-bank settlements, KYC/AML record sharing, or supply chain finance, which paired with AI models allow cross-ledger anomaly detection, fraud scenario simulation, and end-to-end transaction traceability (Azonuche, & Enyejo, 2025). Digital ledger integrations enhance audit trails and evidence support for forensic investigations, enabling auditors to verify data provenance, detect ledger tampering, and match off-chain with on-chain records for consistency. Such integrations help minimize fraud schemes relying on data manipulation or off-system adjustments, improving the detection—and often prevention—of fraudulent behaviors (Javaid & Nobanee, 2023; Louati et al., 2025).

➢ *Case Studies of AI Deployment in Financial Institutions*

Robu, Zhang, and Farkas (2023) provide a compelling case study of banks in the Gulf Cooperation Council (GCC) region deploying a hybrid machine learning fraud detection system that addresses class imbalance, concept drift, adversarial threats, and requirement for explainability as represented in figure 3 (Azonuche, & Enyejo, 2025). Their system increased fraud recall from about 35% using traditional methods to around 85% post-implementation; adversarial robustness improved substantially, and latency (response time) was kept under 150 milliseconds – sufficient for real-time or near real-time transaction monitoring. The practical challenges encountered included integrating the system into legacy processing pipelines, ensuring regulatory compliance (data privacy, model auditability), and establishing human-in-the-loop oversight for flagged transactions (Azonuche, & Enyejo, 2024). Adelakun, Onwubuariri, Adeniran, and Ntiakoh (2024) review multiple case studies including large financial institutions that applied AI techniques (machine learning, NLP, data mining) to combat credit card fraud, procurement fraud, and internal document anomalies (Idika, et al., 2023). For example, one bank used ML-based anomaly detection on credit card transaction streams and reduced false positive rates by consolidating pattern-based features and adapting thresholds regularly. In another case, a multinational firm integrated document analysis using NLP to identify fraudulent invoices misaligned with purchase orders, uncovering schemes that traditional internal audits missed. Government agencies also benefited: procurement fraud detection using historical procurement data allowed prevention of irregular awarding of contracts (Idika, et al., 2023). These case studies underline that AI deployment must be supported by strong data infrastructure, governance, oversight, interpretability tools, and periodic auditing of the AI models themselves to maintain trust and effectiveness (Robu et al., 2023; Adelakun et al., 2024).

Figure 3 shows a collaborative team of professionals gathered around a laptop, analyzing data and documents, which effectively symbolizes case studies of AI deployment in financial institutions. It highlights the multidisciplinary collaboration between auditors, data scientists, and financial experts required to successfully implement AI solutions. The focus on the laptop and visual data indicates the use of advanced AI-driven tools for detecting fraud patterns, monitoring real-time transactions, and enhancing compliance within financial systems. The engaged and interactive nature of the discussion reflects how AI deployment often requires human oversight, contextual interpretation, and decision-making support to validate algorithmic outputs. This representation captures the essence of financial institutions adopting AI not merely as a technological upgrade but as a transformative approach to strengthen fraud detection, improve operational efficiency, and build organizational trust through teamwork and innovation.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

Fig 3 Collaborative Deployment of AI Solutions in Financial Institutions (Dr Emily 2024)

V. IMPLICATIONS FOR GLOBAL FINANCIAL INSTITUTIONS

- *Enhancing Compliance with International Regulatory Standards*

Enhancing compliance with international regulatory standards through the integration of AI in forensic auditing involves aligning audit practices with evolving mandates such as the EU AI Act, PSD2, SOX, Basel III/IV, and global anti-money laundering (AML) and counter-terrorist financing (CTF) requirements (Idika, et al., 2024). Adeyelu, Ugochukwu, and Shonibare (2024) conduct a systematic literature review showing that AI systems have the capacity to automate regulatory compliance mapping, monitor changes in regulation texts via natural language processing, and deploy continuous compliance checks—thus reducing the risk of manual oversight or missed regulatory updates. For example, AI algorithms can parse new regulatory documents, extract obligations, and flag areas where current processes diverge from updated mandates (Idika, et al., 2023). Meanwhile, The necessity of AI audit standards boards (2025) argues for the establishment of external, credible standards boards which set consistent auditing and AI usage standards worldwide. This would reduce regulatory arbitrage across jurisdictions, ensure consistency in how AI audit tools are tested, validated, and certified, and enforce transparency in internal audit functions. It also underscores the need for audit standardization bodies to incorporate governance for explainability, fairness, data protection, and audit trail requirements (Idika, et al., 2024). In practice, financial institutions adopting AI for forensic auditing are able to automate portion of compliance reporting (e.g. Know Your Customer, AML data requirements), generate real time risk assessments against international sanction lists, and demonstrate auditability of systems to regulators. The integration of AI thus enhances compliance by providing (a) quicker adaptation to regulatory changes, (b) richer evidence trails for audits, (c) reduced regulatory violations or fines, and (d) improved confidence among stakeholders that global regulatory standards are being adhered to rigorously (Idika, et al., 2024).

- *Strengthening Internal Controls and Governance Mechanisms*

Strengthening internal controls and governance mechanisms via AI in forensic auditing involves embedding AI-enabled risk assessment, monitoring, and control validation within organizational structures and policy frameworks. Almaqtari (2024) explores IT governance practices as a foundation for integrating AI within accounting and auditing, emphasizing that AI tools must be governed by clear information security policies, data ownership, control rights, role definitions, and oversight functions. For example, an AI system monitoring payment approval must have

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

governance rules that define who reviews flagged transactions, how escalations occur, and how models are audited for performance as presented in table 4 (Idika, et al., 2023). The study from Jordan in *Sustainability* (2025) provides empirical evidence that AI adoption correlates with improved corporate governance effectiveness ($R^2 \approx 0.58$) and risk management ($R^2 \approx 0.50$), demonstrating that firms which integrate AI into governance mechanisms—such as internal audit committees, board oversight, compliance units—tend to report fewer control breakdowns, more robust internal control quality, and enhanced oversight of management (Amebleh& Igba 2024). Technically, AI can help enforce segregation of duties via automated workflows, perform continuous control testing (e.g. validating ledger reconciliations daily), monitor policy adherence (e.g. expense policies, vendor onboarding), and produce dashboards for governance committees with risk indicators. Effective governance ensures the AI models themselves are periodically reviewed (model governance), version controlled, and traceable so that decision paths are documented. By doing so, institutions reduce internal fraud risk, improve control environment maturity, and ensure that forensic auditing is not just reactive but embedded into daily operations (Amebleh& Igba 2024).

Table 4 Strengthening Internal Controls and Governance Mechanisms

Aspect of Governance	AI Application	Key Outcomes	Implications for Practice
Risk Management	AI-powered predictive analytics to identify control weaknesses and emerging risks.	Early detection of vulnerabilities, reduced fraud exposure, and proactive intervention.	Enables financial institutions to anticipate threats and strengthen risk management frameworks.
Compliance Oversight	Automated monitoring systems using AI for adherence to international standards.	Real-time detection of regulatory breaches and improved audit trails.	Enhances accountability while reducing manual oversight errors.
Decision-Making Transparency	Machine learning models for anomaly detection in governance reporting.	Improved transparency, consistent reporting, and unbiased auditing decisions.	Supports trust among stakeholders and reinforces ethical governance practices.
Operational Control	Robotic Process Automation (RPA) to enforce segregation of duties and internal checks.	Reduced operational inefficiencies, minimized human error, and stronger internal control systems.	Strengthens organizational integrity and safeguards against insider threats.

- *Improving Transparency and Accountability in Financial Reporting*

AI contributes significantly to transparency and accountability in financial reporting by facilitating more accurate disclosures, reducing errors, and enabling continuous monitoring of financial statement items (Alhazmi, Islam, and Prokofieva 2025) as represented in figure 4. examine firms listed on the Saudi Stock Exchange and find that AI adoption leads to measurable improvements in the quality of financial reports—reducing restatements and errors in revenue recognition and enhancing the consistency and reliability of disclosures. AI-based tools help extract insights from unstructured data (e.g., footnotes, management discussion & analysis) and detect inconsistencies or omissions that manual review might miss (Abiodun, et al., 2024). The review by Jejeniwa, Zamanjomane, and Jejeniwa (2024) further articulates that AI systems in accounting enable automated validation of data, reconciliation across multiple reporting systems, and enhanced error detection (Igba, et al., 2025). For example, anomalies between subsidiary ledgers and consolidated financial statements, or mismatches in internal reports versus external filings, can be flagged automatically. Also, AI-driven visualization and reporting tools provide stakeholders—including regulators, investors, and audit committees—with real-time dashboards, metrics, and disclosures, boosting accountability (Abiodun, et al., 2024). Moreover, accountability is strengthened by maintaining audit trails of AI model decisions, ensuring explainability of model decisions for material judgments (e.g., impairment testing, provisions), and allowing third-party or regulatory audits of AI systems (Igba, et al., 2025). Transparency is thus not limited to what is reported externally but also internal processes: how certain estimates are derived, how data is validated, and how model assumptions align with regulatory requirements (Abiodun, et al., 2025). The result is stronger stakeholder trust, reduced information asymmetry, and improved detection (or deterrence) of financial reporting fraud.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

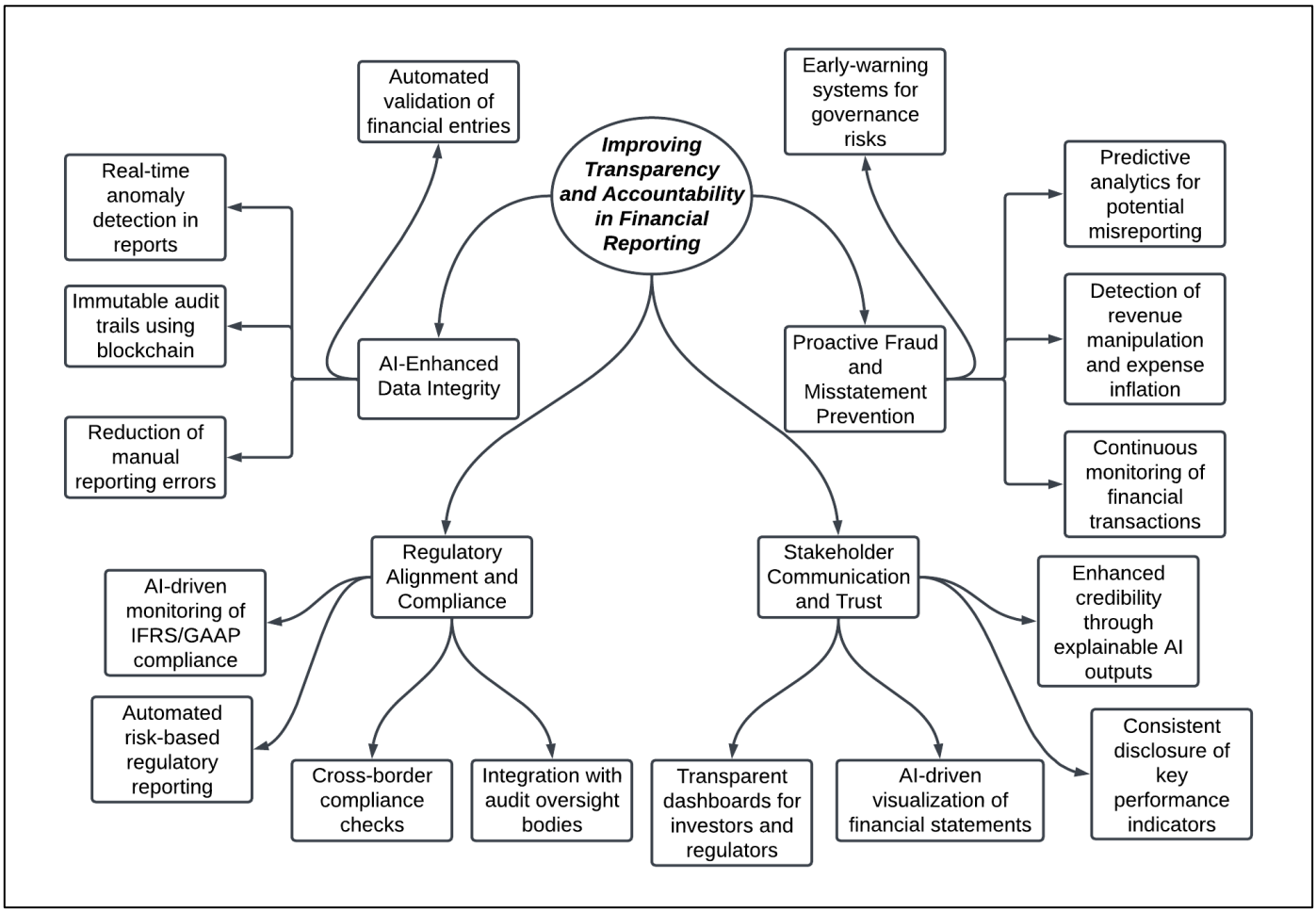

Fig 4 Improving Transparency and Accountability in Financial Reporting

Figure 4 illustrates how AI integration enhances transparency and accountability in financial reporting, forming a robust framework for accurate, reliable, and regulatorily compliant disclosures. AI-enhanced data integrity ensures that every transaction and reporting entry is validated in real time, leveraging blockchain for immutable audit trails to reduce risks of tampering or error. Regulatory alignment and compliance are strengthened by AI systems that automatically check adherence to global standards like IFRS and GAAP while enabling cross-border compliance through adaptive reporting mechanisms. Stakeholder communication and trust is improved through AI-powered dashboards and visualization tools that make financial statements more understandable and verifiable, fostering credibility with regulators, investors, and the public. Finally, proactive fraud and misstatement prevention utilizes continuous monitoring and predictive analytics to detect manipulations, flag inconsistencies, and provide early warnings of governance risks. Collectively, these dimensions highlight AI's transformative role in ensuring transparent, trustworthy, and accountable financial reporting practices in global financial institutions.

- *Opportunities for Cost Reduction and Operational Efficiency*

Opportunities for cost reduction and operational efficiency arise when forensic auditing leverages AI to automate tasks, streamline workflows, and reduce human labour and error. The study Is Artificial Intelligence Improving the Audit Process? (2022) finds that audit firms which have invested substantially in AI see a reduction in audit restatement frequencies (≈5 %) and a reduction in audit fees (≈0.9 %) in the short term, with larger efficiencies accruing over longer horizons. This suggests that automation of data extraction, risk assessment, anomaly detection, and sampling can reduce the manpower and time required for these tasks, thereby lowering costs (Abiodun, et al., 2025). Similarly, Impact of Artificial Intelligence and Industry 4.0 on transforming accounting and auditing practices (2024) shows valid empirical relations between AI, big data, cloud computing, and deep learning with improved audit efficiency and accuracy in Saudi Arabia. Firms adopting these technologies report faster turnaround times in audit cycles, fewer manual reconciliations, quicker error detection, and less duplication of effort. For instance, data processing in audit tasks that previously required multi-day manual review is compressed to hours or minutes (Abiodun, et al., 2025). Operational efficiency is further enhanced through predictive maintenance of controls (anticipating control failures), minimal error correction costs, reuse of audit assets (templates, model components), centralized AI tool development, and shared infrastructure (cloud platforms). Moreover, cost savings are realized in reduced overheads (less manual review, fewer corrections, less staff hours), but

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

also in improved scalability: as institutions scale up transaction volume, model-based processing handles growth without proportional increase in staffing. In financial institutions with high transaction volumes, these operational efficiencies can materially improve margins and allow more resources to be allocated to investigative, judgmental, or strategic tasks (Igba, et al., 2025).

VI. CHALLENGES AND LIMITATIONS

➢ *Algorithmic Bias and Ethical Concerns in Fraud Detection*

Algorithmic bias and ethical concerns arise when fraud detection systems inadvertently replicate or exacerbate pre-existing inequalities or unfair treatment of individuals due to biased training data, disproportionate false positive rates, or opaque decision rules. Murikah and Murgo (2024) identify multiple sources of bias in auditing AI systems, including imbalanced datasets (e.g. fraud cases much rarer than non-fraud), proxies for sensitive attributes, or historical biases encoded in transactional data that reflect socioeconomic or regional disparities. Such biases can lead to unfair targeting of certain groups or erroneous accusations, imposing ethical as well as legal risks. Transaction fraud models pose unique ethical challenges: Kamalaruban et al. (2024) show that fairness metrics that do not account for class imbalance may understate bias; models that aim for high recall (catching more fraud) may generate many false positives, which disproportionately penalize legitimate customers, undermining trust. Their analysis demonstrates that simple removal of sensitive attributes ("fairness through unawareness") is often insufficient, because correlated proxies persist, embedding bias (Igba, igba et al., 2025). Beyond fairness, ethical concerns include privacy, consent, transparency, accountability, and the potential harm of misclassification (Igba, igba et al., 2025). Fraud detection systems must balance aggressiveness (catching fraud early) with not penalizing innocent actors (Igba, et al., 2025). Ethical AI also requires human oversight (human-in-the-loop) so flagged events can be reviewed, and mechanisms for remediation if wrongful actions occur. Ethical guidelines and institutional policies should mandate bias assessments, fairness audits, impact statements, and continuous monitoring (Igba, igba et al., 2025). Integrating bias-mitigation techniques (e.g. adversarial debiasing, reweighing, fairness constraints), ensuring diversity in training data, conducting regular audits, and embedding ethical norms into design and deployment are crucial. Only then can AI-forensic auditing not just be effective, but also just and socially responsible (Igba, igba et al., 2025).

➢ *Data Privacy, Security, and Cross-Border Legal Complexities*

Data privacy, security, and cross-border legal complexities present significant limitations to AI-driven forensic auditing, especially when financial institutions operate across multiple jurisdictions. (Ayodele, et al., 2025) investigates how Anti-Money Laundering (AML) operations that rely on AI require extensive cross-border data sharing, but such sharing is constrained by conflicting data protection laws such as the EU's GDPR, data localization requirements, and regional sovereignty laws (Alaka, et al., 2025). These legal tensions can impede the aggregation, processing, and transfer of transactional, customer, or communication data necessary for high-accuracy fraud detection (Alaka, et al., 2025). Security risks are amplified by large, heterogeneous datasets (e.g. combining transactional, behavioral, device, identity metadata) that must be stored, processed, and transmitted securely (Alaka, et al., 2025). Data breaches, unauthorized access, or adversarial attacks on model inputs or training data can lead to exposure of sensitive information, non-compliance penalties, or reputational harm. Bolgouras et al. (2025) examine key EU regulatory instruments (AI Act, GDPR, NIS2) and highlight how they demand risk-management, privacy by design, and strong security measures. However, the overlap among different legal frameworks often creates compliance burdens, uncertainty, and ambiguity about which obligations dominate in cross-jurisdictional operations (Ogbuonyalu, et al., 2025). Operationally, institutions must implement robust governance frameworks, strong encryption, secure data pipelines, data minimization, anonymization or pseudonymization, access control, and clear logging (Ogbuonyalu, et al., 2025). Legal agreements (data sharing, cross-border transfer) and clarity in international treaty obligations are required (Okpanachi etal., 2025). For real-time fraud detection to function effectively globally, AI systems must navigate varying privacy norms, ensure lawful data acquisition, and maintain data integrity and availability (Ogbuonyalu, et al., 2025). Non-compliance can result in heavy fines and legal enforcement actions, making privacy and legal issues not peripheral but core to design and deployment of AI in forensic audit systems.

➢ *Limitations in Model Interpretability and Explainability*

Model interpretability and explainability remain key challenges in AI-driven auditing and fraud detection because many high-performing models (e.g. deep neural networks, ensemble methods) function as "black boxes." Černevičienė, Budria, and Skaržauskienė (2024) note that while these models often achieve superior predictive performance, their internal decision paths are difficult for auditors, regulators, or affected stakeholders to understand (Okpanachi etal., 2025). In contexts where audit judgements, regulatory compliance, or legal evidence are required, such opacity undermines trust and accountability as presented in table 5 (Abiodun, et al., 2023). Yeo, Okazaki, Sato, and He (2025) expand on these limitations, pointing out that post-hoc explainability tools (SHAP, LIME, attention maps) while useful, often work at either local (single instance) or feature-importance levels; they may not capture global behaviours, interactions among features, or non-linearities in model internals. Additionally, explanations may be misleading or unstable (small perturbations in input can change explanations), making them unreliable for decision justification in high stakes settings (Abiodun, et al., 2023). In forensic auditing especially, material decisions like whether to escalate a transaction, initiate legal proceedings, or report to regulators depend on clear reasoning (Abiodun, et al., 2023). Where models are opaque, auditors may struggle to defend or explain these decisions (Okpanachi etal., 2025). Furthermore, some regulatory regimes require transparency and explainability

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

(e.g., EU AI Act, upcoming auditing standards) which black-box models may fail to satisfy. There is also a trade-off: increasing interpretability often comes at the cost of predictive performance or ability to detect subtle anomalies (Ogbuonyalu, et al., 2024).

Techniques such as using inherently interpretable models (e.g. decision rules, transparent classifiers), combining interpretable parts with black-box parts, or constructing aggregated explanations at attribute or group levels (as in methods like RESHAPE) help, but require additional engineering, may increase computation, and might not scale easily in real-time monitoring environments (Ogbuonyalu, et al., 2025).

Table 5 Limitations in Model Interpretability and Explainability

Challenge	AI Context	Impact on Forensic Auditing	Implications for Practice
Black-Box Nature	Deep learning models (e.g., neural networks) operate with complex internal mechanics not easily interpretable.	Auditors cannot fully justify fraud detection decisions, undermining credibility.	Requires adoption of explainable AI (XAI) to enhance transparency and trust.
Regulatory Compliance	Lack of model clarity limits compliance with auditing standards demanding rationale for decisions.	Risk of regulatory penalties or rejection of audit findings.	Institutions must integrate interpretable models to meet compliance mandates.
Stakeholder Trust	Difficulty in explaining AI-driven insights to boards, regulators, or clients.	Reduced acceptance of AI outcomes in critical fraud detection scenarios.	Necessitates user-friendly visualization and model-agnostic explanation tools (e.g., SHAP, LIME).
Complex Data Environments	Models struggle to provide interpretable outputs in multi-source financial data streams.	Limits forensic auditors' ability to connect anomalies with actionable insights.	Calls for hybrid frameworks combining AI outputs with human expert judgment.

- *Skills Gap and Workforce Readiness in AI-Driven Auditing*

A skills gap and deficient workforce readiness are major impediments to effectively deploying AI in forensic auditing. Kokina and Leung (2025) examine auditing practices in large public accounting firms and reveal that while there is growing investment in AI technologies, many auditors lack technical proficiency (e.g. in data science, ML modelling, software engineering), ethical literacy (bias, privacy, fairness), and domain-knowledge integration (Uzoma et al., 2024). Consequently, audit firms face challenges in hiring or training personnel capable of interpreting model outputs, managing AI pipelines, and ensuring regulatory compliance as represented in figure 5 (Ogbuonyalu, et al., 2024). Similarly, Wassie et al. (2024) in their review of the internal audit function (IAF) point out that many current auditors are trained under traditional audit curricula which emphasize manual sampling, control testing, and financial reporting, with limited exposure to AI, programming, or continuous monitoring techniques (Ogbuonyalu, et al., 2025). Their proposed CACS framework (Commitment, Access, Capability, Skills) underscores that capability (technical systems) and skills development are essential attributes for enabling AI integration. Many institutions lack structured training programs, do not invest sufficiently in digital literacy, or under-provide cross-disciplinary education combining audit, data science, law, and ethics (Uzoma et al., 2024). Operationally, the skills gap results in overreliance on vendors or external consultants, slower model development or deployment, increased risk of model misuse or misinterpretation, and potential audit failures. Workforce readiness solutions include continuous professional education, joint programs with universities, certification in AI ethics and governance, internal secondments or apprenticeships mixing audit and data science skills, and strengthening audit firms' internal data science teams (Okpanachi etal., 2025). Without adequate skills and readiness, even technically superior AI systems may be under-utilized, misconfigured, or ignored in favor of traditional but less effective methods (Okpanachi etal., 2025).

Figure 5 illustrates the concept of skills gap and workforce readiness in AI-driven auditing (6.4) by depicting a futuristic office environment where a humanoid robot works alongside human professionals at computer terminals. The robot, equipped with advanced capabilities, symbolizes automation and artificial intelligence taking on complex auditing tasks, while the humans represent the existing workforce adapting to technological integration. The image highlights both the opportunities and challenges of AI adoption in auditing—such as increased efficiency and real-time analysis—but also underscores the need for reskilling, technical training, and collaboration between human auditors and AI systems. It reflects the critical issue of preparing professionals with the necessary digital literacy, analytical skills, and adaptability to remain relevant in an AI-augmented auditing landscape.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

Fig 5 Bridging the Skills Gap: Human-AI Collaboration in Auditing Neil (2024)

VII. FUTURE DIRECTIONS AND CONCLUSION

➢ *Emerging Trends in AI-Driven Forensic Auditing*

Emerging trends in AI-driven forensic auditing reflect the accelerating shift toward intelligent, adaptive, and proactive fraud detection systems in global financial institutions. One significant trend is the adoption of hybrid AI models that combine supervised, unsupervised, and reinforcement learning techniques to improve the detection of both known and novel fraud patterns. These models are particularly effective in identifying anomalies in high-frequency trading, cross-border transactions, and complex derivatives markets, where traditional rule-based systems fail. Another trend is the integration of explainable AI (XAI), designed to provide transparency into audit outcomes while enhancing trust among regulators, auditors, and clients. XAI frameworks are increasingly embedded into fraud detection pipelines to ensure compliance with ethical and regulatory demands for interpretability. Additionally, AI is being coupled with blockchain and distributed ledger technologies to create immutable, real-time audit trails that reinforce accountability and data integrity across institutions. Predictive analytics and behavioral biometrics are emerging as crucial tools for detecting insider threats and unauthorized access by modeling deviations from standard employee or customer behavior. Financial institutions are also investing in AI-driven continuous auditing systems capable of processing vast datasets in near real time, reducing audit cycles from months to minutes. Furthermore, the incorporation of natural language processing enables forensic auditors to analyze unstructured data, such as emails, contracts, and communications, revealing collusion or hidden intent behind financial misconduct.

Together, these trends signify a paradigm shift from reactive to proactive auditing, positioning AI not merely as a tool for detection but as a strategic partner in building anticipatory frameworks against financial crime. Institutions that embrace these advancements stand to enhance efficiency, strengthen compliance, and safeguard against increasingly sophisticated fraud schemes.

➢ *Policy Recommendations for Regulators and Institutions*

Policy recommendations for regulators and institutions must balance innovation with governance to ensure the effective integration of AI in forensic auditing. Regulators should prioritize the development of harmonized global frameworks that address cross-border fraud detection while minimizing legal conflicts. Standardized guidelines for data sharing, privacy, and AI model validation are essential to overcome jurisdictional disparities that hinder collaborative fraud investigations. Regulators must also establish certification processes for AI auditing systems, ensuring that deployed models meet minimum benchmarks for accuracy, fairness, and explainability. For institutions, policy should mandate the incorporation of transparency measures, such as algorithmic audits and bias impact assessments, into the deployment of AI solutions. Institutions must develop internal governance structures that include AI ethics committees and cross-functional oversight bodies to monitor system performance, safeguard against discriminatory practices, and enforce accountability when errors occur. To address data privacy and cybersecurity challenges, policies should require end-to-end encryption, anonymization protocols, and resilient data governance frameworks that align with both domestic and international regulations. Capacity building is equally critical. Regulators and institutions should collaborate with academic and professional organizations to design curricula, certifications,

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1334

and training programs tailored to AI auditing. Financial institutions should be incentivized, through regulatory relief or funding mechanisms, to invest in AI-driven compliance infrastructures that enhance efficiency without compromising ethical standards. Furthermore, the introduction of "regulatory sandboxes" can allow institutions to test innovative AI-driven auditing models under supervisory oversight, ensuring both safety and agility. By enacting these recommendations, regulators and institutions can foster an environment where AI technologies enhance transparency, compliance, and fraud resilience, while simultaneously ensuring that ethical and legal standards are rigorously upheld.

- *Pathways for Integrating Human Expertise with AI Systems*

The integration of human expertise with AI systems in forensic auditing represents a pathway toward creating robust, adaptive, and trustworthy fraud detection ecosystems. While AI excels at processing vast datasets, recognizing patterns, and flagging anomalies at scale, human auditors provide contextual judgment, ethical reasoning, and domain-specific insights that AI cannot replicate. One effective pathway is the adoption of a human-in-the-loop (HITL) approach, where AI systems generate alerts and humans evaluate their materiality, relevance, and regulatory implications. This collaboration reduces false positives and ensures that audit outcomes align with professional and legal standards. Another pathway involves leveraging AI to augment, rather than replace, auditor competencies. For example, AI can automate repetitive processes such as reconciliations or transaction monitoring, allowing auditors to focus on strategic tasks like risk assessment and investigative analysis. Knowledge transfer frameworks are also critical: institutions must design training programs where auditors gain proficiency in AI tools while AI systems are trained on domain-specific knowledge curated by experts. This bi-directional exchange ensures that models evolve alongside human expertise. Decision-support dashboards powered by AI can serve as bridges, presenting complex analytics in interpretable formats that guide auditor judgment without overwhelming them with technical details. Moreover, institutions can establish collaborative ecosystems where AI outputs are validated through peer review, ensuring multiple layers of oversight. By embedding human ethical frameworks and professional skepticism into AI decision-making pipelines, institutions can mitigate risks of over-reliance on algorithms. Ultimately, integrating human expertise with AI fosters a symbiotic model where machines amplify efficiency and accuracy, while humans safeguard fairness, accountability, and contextual integrity, ensuring AI-driven forensic auditing meets both operational and ethical standards.

- *Conclusion: Building Resilient and Fraud-Resistant Global Financial Systems*

The integration of artificial intelligence into forensic auditing offers transformative potential for building resilient and fraud-resistant global financial systems. By leveraging advanced algorithms, anomaly detection tools, and intelligent automation, institutions can shift from reactive to proactive fraud prevention, addressing risks in real time and across borders. This transition supports financial stability, reduces systemic vulnerabilities, and fosters trust among stakeholders. However, technological advancement alone cannot guarantee resilience; it must be underpinned by governance, ethical oversight, and human expertise. Resilience in this context requires embedding AI systems into comprehensive frameworks that account for compliance, transparency, and adaptability. Institutions must continuously update their fraud detection models to respond to evolving threats, while regulators should enforce harmonized standards that promote interoperability and collaboration across jurisdictions. Cross-sector partnerships between banks, technology firms, and regulators can enhance data sharing and foster collective defenses against increasingly complex fraud schemes. Equally important is the human dimension. AI can enhance efficiency, but auditors remain the guardians of professional judgment and accountability. Equipping the workforce with advanced training, interpretability tools, and interdisciplinary expertise ensures that AI augments rather than undermines the integrity of forensic auditing practices. Ethical safeguards, including bias audits and explainable decision-making, are crucial to preserving fairness and protecting individuals from harm. In conclusion, resilient and fraud-resistant global financial systems will emerge not from technology alone but from the convergence of AI innovation, human expertise, ethical governance, and global regulatory alignment. This synergy can empower institutions to navigate financial complexities with agility, maintain public trust, and safeguard the integrity of the financial ecosystem in an increasingly digital and interconnected world.

REFERENCES

[1]. 161. Atalor, S. I., Ijiga, O. M., & Enyejo, J. O. (2023). Harnessing Quantum Molecular Simulation for Accelerated Cancer Drug Screening. *International Journal of Scientific Research and Modern Technology*, *2*(1), 1–18. https://doi.org/10.38124/ijsrmt.v2i1.502

[2]. Abiodun, K., Alaka, E., Jinadu, S. O., Igba, E., & Ezeh, V. N. (2025). A Review of Federated Learning Approaches for Predictive Modeling and Confidential Data Analysis in Lending and Borrowing Behavior Across Decentralized Financial Networks. Finance & Accounting Research Journal, X (3), July 2025. https://doi.org/10.51594/farj.v7i3.

[3]. Abiodun, K., Jinadu, S. O., Alaka, E., Igba, E., & Ezeh, V. N. (2024). Risk-Sensitive Financial Dashboards with Embedded Machine Learning: A User-Centric Approach to Operational Transparency. *International Journal of Scientific Research and Modern Technology*, *3*(2), 1–18. https://doi.org/10.38124/ijsrmt.v3i2.678

[4]. Abiodun, K., Ogbuonyalu, U. O., Dzamefe, S., Vera, E. N., Oyinlola, A., & Igba, E. (2023). Exploring Cross-Border Digital Assets Flows and Central Bank Digital Currency Risks to Capital Markets Financial Stability. *International Journal of Scientific Research*

and Modern Technology, *2*(11), 32–45. https://doi.org/10.38124/ijsrmt.v2i11.447

[5]. Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. (Javaid, M., & Nobanee, H., 2023) *International Journal of Accounting Information Systems, 48*, 100598. https://doi.org/10.1016/j.accinf.2022.100598

[6]. Addy, W. A., & Sanni, M. (2024). Predictive analytics in credit risk management for banks: trends, challenges, and performance evaluations. *GSC Advanced Research and Reviews, 18*(2), 434-449.

[7]. Adelakun, B. O., Onwubuariri, E. R., Adeniran, G. A., & Ntiakoh, A. (2024). Enhancing fraud detection in accounting through AI: Techniques and case studies. *Finance & Accounting Research Journal, 6*(6), 1232. https://doi.org/10.51594/farj.v6i6.1232

[8]. Adeyelu, O. O., Ugochukwu, C. E., & Shonibare, M. A. (2024). Automating financial regulatory compliance with AI: A review and application scenarios. *Finance & Accounting Research Journal, 6*(4), 1035. https://doi.org/10.51594/farj.v6i4.1035

[9]. AI and Financial Fraud Prevention: Mapping the Trends and Challenges Through a Bibliometric Lens." (2024). *Journal of Risk and Financial Management, 18*(6), 323. https://doi.org/10.3390/jrfm18060323

[10]. AI-Driven Financial Transparency and Corporate Governance: Enhancing Accounting Practices with Evidence from Jordan. (2025). *Sustainability, 17*(9), 3818. https://doi.org/10.3390/su17093818

[11]. Alaka, E., Abiodun, K., Jinadu, S. O., Igba, E. & Ezeh, V. N. (2025). Data Integrity in Decentralized Financial Systems: A Model for Auditable, Automated Reconciliation Using Blockchain and AI, *International Journal of Management and Commerce Innovations* Vol. 13, Issue 1, pp: (136-158) DOI: https://doi.org/ 10.5281/zenodo.15753099

[12]. Alhazmi, A., Islam, S. M. N., & Prokofieva, M. (2025). The impact of artificial intelligence adoption on the quality of financial reports on the Saudi Stock Exchange. *International Journal of Financial Studies, 13*(1), 21. https://doi.org/10.3390/ijfs13010021 MDPI

[13]. Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. *Applied Sciences, 12*(19), 9637. https://doi.org/10.3390/app12199637

[14]. Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. *Applied Sciences, 12*(19), 9637. https://doi.org/10.3390/app12199637

[15]. Almaqtari, F. A. (2024). The Role of IT Governance in the Integration of AI in Accounting and Auditing Operations. *Economies, 12*(8), 199. https://doi.org/10.3390/economies12080199 MDPI

[16]. Amebleh, J., & Igba, E. (2024). Causal Uplift for Rewards Aggregators: Doubly-Robust Heterogeneous Treatment-Effect Modeling with SQL/Python Pipelines and Real-Time Inference. *International Journal of Scientific Research and Modern Technology*, *3*(5), 39–55. https://doi.org/10.38124/ijsrmt.v3i5.819

[17]. Atalor, S. I. & Enyejo, J. O. (2025). Integration of extended reality (XR) for oncology pharmacist training in chemotherapeutic compounding and risk mitigation International *Medical Science Research Journal* Volume 5, Issue 4, DOI URL: https://doi.org/10.51594/imsrj.v5i4.1931

[18]. Atalor, S. I. & Omachi, A. (2025). Transformer-Based Natural Language Processing Models for Mining Unstructured Oncology Clinical Notes to Improve Drug Matching, *International Journal of Scientific Research in Science, Engineering and Technology Volume* 12, Issue 2 doi: https://doi.org/10.32628/IJSRSET25122197

[19]. Atalor, S. I. (2019). Federated Learning Architectures for Predicting Adverse Drug Events in Oncology Without Compromising Patient Privacy *ICONIC RESEARCH AND ENGINEERING JOURNALS* JUN 2019 | IRE Journals | Volume 2 Issue 12 | ISSN: 2456-8880

[20]. Atalor, S. I. (2022). Blockchain-Enabled Pharmacovigilance Infrastructure for National Cancer Registries. *International Journal of Scientific Research and Modern Technology*, *1*(1), 50–64. https://doi.org/10.38124/ijsrmt.v1i1.493

[21]. Atalor, S. I. (2022). Data-Driven Cheminformatics Models for Predicting Bioactivity of Natural Compounds in Oncology. International Journal of Scientific Research and Modern Technology, 1(1), 65–76. https://doi.org/10.38124/ijsrmt.v1i1.496

[22]. Atalor, S. I. (2024). Building a geo-analytic public health dashboard for tracking cancer drug deserts in U.S. counties, *International Medical Science Research Journal* Volume 4, Issue 11, Fair East Publishers DOI: 10.51594/imsrj. v4i11.1932

[23]. Atalor, S. I., & Enyejo, J. O. (2025). Mobile Health Platforms for Medication Adherence among Oncology Patients in Rural Populations *International Journal of Innovative Science and Research Technology* Volume 10, Issue 5, ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25may415

[24]. Atalor, S. I., Raphael, F. O. & Enyejo, J. O. (2023). Wearable Biosensor Integration for Remote Chemotherapy Monitoring in Decentralized Cancer Care Models. *International Journal of Scientific Research in Science and Technology* Volume 10, Issue 3 (www.ijsrst.com) doi: https://doi.org/10.32628/IJSRST23113269

[25]. Ayodele, E., Oye, M. A., Alimi, B. C., & Obitolu, S. B. (2025). Investigating blockchain-based smart contracts for cross-border payment settlement, regulatory compliance and risk reduction in international finance.

[26]. Azonuche T. I, Aigbogun, M. E & Enyejo, J. O. (2025). Investigating Hybrid Agile Frameworks Integrating Scrum and Devops for Continuous Delivery in Regulated Software Environments. *International Journal of Innovative Science and Research*

Technology Volume 10, Issue 4, ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25apr1164

[27]. Azonuche, T. I., & Enyejo, J. O. (2024). Agile Transformation in Public Sector IT Projects Using Lean-Agile Change Management and Enterprise Architecture Alignment. *International Journal of Scientific Research and Modern Technology*, *3*(8), 21–39. https://doi.org/10.38124/ijsrmt.v3i8.432

[28]. Azonuche, T. I., & Enyejo, J. O. (2024). Evaluating the Impact of Agile Scaling Frameworks on Productivity and Quality in Large-Scale Fintech Software Development. *International Journal of Scientific Research and Modern Technology*, *3*(6), 57–69. https://doi.org/10.38124/ijsrmt.v3i6.449

[29]. Azonuche, T. I., & Enyejo, J. O. (2024). Exploring AI-Powered Sprint Planning Optimization Using Machine Learning for Dynamic Backlog Prioritization and Risk Mitigation. *International Journal of Scientific Research and Modern Technology*, *3*(8), 40–57. https://doi.org/10.38124/ijsrmt.v3i8.448.

[30]. Azonuche, T. I., & Enyejo, J. O. (2025). Adaptive Risk Management in Agile Projects Using Predictive Analytics and Real-Time Velocity Data Visualization Dashboard. International Journal of Innovative Science and Research Technology Volume 10, Issue 4, April – 2025 ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25apr2002

[31]. Bakumenko, A., & Tropmann-Frick, M. (2022). Detecting anomalies in financial data using machine learning: applications to general ledger auditing. *Systems*, 10(5), 130. https://doi.org/10.3390/systems10050130

[32]. Bias and ethics of AI systems applied in auditing - A systematic review. *Scientific African, 25*, e02281. (2024). https://doi.org/10.1016/j.sciaf.2024.e02281

[33]. Bolgouras, V., Zarras, A., Leka, C., Stylianou, I., Farao, A., & Xenakis, C. (2025). EU regulatory ecosystem for ethical AI. *AI and Ethics*. https://doi.org/10.1007/s43681-025-00749-x

[34]. Boulieris, P., Symeonidis, A. L., & Sergiadis, G. (2024). Fraud detection with natural language processing. *Machine Learning*, 113, 1235-1265. https://doi.org/10.1007/s10994-023-06354-5

[35]. Černevičienė, J., Budria, S., & Skaržauskienė, R. (2024). Explainable artificial intelligence (XAI) in finance. *Artificial Intelligence Review*, 57, 10854-8. https://doi.org/10.1007/s10462-024-10854-8

[36]. Cyuma, J. L.C., George, M. B., Enyejo, J. O. & Kachalla, I. (2025). Developing Smart Agroforestry Systems with Fire-Resistant Plant Species and Controlled Burning for Sustainable Land Management. *International Journal of Innovative Science and Research Technology, Volume 10 - 2025, Issue 3 - March.* https://doi.org/10.38124/ijisrt/25mar1335.

[37]. Digital payment fraud detection methods in digital ages and Industry 4.0." (2022). *Computers & Electrical Engineering, 100*, 107734. https://doi.org/10.1016/j.compeleceng.2022.107734

[38]. Dr Emily cook (2024) https://www.independent.co.uk/news/business/top-employers/hr-gen-z-wellbeing-workplace-employers-b2632788.html

[39]. Hemati, H., Schreyer, M., & Borth, D. (2021). Continual Learning for Unsupervised Anomaly Detection in Continuous Auditing of Financial Accounting Data. *arXiv*. https://arxiv.org/abs/2112.13215

[40]. Hemati, H., Schreyer, M., & Borth, D. (2021). Continual Learning for Unsupervised Anomaly Detection in Continuous Auditing of Financial Accounting Data. *arXiv*. https://doi.org/10.48550/arXiv.2112.13215

[41]. Huang, F., & Vasarhelyi, M. A. (2019). Applying robotic process automation in auditing. *Journal of Emerging Technologies in Accounting*, 16(1), 113-127. https://doi.org/10.2308/jeta-52216

[42]. Idika, C. N., James, U. U., Ijiga, O. M., Okika, N. & Enyejo, L. A, (2024). Secure Routing Algorithms Integrating Zero Trust Edge Computing for Unmanned Aerial Vehicle Networks in Disaster Response Operations *International Journal of Scientific Research and Modern Technology, (IJSRMT)* Volume 3, Issue 6, https://doi.org/10.38124/ijsrmt.v3i6.635

[43]. Idika, C. N., James, U.U, Ijiga, O. M., Enyejo, L. A. (2023). Digital Twin-Enabled Vulnerability Assessment with Zero Trust Policy Enforcement in Smart Manufacturing Cyber-Physical System *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* Volume 9, Issue 6 doi: https://doi.org/10.32628/IJSRCSEIT

[44]. Igba, E., Abiodun, K. & Ali, E. O. (2025). Building the Backbone of the Digital Economy and Financial Innovation through Strategic Investments in Data Centers. *International Journal of Innovative Science and Research Technology*, ISSN No: -2456-2165. https://doi.org/10.5281/zenodo.14651210

[45]. Igba, E., Olarinoye, H. S., Nwakaego, V. E., Sehemba, D. B., Oluhaiyero. Y. S. & Okika, N. (2025). Synthetic Data Generation Using Generative AI to Combat Identity Fraud and Enhance Global Financial Cybersecurity Frameworks. *International Journal of Scientific Research and Modern Technology (IJSRMT)* Volume 4, Issue 2, 2025. DOI: https://doi.org/10.5281/zenodo.14928919

[46]. Igba, E., Olarinoye, H. S., Ezeh, N. V., Sehemba, D. B., Oluhaiyero, Y. S., & Okika, N. (2025). Synthetic Data Generation Using Generative AI to Combat Identity Fraud and Enhance Global Financial Cybersecurity Frameworks. *International Journal of Scientific Research and Modern Technology (IJSRMT)* Volume 4, Issue 2, 2025. DOI: https://doi.org/10.5281/zenodo.14928919

[47]. Imoh, P. O. & Enyejo, J. O. (2025). Analyzing Social Communication Deficits in Autism Using Wearable Sensors and Real-Time Affective Computing Systems, *International Journal of Innovative Science and Research Technology* Volume 10, Issue 5 https://doi.org/10.38124/ijisrt/25may866

[48]. Imoh, P. O. (2023). Impact of Gut Microbiota Modulation on Autism Related Behavioral Outcomes

via Metabolomic and Microbiome-Targeted Therapies *International Journal of Scientific Research and Modern Technology (IJSRMT)* Volume 2, Issue 8, 2023 DOI: https://doi.org/10.38124/ijsrmt.v2i8.494

[49]. Imoh, P. O., & Idoko, I. P. (2022). Gene-Environment Interactions and Epigenetic Regulation in Autism Etiology through Multi-Omics Integration and Computational Biology Approaches. *International Journal of Scientific Research and Modern Technology*, *1*(8), 1–16. https://doi.org/10.38124/ijsrmt.v1i8.463

[50]. Imoh, P. O., & Idoko, I. P. (2023). Evaluating the Efficacy of Digital Therapeutics and Virtual Reality Interventions in Autism Spectrum Disorder Treatment. *International Journal of Scientific Research and Modern Technology*, *2*(8), 1–16. https://doi.org/10.38124/ijsrmt.v2i8.462

[51]. Imoh, P.O., Ajiboye,A. S., Balogun, T. K., Ijiga, A. C., Olola, T, M. & Ahmadu, E. O. (2025). Exploring the integration of psychedelic-assisted therapy and digital mental health interventions in trauma recovery for underserved adults with high-functioning autism, *Magna Scientia Advanced Research and Reviews*, 2025, DOI:https://doi.org/10.30574/msarr.2025.14.1.0079

[52]. Impact of artificial intelligence and Industry 4.0 on transforming accounting and auditing practices. (2024). *Journal of Open Innovation: Technology, Market, and Complexity, 10*(1), 100218. https://doi.org/10.1016/j.joitmc.2024.100218

[53]. Is artificial intelligence improving the audit process?" (2022). *Review of Accounting Studies, 27*, 938–985. https://doi.org/10.1007/s11142-022-09697-x

[54]. Izundu, F. C., Imoh, P. O., Enyejo, J. O. & Olola, T. M. (2025). Designing Inclusive Urban Planning Platforms Integrating Real-Time Sign Language Interpretation for Deaf Community Participation in Policymaking *International Journal of Social Science and Humanities Research* DOI: https://doi.org/10.5281/zenodo.16894453

[55]. Jagdale, R., & Deshmukh, M. (2025). Natural Language Processing in Finance: Techniques, Applications, and Future Directions. In *Machine Learning and Modeling Techniques in Financial Data Science* (pp. 411-434). IGI Global Scientific Publishing.

[56]. Javaid, H. A. (2024). Improving fraud detection and risk assessment in financial service using predictive analytics and data mining. *Integrated Journal of Science and Technology*, *1*(3).

[57]. Javaid, M., & Nobanee, H. (2023). Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *International Journal of Accounting Information Systems, 48*, 100598. https://doi.org/10.1016/j.accinf.2022.100598

[58]. Kamalaruban, P., Pi, Y., Burrell, S., Drage, E., Skalski, P., Wong, J., & Sutton, D. (2024). Evaluating fairness in transaction fraud models: Fairness metrics, bias audits, and challenges. *arXiv*, 2409.04373. https://arxiv.org/abs/2409.04373

[59]. Kokina, J., & Leung, P. (2025). Challenges and opportunities for artificial intelligence in auditing by large public accounting firms. *International Journal of Accounting Information Systems*. https://doi.org/10.1016/j.intaccinf.2025.100819

[60]. Leocádio, D., Malheiro, L., & Reis, J. (2024). *Artificial Intelligence in Auditing: A Conceptual Framework for Auditing Practices*. Administrative Sciences, 14(10), 238. https://doi.org/10.3390/admsci14100238

[61]. Louati, H., Louati, A., Kariri, E., & Almekhlafi, A. (2025). AI-Based Anomaly Detection and Optimization Framework for Blockchain Smart Contracts. *Administrative Sciences, 15*(5), 163. https://doi.org/10.3390/admsci15050163

[62]. Murikah, W., & Murgo, M. (2024). Bias and ethics of AI systems applied in auditing. *Scientific African, 25*, e02281. https://doi.org/10.1016/j.sciaf.2024.e02281

[63]. Neil Sahota (2024) https://www.neilsahota.com/ai-and-workforce-how-ai-is-changing-jobs-and-careers/

[64]. Odeyemi, O., Ibeh, C. V., Zamanjomane, N., Asuzu, O. F., & Awonuga, K. F. (2024). *Forensic accounting and fraud detection: A review of techniques in the digital age*. Finance & Accounting Research Journal, 6(2), 788. https://doi.org/10.51594/farj.v6i2.788

[65]. Ogbuonyalu, U. O, Abiodun, K., Dzamefe, S., Vera, E. N., Oyinlola, A. & Igba, E. (2025). Integrating Decentralized Finance Protocols with Systemic Risk Frameworks for Enhanced Capital Markets Stability and Regulatory Oversight. *International Journal of Innovative Science and Research Technology* Volume 10, Issue 4, ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25apr1165

[66]. Ogbuonyalu, U. O., Abiodun, K., Dzamefe, S., Vera, E. N., Oyinlola, A., & Igba. E. (2024). Assessing Artificial Intelligence Driven Algorithmic Trading Implications on Market Liquidity Risk and Financial Systemic Vulnerabilities. *International Journal of Scientific Research and Modern Technology*, *3*(4), 18–21. https://doi.org/10.38124/ijsrmt.v3i4.433

[67]. Ogbuonyalu, U. O., Abiodun, K., Dzamefe, S., Vera, E. N., Oyinlola, A. & Igba, E. (2025). Beyond the credit score: The untapped power of LLMS in banking risk models. *Finance & Accounting Research Journal*, 7(4), May 2025. https://doi.org/10.51594/farj.v7i4.1905

[68]. Okpanachi, A. T., Adeniyi, M., Igba, E. & Dzakpasu, N. H. (2025). Enhancing Blood Supply Chain Management with Blockchain Technology to Improve Diagnostic Precision and Strengthen Health Information Security. *International Journal of Innovative Science and Research Technology* Volume 10, Issue 4, ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25apr214

[69]. Okpanachi, A. T., Igba, E., Imoh, P. O., Dzakpasu, N. H. & Nyaledzigbor, M. (2025). Leveraging Digital Biomarkers and Advanced Data Analytics in Medical Laboratory to Enhance Early Detection and Diagnostic Accuracy in Cardiovascular Diseases. *International Journal of Scientific Research in Science and*

Technology Volume 12, doi : https://doi.org/10.32628/IJSRST251222590

[70]. Ononiwu, M., Azonuche, T. I., & Enyejo, J. O. (2023). Exploring Influencer Marketing Among Women Entrepreneurs using Encrypted CRM Analytics and Adaptive Progressive Web App Development. *International Journal of Scientific Research and Modern Technology*, *2*(6), 1–13. https://doi.org/10.38124/ijsrmt.v2i6.562

[71]. Ononiwu, M., Azonuche, T. I., & Enyejo, J. O. (2025). Analyzing Email Marketing Impacts on Revenue in Home Food Enterprises using Secure SMTP and Cloud Automation *International Journal of Innovative Science and Research Technology* Volume 10, Issue 6, https://doi.org/10.38124/ijisrt/25jun286

[72]. Ononiwu, M., Azonuche, T. I., & Enyejo, J. O. (2025). Assessing Kanban Implementation for Secure Workflow Optimization in Cloud DevOps Using Zero Trust Architecture Enhancements, *Magna Scientia Advanced Research and Reviews*, 2025, DOI: https://doi.org/10.30574/msarr.2025.14.1.0072

[73]. Ononiwu, M., Azonuche, T. I., & Enyejo, J. O. (2025). Investigating Agile Portfolio Management Techniques for Prioritizing Strategic Initiatives in Large-Scale Government IT Projects International *Journal of Management & Entrepreneurship Research* Fair East Publishers Volume: 7 Issue: 6 Page No: 464-483 https://doi.org/10.51594/ijmer.v7i6.1941

[74]. Ononiwu, M., Azonuche, T. I., & Enyejo, J. O. (2025). Mobile Commerce Adoption and Digital Branding Techniques for Startup Growth in Sub-Saharan African Urban Centers International *Journal of Management & Entrepreneurship Research* Fair East Publishers Volume: 7 Issue: 6 Page No: 443-463 DOI URL: https://doi.org/10.51594/ijmer.v7i6.1940

[75]. Ononiwu, M., Azonuche, T. I., Imoh, P. O. & Enyejo, J. O. (2023). Exploring SAFe Framework Adoption for Autism-Centered Remote Engineering with Secure CI/CD and Containerized Microservices Deployment *International Journal of Scientific Research in Science and Technology* Volume 10, Issue 6 doi: https://doi.org/10.32628/IJSRST

[76]. Ononiwu, M., Azonuche, T. I., Imoh, P. O. & Enyejo, J. O. (2024). Evaluating Blockchain Content Monetization Platforms for Autism-Focused Streaming with Cybersecurity and Scalable Microservice Architectures *ICONIC RESEARCH AND ENGINEERING JOURNALS* Volume 8 Issue 1

[77]. Ononiwu, M., Azonuche, T. I., Okoh, O. F., & Enyejo, J. O. (2023). AI-Driven Predictive Analytics for Customer Retention in E-Commerce Platforms using Real-Time Behavioral Tracking. *International Journal of Scientific Research and Modern Technology*, *2*(8), 17–31. https://doi.org/10.38124/ijsrmt.v2i8.561

[78]. Ononiwu, M., Azonuche, T. I., Okoh, O. F. & Enyejo, J. O. (2023). Machine Learning Approaches for Fraud Detection and Risk Assessment in Mobile Banking Applications and Fintech Solutions *International Journal of Scientific Research in Science, Engineering and Technology* Volume 10, Issue 4 doi: https://doi.org/10.32628/IJSRSET

[79]. Perdana, A., Lee, W. E., & Kim, C. M. (2023). Prototyping and implementing Robotic Process Automation in accounting firms: Benefits, challenges and opportunities to audit automation. *International journal of accounting information systems*, *51*, 100641.

[80]. Ramzan, S., & Lokanan, M. (2024). The application of machine learning to study fraud in the accounting literature. *Journal of Accounting Literature*. https://doi.org/10.1108/JAL-11-2022-0112

[81]. Review of Accounting Studies: Is artificial intelligence improving the audit process? (2022). *Review of Accounting Studies, 27*(3), 938-985. https://doi.org/10.1007/s11142-022-09697-x

[82]. Robu, V., Zhang, S., & Farkas, C. (2023). Robust AI for Financial Fraud Detection in the GCC: A Hybrid Framework for Imbalance, Drift, and Adversarial Threats. *Journal of Theoretical and Applied Electronic Commerce Research, 20*(2), 121. https://doi.org/10.3390/jtaer20020121

[83]. Robu, V., Zhang, S., & Farkas, C. (2023). Robust AI for Financial Fraud Detection in the GCC: A Hybrid Framework for Imbalance, Drift, and Adversarial Threats. *Journal of Theoretical and Applied Electronic Commerce Research, 20*(2), 121. https://doi.org/10.3390/jtaer20020121

[84]. Schreyer, M., Sattarov, T., Borth, D., Dengel, A., & Reimer, B. (2017). Detection of anomalies in large scale accounting data using deep autoencoder networks. *arXiv*. https://arxiv.org/abs/1709.05254

[85]. Temitayo Oluwaseun Jejeniwa, Noluthando Zamanjomane Mhlongo, & Titilola Olaide Jejeniwa. (2024). A comprehensive review of the impact of artificial intelligence on modern accounting practices and financial reporting. *Computer Science & IT Research Journal, 5*(4), 1031-1047. https://doi.org/10.51594/csitrj.v5i4.1086

[86]. The application of machine learning to study fraud in the accounting literature" (Ramzan & Lokanan, 2024) *Journal of Accounting Literature*. https://doi.org/10.1108/JAL-11-2022-0112

[87]. The necessity of AI audit standards boards. (2025). *AI & Society*. https://doi.org/10.1007/s00146-025-02320-y

[88]. Uzoma, E., Igba, E. & Olola, T. M. (2024). Analyzing Edge AI Deployment Challenges within Hybrid IT Systems Utilizing Containerization and Blockchain-Based Data Provenance Solutions. *International Journal of Scientific Research and Modern Technology*, *3*(12), 125–141. https://doi.org/10.38124/ijsrmt.v3i12.408

[89]. Vivek Chandan (2025) https://firmway.in/early-audit-benefits-unlock-accuracy-and-save-time/

[90]. Wassie, F. A., & others. (2024). Artificial intelligence and the future of the internal audit function. *Humanities and Social Sciences Communications, 11*, 1234. https://doi.org/10.1057/s41599-024-02905-w

[91]. Yeo, W. J., Okazaki, M., Sato, T., & He, Y. (2025). A comprehensive review on financial explainable AI. *Machine Learning*, *SpringerLink*. https://doi.org/10.1007/s10462-024-11077-7