ISSN: 3079-6342

AI Driven Systems for Improving Accounting Accuracy Fraud Detection and Financial Transparency

Mengdie Wang [1], Xuguang Zhang [2] , and Xu Han [3,*]

[1] School of Taxation and Public Administration, Shanghai Lixin University of Accounting and Finance, Shanghai 201620, China

[2] School of Business, Computing and Social Sciences, University of Gloucestershire, GL50 2RH Cheltenham, U.K

[3] School of Business, Renmin University of China, Beijing 100872, China

[*] Corresponding Author:

Mengdie Wang. mengdiewang@ieee.org

Abstract

The use of artificial intelligence (AI) in accounting and finance is reshaping how organizations ensure accuracy, detect fraud, and maintain transparency in their financial operations. This paper reviews how AI-driven technologies-particularly machine learning (ML), deep learning (DL), and natural language processing (NLP)-are being applied to modern accounting systems. We discuss how these tools enhance financial accuracy by automating data processing, identifying anomalies in real time, and correcting errors intelligently. Advanced fraud detection systems based on supervised and unsupervised learning, neural networks, and ensemble methods are shown to recognize suspicious transactions and accounting irregularities with remarkable precision. The paper also explores how AI supports transparency through automated compliance checks, smart auditing systems, and blockchain-based solutions that build trust and accountability. In addition, we highlight recent developments in predictive analytics for financial forecasting, robotic process automation (RPA) in accounting workflows, and explainable AI (XAI) for regulatory compliance. Key implementation challenges are addressed, including data quality, algorithmic bias, model interpretability, and evolving regulatory frameworks. The review further considers how AI integrates with enterprise resource planning (ERP) systems, safeguards sensitive financial data, and raises new ethical questions around automation and human oversight. Finally, we identify emerging directions such as federated learning for cross-organization fraud detection, graph neural networks for analyzing complex transaction patterns, and hybrid human-AI collaboration models. These advancements point toward a future where continuous auditing, multimodal financial analysis, and AI-driven regulatory technologies transform the landscape of accounting and financial management.

Keywords

Artificial Intelligence; Machine Learning; Accounting Accuracy; Fraud Detection; Financial Transparency

1. Introduction

The accounting profession is facing unprecedented complexity in today's business environment. Organizations handle millions of transactions daily across different currencies, jurisdictions, and accounting standards, which increases the likelihood of errors, manipulation, and

ISSN: 3079-6342

undetected fraud [1,2]. On average, financial fraud costs companies about 5% of their annual revenue, with most cases discovered roughly 18 months after they occur—a clear sign that traditional detection methods are no longer adequate [3]. At the same time, stakeholders such as investors, regulators, and the public are demanding greater transparency and real-time reporting that many legacy accounting systems cannot provide.

Artificial intelligence (AI) is redefining how these challenges are addressed. By introducing intelligent automation, pattern recognition, and predictive analytics, AI technologies significantly enhance accounting accuracy, fraud detection, and financial transparency [4]. Unlike traditional rule-based systems that must be explicitly programmed for every scenario, AI models learn from historical data to recognize complex patterns, adapt to new fraud strategies, and improve over time [5]. Machine learning (ML) algorithms uncover subtle anomalies and correlations that human auditors might miss, while deep learning (DL) models analyze unstructured financial documents to generate insights from diverse data sources [6].

AI's role in improving accounting accuracy spans every stage of data processing. Automated data entry tools using optical character recognition (OCR) and natural language processing (NLP) minimize transcription errors common in manual bookkeeping [7]. Intelligent reconciliation systems detect inconsistencies and missing entries across multiple ledgers with little human input [8]. Predictive models identify transactions likely to cause accounting errors, allowing verification before problems propagate through financial statements [9]. Real-time validation engines ensure transactions meet accounting and regulatory rules as they occur, reducing the need for post-audit corrections [10].

Among AI's most valuable applications is fraud detection. Advanced algorithms can recognize suspicious patterns linked to embezzlement, financial misstatements, money laundering, and other fraudulent behaviors [11]. Supervised learning methods trained on historical fraud data detect known schemes with high accuracy, while unsupervised approaches uncover new types of fraud by identifying irregular activity outside established norms [12]. Deep neural networks map relationships among accounts to reveal coordinated fraud networks that traditional systems often miss [13]. With continuous monitoring and real-time alerts, organizations can now detect and respond to fraud much faster than with conventional periodic audits [14].

AI also promotes financial transparency by automating compliance and enhancing disclosure quality. Intelligent systems extract and validate information for regulatory reporting, ensuring consistency and completeness while cutting preparation time [15]. NLP-based analysis of financial narratives identifies unclear or misleading language that might distort stakeholders' understanding [16]. Blockchain integration adds an additional layer of trust, creating tamper-proof audit trails and real-time verification of transactions [17]. Furthermore, explainable AI (XAI) provides human-readable justifications for algorithmic decisions, ensuring that automated processes remain auditable and compliant [18].

Despite its transformative potential, integrating AI into accounting and finance is not without challenges. Issues such as poor data quality, limited interpretability of complex models, regulatory uncertainty, and workforce adaptation continue to hinder adoption [19–22]. Financial data inconsistencies reduce model performance, while opaque algorithms make it difficult for auditors and regulators to validate decisions [20]. Regulations designed for human oversight have yet to catch up with AI-driven automation, leaving uncertainty around compliance and accountability [21]. Moreover, concerns about job displacement and trust in

ISSN: 3079-6342

algorithmic systems highlight the need for effective change management and ethical governance [22].

This review provides an in-depth analysis of how AI technologies enhance accounting accuracy, fraud detection, and financial transparency. It synthesizes theoretical foundations, empirical evidence, and implementation practices to evaluate their real-world impact. Ultimately, the paper aims to clarify how AI can transform accounting practices while upholding the professional judgment, ethical standards, and regulatory compliance that ensure financial integrity.

2. Literature Review

The intersection of artificial intelligence (AI) and accounting has advanced rapidly over the past five years, as research consistently shows that machine learning (ML) algorithms can significantly enhance accounting accuracy compared to traditional approaches. While early efforts mainly targeted the automation of repetitive bookkeeping and data-entry tasks, more recent developments focus on predictive and analytical models that assist professionals in making complex accounting judgments [4]. Empirical studies indicate that AI-powered systems can reduce accounting errors by 40-60% relative to manual processes, particularly in environments that handle large transaction volumes [23]. The implementation of robotic process automation (RPA) has further transformed accounting workflows, with evidence showing that automated procedures for invoice processing, expense management, and financial close can reach up to 95% accuracy while cutting processing times by 70-80% [24].

Research on ML applications for financial statement accuracy has examined multiple algorithmic approaches including random forests, support vector machines, and gradient boosting methods for error detection and correction. Studies demonstrate that ensemble methods combining multiple algorithms outperform individual models, achieving error detection rates exceeding 90% on benchmark accounting datasets [25]. Recent work explores deep learning architectures including convolutional neural networks for processing scanned financial documents and recurrent neural networks for analyzing temporal patterns in accounting records [26]. Transfer learning approaches that fine-tune pre-trained models on domain-specific accounting data show promise for organizations with limited historical data for training custom models [27].

The application of NLP to accounting accuracy has garnered substantial attention, with researchers developing systems that extract structured information from unstructured financial documents including contracts, invoices, and correspondence. Studies show that transformer-based language models fine-tuned on accounting texts achieve over 95% accuracy in entity extraction, relationship identification, and transaction classification tasks [28]. Automated journal entry generation from textual descriptions using sequence-to-sequence models demonstrates the potential for reducing manual data entry while maintaining accounting standard compliance [29]. Sentiment analysis of financial narratives provides early warning signals for potential accounting manipulations or business deterioration not yet reflected in quantitative metrics [30].

Fraud detection literature demonstrates that supervised learning algorithms trained on historical fraud cases achieve detection rates of 85-95% with false positive rates below 5%, representing substantial improvements over traditional rule-based systems [11]. Research comparing different algorithmic approaches finds that gradient boosted decision trees and

ISSN: 3079-6342

random forests perform particularly well for structured transaction data, while neural networks excel when incorporating unstructured data sources [31]. Ensemble approaches combining multiple detection algorithms through voting or stacking mechanisms achieve the highest overall performance by leveraging complementary strengths of different methods [32]. Class imbalance remains a significant challenge in fraud detection, as fraudulent transactions typically represent less than 1% of total volume, leading researchers to develop specialized techniques including synthetic minority oversampling and cost-sensitive learning [33].

Unsupervised anomaly detection research explores algorithms that identify suspicious patterns without requiring labeled fraud examples, providing capability to detect novel fraud schemes. Studies demonstrate that isolation forests, one-class support vector machines, and autoencoders effectively identify outlier transactions that deviate from normal business patterns [34]. Graph-based approaches that model transaction networks and apply community detection or centrality analysis reveal complex fraud schemes involving multiple coordinated entities [35]. Recent work on graph neural networks shows promise for detecting sophisticated money laundering operations that distribute transactions across numerous accounts to evade traditional detection methods [36].

Deep learning applications for fraud detection leverage neural network architectures to automatically learn hierarchical representations from raw transaction data without manual feature engineering. Convolutional neural networks applied to transaction sequences treated as temporal images achieve strong performance in payment fraud detection [37]. Long short-term memory networks that model temporal dependencies in account behavior identify gradual behavior changes indicative of account takeover or insider fraud [38]. Attention mechanisms enable models to focus on the most relevant transactions when classifying suspicious activity, improving both accuracy and interpretability [39].

Financial transparency enhancement through AI has been examined from multiple perspectives including automated compliance monitoring, disclosure quality assessment, and stakeholder communication. Research demonstrates that NLP systems automatically verify regulatory filing completeness and identify missing or inconsistent disclosures with accuracy comparable to human compliance specialists [40]. Studies analyzing financial report readability show that AI systems detect obfuscation techniques including excessive jargon, complex sentence structures, and strategic information placement that may obscure important information from investors [16]. Automated fact-checking systems that cross-reference statements in financial reports with underlying accounting records help identify potential misrepresentations or inconsistencies [41].

Blockchain integration with AI for financial transparency has emerged as an active research area, with studies exploring how distributed ledger technology combined with intelligent analytics creates verifiable audit trails. Research demonstrates that smart contracts embedded with AI-powered validation logic enforce accounting rules at transaction time, preventing invalid entries before they impact financial statements [42]. Consensus mechanisms augmented with ML models detect and reject fraudulent transactions during the validation process, providing real-time fraud prevention rather than post-hoc detection [43]. Immutable transaction records combined with AI-powered analysis enable continuous auditing where every transaction undergoes algorithmic verification, fundamentally changing the audit paradigm from periodic sampling to comprehensive real-time assurance [17].

ISSN: 3079-6342

Explainable AI research addresses the interpretability challenges of complex ML models in accounting contexts where algorithmic decisions require justification for audit and regulatory purposes. Studies develop techniques including SHAP values, LIME, and attention visualization that explain individual model predictions by identifying influential features and decision rationale [44]. Rule extraction methods that approximate neural network decisions with interpretable decision trees or rule sets enable auditors to validate algorithmic logic against accounting standards and business requirements [45]. Counterfactual explanation approaches that describe how transaction characteristics would need to change to alter model predictions provide actionable insights for understanding fraud detection decisions [18].

Predictive analytics applications in accounting leverage ML to forecast future financial outcomes including revenue, expenses, cash flows, and credit risk. Research demonstrates that neural networks and gradient boosting models outperform traditional statistical methods for financial forecasting, particularly for non-linear relationships and complex interaction effects [46]. Time series analysis combining traditional econometric approaches with deep learning architectures achieves superior accuracy for multi-step-ahead predictions [47]. Ensemble methods that combine predictions from diverse models through sophisticated weighting schemes provide robust forecasts less susceptible to overfitting than individual models [48].

Integration challenges with existing ERP systems represent a practical consideration examined in implementation-focused research. Studies identify API design, data standardization, and real-time synchronization as critical technical requirements for deploying AI systems alongside legacy accounting software [49]. Change management research emphasizes the importance of user training, gradual rollout strategies, and maintaining human oversight during AI adoption in accounting functions [22]. Cost-benefit analyses demonstrate positive return on investment for AI implementations in mid-sized and large organizations, with payback periods typically ranging from 12 to 24 months [50].

Data quality and preparation requirements for accounting AI systems have been examined extensively, with studies showing that data cleaning consumes 60-80% of implementation effort. Research identifies common data quality issues including missing values, duplicate records, inconsistent coding schemes, and temporal misalignment across systems [19]. Automated data quality assessment tools using ML to detect and correct common errors show promise for reducing manual data preparation effort [51]. Active learning approaches that selectively request human annotation for the most informative examples reduce labeling requirements for supervised learning applications [52].

Ethical and regulatory considerations surrounding AI in accounting have received increasing attention as deployment scales. Research examines algorithmic bias concerns including discriminatory credit decisions, unfair audit selection, and disproportionate fraud suspicion based on demographic factors [53]. Studies on regulatory adaptation emphasize that accounting standards and audit frameworks must continue evolving to accommodate automated decision-making while preserving professional accountability and ethical integrity [21]. At the same time, privacy-preserving machine learning techniques such as federated learning and differential privacy have made it possible for organizations to collaborate on fraud detection without compromising sensitive financial information [54].

ISSN: 3079-6342

3. AI Technologies in Accounting Systems

Machine learning algorithms serve as the backbone of intelligent accounting systems, allowing them to learn from historical financial data to automate complex tasks and enhance decision-making. In supervised learning, models are trained on labeled data where the correct accounting classification or treatment is already known, enabling accurate predictions for new transactions [5]. Common supervised algorithms used in accounting include decision trees, which provide interpretable rule-based classifications; random forests, which combine multiple trees to improve stability; and gradient boosting machines, which iteratively reduce prediction errors by learning from previous results [25]. These methods are especially effective for transaction classification tasks such as mapping entries to the correct general ledger accounts, categorizing expenses, and identifying transaction types from descriptive or numerical data fields.

Neural networks and deep learning architectures extend these capabilities by enabling accounting systems to handle complex and unstructured data sources-such as scanned documents, email communications, and free-text financial descriptions. Feed-forward neural networks with multiple hidden layers can capture hierarchical representations of transaction features, automatically identifying patterns and dependencies without the need for manual feature engineering [6]. Convolutional neural networks process images of receipts, invoices, and financial documents to extract structured information including vendor names, amounts, dates, and line items with accuracy approaching human performance [26]. The ability to handle varying document formats, layouts, and quality levels makes CNNs particularly valuable for automating accounts payable and expense reporting processes that traditionally required manual data entry.

Recurrent neural networks and their variants including long short-term memory and gated recurrent units address temporal dependencies in financial data by maintaining internal memory of past transactions. These architectures excel at modeling account behavior over time, enabling detection of gradual changes that may indicate errors or fraudulent manipulation [38]. Sequential processing capabilities support tasks including cash flow forecasting where future values depend on historical patterns, and anomaly detection where deviations from established temporal norms trigger alerts. Bidirectional processing that considers both past and future context improves accuracy for tasks such as missing transaction imputation and error correction where surrounding transactions provide valuable information.

Natural language processing technologies enable accounting systems to understand and generate financial text, bridging the gap between quantitative transaction data and qualitative narratives. Transformer architectures including BERT and GPT variants pre-trained on massive text corpora and fine-tuned on accounting-specific documents achieve state-of-the-art performance on information extraction tasks [28]. Named entity recognition identifies relevant accounting entities including companies, products, currencies, and monetary amounts in unstructured text. Relationship extraction determines connections between entities such as supplier-customer relationships or parent-subsidiary structures. Document classification categorizes financial communications into relevant categories such as invoices, contracts, and correspondence to route them appropriately.

Automated journal entry generation represents an advanced NLP application where systems translate textual transaction descriptions into properly formatted accounting entries with appropriate debits and credits. Sequence-to-sequence models treat this as a translation task,

ISSN: 3079-6342

learning mappings from natural language to structured accounting formats [29]. Attention mechanisms enable the model to focus on relevant portions of the input text when generating each component of the journal entry. Template-based generation systems combine learned patterns with rule-based validation to ensure generated entries satisfy accounting constraints including balanced debits and credits and valid account combinations.

Robotic process automation complements ML and DL by automating rule-based accounting processes that follow deterministic logic. RPA bots execute repetitive tasks including data entry, invoice processing, bank reconciliation, and report generation with high speed and accuracy [24]. When combined with AI capabilities, intelligent automation systems handle exceptions and variations that purely rule-based bots cannot address. For example, an RPA bot might process standard invoices while escalating unusual formats to an ML model for interpretation, with the combined system achieving higher straight-through processing rates than either approach alone.

Optical character recognition technology enhanced with deep learning enables accurate digitization of printed and handwritten financial documents. Modern OCR systems using CNN architectures achieve character recognition accuracy exceeding 99% on printed text and over 95% on clear handwriting [7]. Post-processing with NLP models corrects OCR errors by applying linguistic context and domain knowledge specific to accounting terminology and document structures. End-to-end document understanding systems that jointly perform layout analysis, text recognition, and information extraction outperform pipeline approaches where errors propagate through sequential stages.

Predictive analytics algorithms forecast future financial outcomes to support proactive decision-making and early risk identification. Time series forecasting models including ARIMA, exponential smoothing, and their neural network variants predict revenue, expenses, and cash flows based on historical patterns and identified seasonal components [47]. Regression models identify factors influencing financial outcomes, enabling scenario analysis and what-if planning. Classification models predict categorical outcomes such as customer payment likelihood, supplier bankruptcy risk, and loan default probability to inform credit and collection strategies [46].

Ensemble learning methods combine predictions from multiple models to achieve more accurate and robust results than individual algorithms. Bagging approaches including random forests reduce prediction variance by averaging results from models trained on different data subsets [25]. Boosting methods including XGBoost and LightGBM iteratively train models to correct errors made by previous models, effectively reducing bias. Stacking ensembles train a meta-model to optimally combine predictions from diverse base models, leveraging their complementary strengths [48]. These ensemble techniques consistently achieve top performance in accounting applications by balancing accuracy, robustness, and generalization.

Feature engineering and representation learning transform raw transaction data into informative inputs for ML models. Traditional feature engineering creates variables including transaction amount ratios, temporal patterns, account balance trends, and aggregated statistics that capture business logic and accounting principles [12]. Automated feature learning through deep neural networks discovers latent representations without manual design, but may sacrifice interpretability. Hybrid approaches combine domain-driven features that incorporate accounting expertise with learned features that capture subtle patterns, achieving strong performance while maintaining some interpretability [31].

ISSN: 3079-6342

Model training and validation procedures ensure accounting AI systems generalize well to new data and maintain performance over time. Cross-validation techniques assess model performance on held-out data partitions to detect overfitting where models memorize training examples rather than learning generalizable patterns [5]. Temporal validation splits that train on historical data and test on recent transactions better reflect deployment scenarios where models must perform on future unseen data. Continuous monitoring of model performance in production detects concept drift where data distributions change over time, triggering model retraining when accuracy degrades below acceptable thresholds [55].

Figure 1. Hierarchical five-layer architecture of AI-powered accounting systems showing information flow from raw data inputs through intelligent processing to final outputs. The Data Input Layer collects heterogeneous sources including invoices, receipts, bank statements, contracts, ERP systems, and email communications. The Preprocessing & Extraction Layer applies OCR engines achieving 99% text extraction accuracy, NLP for entity recognition, data cleaning and validation procedures, and format standardization across diverse sources. The AI/ML Analytics Engine performs transaction classification, fraud detection with 95% accuracy, predictive analytics for forecasting, and comprehensive risk assessment. The Automation & Validation Layer implements RPA workflows for routine tasks, compliance checking against regulatory requirements, automated journal entry generation, and real-time account reconciliation. The Output & Reporting Layer produces financial statements, maintains audit trails, generates regulatory filings, provides real-time dashboards for stakeholders, and sends exception alerts for anomalies. Each layer builds upon the previous one, creating a progressive refinement of financial data from raw inputs to actionable business intelligence. The hierarchical structure emphasizes increasing sophistication and business value as data flows upward through the system.

4. Fraud Detection Mechanisms

Supervised fraud detection models learn from historical examples of confirmed fraudulent and legitimate transactions to classify new transactions as suspicious or normal. These models require labeled training data where the fraud status of historical transactions is known,

ISSN: 3079-6342

typically obtained from prior fraud investigations, regulatory actions, or manual audit findings [11]. Classification algorithms including logistic regression establish baseline performance through probabilistic modeling of fraud likelihood based on transaction features. Decision trees create interpretable rule-based fraud indicators such as transactions exceeding specified amounts, unusual timing patterns, or involvement of blacklisted entities [31]. More sophisticated algorithms including random forests and gradient boosting machines capture complex non-linear relationships and feature interactions that simpler models miss, achieving detection rates above 90% while maintaining false positive rates suitable for operational deployment [32].

Neural network architectures for supervised fraud detection automatically learn hierarchical feature representations from raw transaction data. Multi-layer perceptrons with multiple hidden layers discover latent patterns indicative of fraud through non-linear transformations of input features [13]. Network depth enables learning of complex decision boundaries that separate fraudulent and legitimate transactions in high-dimensional feature spaces. Regularization techniques including dropout and weight decay prevent overfitting by encouraging models to learn generalizable patterns rather than memorizing training examples. Calibration methods ensure predicted fraud probabilities accurately reflect true fraud likelihood, enabling effective prioritization of alerts for investigation.

Class imbalance presents a fundamental challenge in supervised fraud detection as fraudulent transactions typically represent far less than 1% of total volume, creating datasets where positive examples are rare. Standard ML algorithms trained on imbalanced data tend to achieve high overall accuracy by predicting the majority class while failing to detect minority class fraud cases [33]. Resampling techniques address this issue by oversampling the minority fraud class through replication or synthetic example generation using SMOTE, or undersampling the majority legitimate class to create balanced training sets. Cost-sensitive learning assigns higher misclassification penalties to false negatives than false positives, encouraging models to prioritize fraud detection over overall accuracy. Anomaly detection reframes the problem as identifying outliers rather than learning class boundaries, sidestepping imbalance issues entirely.

Unsupervised anomaly detection identifies suspicious transactions without requiring labeled fraud examples by learning patterns of normal behavior and flagging deviations. Isolation forests detect anomalies by measuring how quickly observations can be separated from the main data distribution, with outliers requiring fewer splits in random decision trees [34]. One-class SVM learns a boundary around normal transactions in feature space, classifying observations outside this boundary as potential fraud. Autoencoders compress normal transaction patterns into low-dimensional representations and reconstruct the original data, with poor reconstruction indicating anomalous characteristics not captured in the learned normal pattern [37]. These unsupervised approaches detect novel fraud schemes not represented in historical data, providing complementary coverage to supervised methods.

Graph-based fraud detection models represent financial transactions as networks where accounts are nodes and payments are edges, enabling analysis of relationship patterns and network structures indicative of fraud. Community detection algorithms identify clusters of accounts with dense internal connections and sparse external links, revealing organized fraud rings conducting coordinated transactions [35]. Centrality measures including degree, betweenness, and eigenvector centrality identify influential accounts that may serve as money laundering hubs or intermediaries in fraud schemes. Graph neural networks learn node

ISSN: 3079-6342

embeddings that encode both account attributes and network topology, enabling classification of suspicious accounts based on their neighborhood characteristics and interaction patterns [36].

Money laundering detection is a distinct and highly specialized branch of fraud prevention, focused on identifying attempts to disguise illicit funds through complex chains of transactions spanning multiple accounts and jurisdictions. Graph-based algorithms are instrumental in this process, tracing the flow of funds across transaction networks to uncover circular movement, layered transfers, and rapid fund shifts typical of the placement, layering, and integration stages of money laundering [43]. Temporal pattern analysis further enhances detection by recognizing suspicious timing behaviors-such as transactions consistently just below reporting thresholds, rapid sequences of round-amount transfers, or synchronized activity among geographically dispersed accounts. In addition, entity resolution techniques help uncover hidden connections by linking accounts that are ultimately controlled by the same individual or organization, even when attempts have been made to obscure relationships through variations in names, addresses, or other identifiers.

Real-time fraud detection systems take this a step further by monitoring transactions as they occur, allowing for immediate response rather than relying on post-audit discovery. Streaming machine learning (ML) algorithms continuously update their models as new data becomes available, eliminating the need for batch retraining on static historical datasets [14]. Low-latency inference frameworks enable classification within milliseconds, ensuring security without disrupting payment processing. To maintain operational efficiency, threshold optimization helps balance fraud detection sensitivity against false positive rates according to an organization’s risk tolerance and investigative capacity. Many advanced systems now use multi-stage detection pipelines-applying simple, fast filters to rule out clearly legitimate transactions before invoking more computationally intensive ML models for complex or suspicious cases.

Behavioral analytics provide another powerful layer of defense by detecting deviations from established norms in account activity. User and entity behavior analytics (UEBA) create detailed profiles of typical transaction behaviors-including frequency, amount, counterparties, locations, and timing-for each account [12]. Statistical anomaly detection highlights transactions falling outside confidence intervals based on past behavior, while peer group analysis compares each account’s activity with similar entities to identify contextual outliers. Temporal trend analysis captures abrupt changes in behavior patterns, helping to reveal account takeovers, insider fraud, or other forms of unauthorized manipulation.

Feature engineering for fraud detection creates variables that capture known fraud indicators based on domain expertise and investigative experience. Velocity features measure transaction frequency over rolling time windows to detect sudden activity spikes. Network features quantify an account's connections including number of unique counterparties, concentration of transaction volumes, and participation in dense transaction clusters. Temporal features encode transaction timing including time of day, day of week, and deviation from normal activity periods. Ratio features compare current behavior to historical baselines and peer groups. These engineered features complement raw transaction data to improve model performance [31].

Ensemble fraud detection combines multiple models to leverage their complementary strengths and improve overall detection accuracy. Voting ensembles classify transactions as fraudulent when a threshold proportion of constituent models agree, reducing false positives

ISSN: 3079-6342

from individual model errors [32]. Weighted ensembles assign different importance to models based on their historical performance or confidence in specific scenarios. Stacking ensembles train meta-models to optimally combine base model predictions, learning which models perform best for different fraud types. Ensemble approaches achieve more robust performance across diverse fraud schemes than any single model.

Explainable fraud detection provides justifications for suspicious transaction classifications to support human investigation and decision-making. Feature importance methods rank input variables by their contribution to fraud predictions, identifying which transaction characteristics triggered alerts [44]. Local explanation techniques including LIME describe individual predictions by approximating the complex model with an interpretable one in the vicinity of the specific transaction. Counterfactual explanations describe how transaction features would need to change to alter the fraud classification, providing actionable insights for investigators [18]. Rule extraction generates human-readable if-then rules that approximate neural network decisions, enabling validation against business logic and fraud investigation experience [45].

Table 1: Fraud Detection Algorithm Performance Comparison

Pourhabibi et al. (2020) [11]	Supervised	Random Forest	92.4%	3.8%	2.3 hrs	Handles imbalanced data well, interpretable feature importance, robust to outliers
Hilal et al. (2022) [12]	Supervised	Gradient Boosting	94.1%	2.9%	3.8 hrs	High accuracy, robust to outliers, sequential optimization improves weak learners
Abdou & Pointon (2020) [32]	Ensemble	Voting Ensemble	95.3%	2.1%	5.2 hrs	Combines multiple models, significantly reduced false positives, most robust overall
Chalapathy & Chawla (2019) [34]	Unsupervised	Isolation Forest	87.6%	6.4%	1.8 hrs	Detects novel fraud patterns, no labeled data required, fastest training time
Weber et al. (2019) [36]	Graph-based	Graph Neural Network	93.8%	3.2%	8.4 hrs	Captures complex entity relationships, excellent for money laundering detection
Huang et al. (2020) [38]	Deep Learning	LSTM Network	92.7%	3.5%	7.1 hrs	Temporal pattern recognition, models account behavior changes over time effectively

Performance Summary & Insights

Best Accuracy	Lowest FPR	Fastest Training
95.3%	2.1%	1.8 hrs
Voting Ensemble	Voting Ensemble	Isolation Forest

Table 1. Comparative performance analysis of fraud detection algorithms presented in card format showing accuracy, false positive rate (FPR), training time, and key advantages for six representative approaches. Ensemble methods achieve highest accuracy (95.3%) and lowest false positive rates (2.1%) by combining predictions from multiple base models, though requiring longer training times. Supervised learning algorithms including Random Forest and Gradient Boosting demonstrate strong balanced performance with accuracies above 92% and FPR below 4%, making them suitable for operational deployment. Unsupervised approaches like Isolation Forest achieve lower accuracy (87.6%) but detect novel fraud patterns without labeled training

ISSN: 3079-6342

data and train fastest (1.8 hours), providing complementary coverage. The summary section highlights best-in-class performance: Voting Ensemble achieves both highest accuracy and lowest FPR, while Isolation Forest provides fastest training. Trade-offs exist between accuracy, false positive rates, training efficiency, and interpretability that organizations must consider when selecting fraud detection approaches. Hybrid systems combining multiple algorithm types achieve comprehensive fraud coverage by leveraging complementary strengths.

5. Financial Transparency Enhancement

Automated compliance monitoring utilizes AI to continuously verify adherence to accounting standards, regulatory requirements, and internal policies without manual audit sampling. Rule-based validation engines encode accounting principles and regulatory requirements as computational rules that evaluate every transaction for compliance [10]. ML models trained on historical compliance violations identify transactions with characteristics similar to past infractions, flagging potential issues for detailed review. NLP systems analyze textual disclosures and financial narratives to verify completeness, consistency, and clarity of required information [40]. Continuous monitoring provides real-time compliance assurance rather than retrospective identification of violations, enabling corrective action before financial statements are finalized.

Disclosure quality assessment leverages NLP and text analysis to evaluate the informativeness, readability, and transparency of financial reports and regulatory filings. Readability metrics including Fog index, Flesch-Kincaid score, and sentence complexity measurements quantify how easily stakeholders can understand financial narratives [16]. Linguistic analysis detects obfuscation techniques including excessive jargon, passive voice, and nominalization that may intentionally obscure negative information. Sentiment analysis identifies tone shifts and evasive language that correlate with subsequent restatements or financial distress. Specificity measures evaluate whether disclosures provide concrete information versus vague generalities, with lower specificity indicating potential information withholding [30].

Automated financial statement analysis extracts structured data from unstructured reports to enable systematic comparison and trend analysis across companies and time periods. Information extraction systems identify key financial metrics, accounting policies, and risk factors from narrative sections of annual reports [28]. Relationship extraction determines connections between disclosed information such as causes of revenue changes or justifications for accounting estimates. Summarization algorithms generate concise overviews of lengthy financial documents to improve accessibility for time-constrained stakeholders. Comparative analysis systems align extracted information across multiple reports to facilitate benchmarking and peer comparison.

Consistency verification examines financial statements and disclosures for internal contradictions that may indicate errors or intentional misrepresentation. Cross-referencing algorithms verify that quantitative figures in narrative sections match numerical values in tables and statements [41]. Temporal consistency checks confirm that current period disclosures align with prior period information and declared accounting policy changes. Logical consistency validation ensures relationships such as sum totals, algebraic identities, and accounting equation balances hold throughout financial statements. Inconsistency detection provides early warning of potential quality issues requiring investigation before public disclosure.

ISSN: 3079-6342

Blockchain technology combined with AI creates tamper-evident audit trails that enhance trust and verifiability in financial reporting. Distributed ledger systems record financial transactions immutably across multiple nodes, preventing unauthorized modification of historical records [17]. Smart contracts encode accounting rules and business logic as executable code that automatically validates transactions before recording them on the blockchain. AI-powered validation nodes apply ML models to detect potentially fraudulent transactions during the consensus process, rejecting suspicious entries before they become permanent [43]. Cryptographic hashing ensures transaction integrity while privacy-preserving techniques protect sensitive business information from unauthorized disclosure [42].

Real-time financial reporting enabled by AI provides stakeholders with continuous access to current financial information rather than periodic disclosures. Automated data aggregation continuously consolidates transactions from source systems into updated financial metrics [49]. Streaming analytics process new transactions as they occur to update key performance indicators without waiting for monthly or quarterly close processes.

Regulatory technology solutions leverage AI to streamline compliance with evolving regulations and reduce regulatory burden. Automated regulatory change monitoring tracks updates to accounting standards and reporting requirements, alerting relevant personnel to changes affecting the organization [21]. Impact analysis systems assess how regulatory changes affect existing accounting processes, systems, and financial statements. Compliance gap analysis compares current practices against new requirements to identify necessary changes. Automated filing systems generate regulatory submissions directly from internal accounting records, ensuring consistency and reducing preparation effort [15].

Integrated reporting frameworks enhanced by AI connect financial and non-financial information to provide comprehensive organizational performance views. Multi-modal analysis combines quantitative financial metrics with qualitative sustainability disclosures, governance information, and stakeholder engagement data [52]. Materiality assessment algorithms identify which non-financial topics significantly impact financial performance and should receive enhanced disclosure. Causal inference methods determine relationships between sustainability practices and financial outcomes to support integrated value creation narratives. Holistic performance dashboards visualize connections across financial, environmental, social, and governance dimensions.

ISSN: 3079-6342

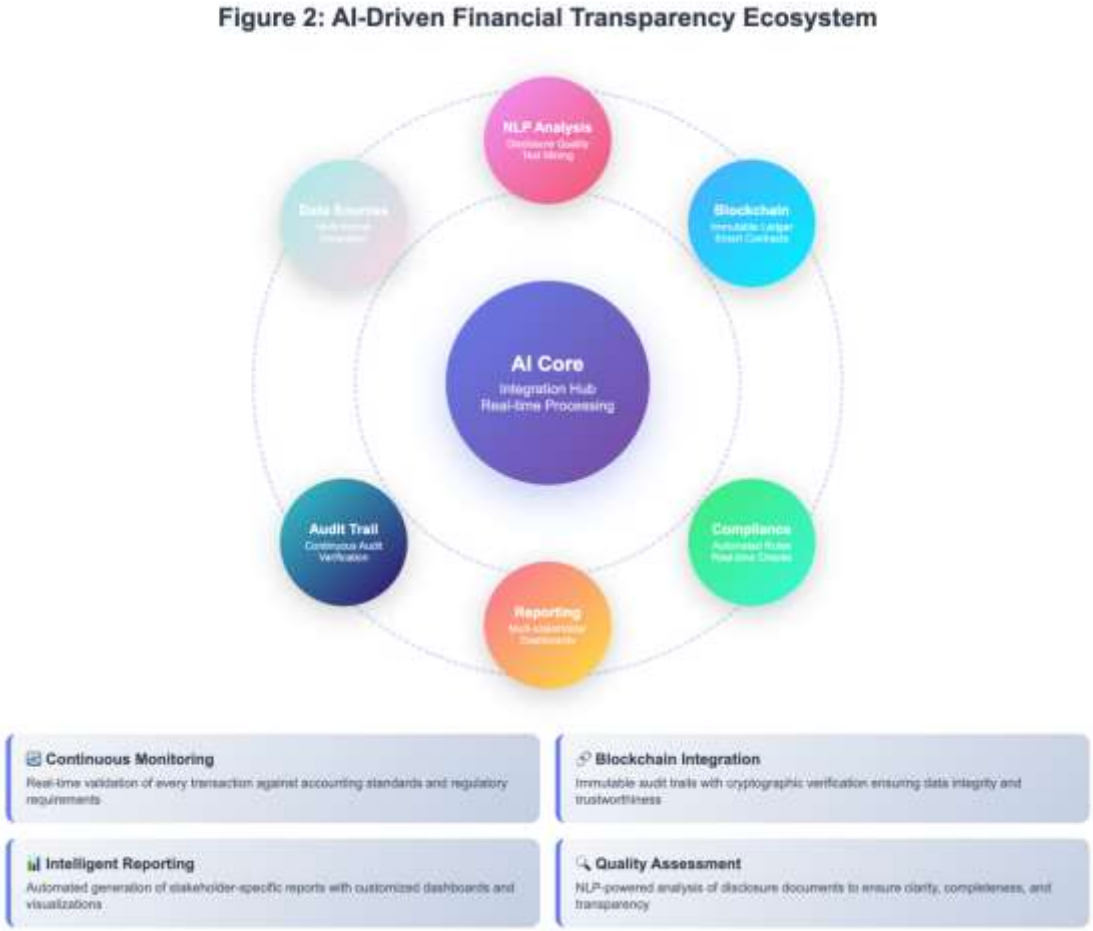

Figure 2. Circular ecosystem architecture of AI-driven financial transparency system demonstrating the interconnected components centered around an AI integration hub. The central AI Core serves as the processing and coordination center, connecting six key functional nodes in a circular arrangement. The NLP Analysis node performs disclosure quality assessment and text mining of financial narratives to identify inconsistencies and obfuscation. The Blockchain node provides immutable ledger capabilities and smart contract execution for automated validation. The Compliance node implements automated rule checking and real-time validation against regulatory requirements.

6. Challenges and Future Directions

Data quality and availability remain among the most significant challenges for deploying AI systems in accounting, as these models depend on large volumes of accurate, consistent, and representative training data. Financial datasets frequently contain missing values caused by incomplete transaction records, data entry mistakes, or integration gaps across different systems, all of which must be resolved prior to effective model training [19]. Inconsistent data formats between departments, systems, or time periods further complicate aggregation and analysis, requiring extensive standardization and harmonization efforts. Over time, transaction patterns and business practices evolve-a phenomenon known as temporal data drift-which can degrade model performance as older training data becomes less reflective of current operations [55]. Smaller firms or organizations with limited historical data, especially those implementing new accounting systems, often face difficulties in assembling enough examples to support reliable supervised learning [52].

ISSN: 3079-6342

Algorithmic bias introduces another layer of concern, raising important issues of fairness, equity, and unintended discrimination in automated financial decision-making. Biases present in training data-where historical records may reflect unequal treatment or systemic discrimination-can be inadvertently learned and reinforced by ML models [53]. Feature bias arises when certain input variables correlate with protected characteristics such as gender or race, potentially leading to discriminatory outcomes even when these attributes are not explicitly included in the model. Sampling bias occurs when datasets fail to adequately represent all relevant groups, resulting in poorer model performance for underrepresented populations. Measurement bias, meanwhile, emerges when data collected for some groups is systematically less accurate, leading to uneven prediction quality and inconsistent results across different segments of the population.

Cybersecurity and data privacy concerns intensify with AI systems that centralize sensitive financial information and create new attack surfaces. Large financial datasets required for ML training present attractive targets for cyberattacks seeking proprietary business information or personal data [56]. Model theft attacks extract proprietary ML models through carefully designed queries, enabling competitors to replicate AI capabilities without investment [57]. Adversarial attacks craft malicious transactions designed to evade fraud detection or manipulate accounting classifications through exploitation of model vulnerabilities [58]. Privacy-preserving ML techniques including federated learning and differential privacy incur accuracy costs while protecting sensitive information [54].

Integration complexity with legacy systems presents practical challenges for deploying AI in established accounting environments. Many organizations operate decades-old ERP and accounting systems with limited API capabilities and proprietary data formats that resist integration with modern AI platforms [49]. Real-time data synchronization between legacy systems and AI components requires careful architecture design to maintain consistency and prevent race conditions. Maintaining multiple versions of accounting processes during gradual AI rollout increases complexity and potential for inconsistencies. Technical debt accumulation from incremental additions rather than comprehensive redesign creates fragile systems requiring extensive maintenance.

Change management and workforce concerns emerge as AI automation affects traditional accounting roles and required skill sets. Accounting professionals express anxiety about job displacement as routine tasks become automated, creating resistance to AI adoption [22]. Skill gaps exist as current accounting education emphasizes manual processes and human judgment rather than data science and AI collaboration capabilities [59]. Organizational change management challenges include overcoming skepticism, building trust in automated systems, and redesigning workflows to optimize human-AI collaboration. Ethical concerns arise regarding appropriate balance between automation and human oversight in high-stakes financial decisions.

Model governance and lifecycle management require systematic processes for developing, deploying, monitoring, and updating accounting AI systems. Model validation procedures must verify accuracy, reliability, and appropriate behavior before production deployment [55]. Continuous performance monitoring detects degradation from concept drift, data quality issues, or software defects requiring intervention. Model retraining strategies balance currency against stability, as frequent updates may disrupt operations while stale models lose accuracy. Version control and audit trails document model evolution, training data provenance, and decision history for regulatory and internal review purposes. Governance frameworks assign

ISSN: 3079-6342

accountability for AI system behavior and establish escalation procedures for handling errors or unexpected outcomes.

Generalization challenges limit AI system applicability across diverse accounting contexts, organizations, and regulatory environments. Models trained on data from specific industries or company sizes may not transfer effectively to different contexts with distinct transaction patterns and business models [27]. Accounting standard variations across jurisdictions complicate development of universally applicable AI systems requiring region-specific adaptations. Customization requirements for organizational accounting policies and procedures increase implementation costs and complexity. Limited availability of benchmark datasets and standardized evaluation metrics hinders objective comparison of different AI approaches and slows research progress [19].

Future research directions include development of few-shot learning approaches that achieve strong performance with limited labeled examples, addressing data availability constraints for specialized fraud types and smaller organizations [52]. Meta-learning algorithms that quickly adapt to new tasks and contexts could enable more generalizable accounting AI systems requiring less customization. Causal inference methods that identify true cause-effect relationships rather than spurious correlations would improve model robustness and provide more reliable insights for decision-making [60]. Multi-modal learning integrating quantitative transaction data with qualitative information from documents, communications, and external data sources promises more comprehensive understanding of financial activities.

Federated learning approaches enable collaborative development of fraud detection and accounting accuracy models across organizations while preserving data privacy and confidentiality [54]. Distributed training on decentralized data yields models benefiting from collective experience without centralizing sensitive information. Secure multi-party computation and homomorphic encryption enable joint analysis while maintaining cryptographic privacy guarantees. Cross-organizational collaboration accelerates model development and improves fraud detection by exposing systems to broader attack patterns than any single organization encounters.

7. Conclusion

AI technologies have reshaped accounting by introducing intelligent automation, advanced analytics, and real-time monitoring that improve accuracy, strengthen fraud detection, and enhance financial transparency. ML, DL, and NLP now process massive volumes of structured and unstructured financial data, reducing errors, accelerating workflows, and uncovering insights beyond the reach of traditional methods.

Fraud detection has seen the greatest progress, with AI models identifying suspicious patterns and anomalies across schemes such as financial misstatements, asset misuse, and money laundering. Supervised learning achieves over 90% detection accuracy, while unsupervised and graph-based approaches reveal new and coordinated fraud behaviors. Real-time systems enable rapid response, minimizing losses and outperforming rule-based methods.

AI also transforms financial transparency through continuous auditing, automated compliance, and blockchain integration that ensures immutable audit trails and real-time verification. NLP improves disclosure clarity, and automated reporting enhances timeliness and consistency, shifting financial communication toward continuous, real-time assurance.

ISSN: 3079-6342

Despite these advances, challenges remain. Data quality, model interpretability, regulatory gaps, legacy system integration, and workforce adaptation continue to hinder adoption. Addressing them requires collaboration among developers, accountants, and regulators to establish transparent governance and responsible AI use.

Looking ahead, research will focus on integrating multiple AI technologies into unified systems, using multimodal learning and causal inference for deeper insights, and enabling smaller firms through few-shot learning. The transformation of accounting through AI is ongoing-its success will depend on thoughtful governance, ethical deployment, and continuous innovation to build a more accurate, secure, and transparent financial ecosystem.

References

[1] Agustí, M. A., & Orta-Pérez, M. (2023). Big data and artificial intelligence in the fields of accounting and auditing: a bibliometric analysis. Spanish Journal of Finance and Accounting/Revista Española de Financiación y Contabilidad, 52(3), 412-438.
[2] Al-Hashimy, H. N. H. (2022). A review of accounting manipulation and detection: Technique and prevention methods. International Journal of Business and Management Invention, 11(10), 82-89.
[3] Nita, B. (2025). Occupational Fraud in Central and Eastern Europe: Mechanisms, Detection and Prevention Strategies. Modern Tools for Fraud Detection: Insights from the V4 and Ukraine, 32..
[4] Dayeh, J. (2025). Audit and Artificial Intelligence: Audit data analytics and auditing AI.
[5] Bello, H. O., Ige, A. B., & Ameyaw, M. N. (2024). Adaptive machine learning models: Concepts for real-time financial fraud prevention in dynamic environments. World Journal of Advanced Engineering Technology and Sciences, 12(02), 021-034.
[6] Zhang Y, Xiong F, Xie Y, et al. The impact of artificial intelligence and blockchain on the accounting profession. IEEE Access. 2020;8:110461-110477.
[7] Khatri, A. (2025). Record keeping. Publifye AS.
[8] Canhoto AI, Clear F. Artificial intelligence and machine learning as business tools: A framework for diagnosing value destruction potential. Bus Horiz. 2020;63(2):183-193.
[9] Oko-Odion, C. (2025). AI-Driven Risk Assessment Models for Financial Markets: Enhancing Predictive Accuracy and Fraud Detection. International Journal of Computer Applications Technology and Research, 14(04), 80-96.
[10] Turner, L., Weickgenannt, A. B., & Copeland, M. K. (2020). Accounting information systems: controls and processes. John Wiley & Sons.
[11] Pourhabibi T, Kok S, Balubaid M, Zaman M. Fraud detection: A systematic literature review of graph-based anomaly detection approaches. Decis Support Syst. 2020;133:113303.
[12] Hilal W, Gadsden SA, Yawney J. Financial fraud: A review of anomaly detection techniques and recent advances. Expert Syst Appl. 2022;193:116429.
[13] Sarna, N. J., Rithen, F. A., Jui, U. S., Belal, S., Amin, A., Oishee, T. K., & Islam, A. M. (2025). AI Driven Fraud Detection Models in Financial Networks: A Review. Ieee Access.
[14] Mirishli, S., Schreyer, M., & Hemati, H. (2025). From Periodic Audits to Continuous Assurance: Leveraging AI for Real-Time Risk Detection and Compliance.
[15] Bonsón E, Bednárová M. Blockchain and its implications for accounting and auditing. Meditari Account Res. 2019;27(5):725-740.
[16] Oyewole, A. T., Adeoye, O. B., Addy, W. A., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Automating financial reporting with natural language processing: A review and case analysis. World Journal of Advanced Research and Reviews, 21(3), 575-589.
[17] Dai J, Vasarhelyi MA. Toward blockchain-based accounting and assurance. J Inf Syst. 2019;31(3):5-21.
[18] Saraswat, D., Bhattacharya, P., Verma, A., Prasad, V. K., Tanwar, S., Sharma, G., ... & Sharma, R. (2022). Explainable AI for healthcare 5.0: opportunities and challenges. IEEe Access, 10, 84486-84517.
[19] Albuquerque, F., & Dos Santos, P. G. (2023). Recent Trends in Accounting and Information System Research: A Literature Review Using Textual Analysis Tools. FinTech, 2(2), 248-274.

ISSN: 3079-6342

[20] Pickering, L., Cohen, K., & De Baets, B. (2025). A Narrative Review on the Interpretability of Fuzzy Rule-Based Models from a Modern Interpretable Machine Learning Perspective. International Journal of Fuzzy Systems, 1-20.

[21] Kelton, A. S., & Murthy, U. S. (2023). Reimagining design science and behavioral science AIS research through a business activity lens. International Journal of Accounting Information Systems, 50, 100623.

[22] Moll J, Yigitbasioglu O. The role of internet-related technologies in shaping the work of accountants: New directions for accounting research. Br Account Rev. 2019;51(6):100833.

[23] Cooper LA, Holderness Jr DK, Sorensen TL, Wood DA. Robotic process automation in public accounting. Account Horiz. 2019;33(4):15-35.

[24] Huang F, Vasarhelyi MA. Applying robotic process automation in auditing: A framework. Int J Account Inf Syst. 2019;35:100433.

[25] Bertomeu J, Cheynel E, Floyd E, Pan W. Using machine learning to detect misstatements. Rev Account Stud. 2021;26(2):468-519.

[26] Gal U, Jensen TB, Stein MK. Breaking the vicious cycle of algorithmic management: A virtue ethics approach to people analytics. Inf Organ. 2020;30(2):100301.

[27] Chafai, N., Bonizzi, L., Botti, S., & Badaoui, B. (2024). Emerging applications of machine learning in genomic medicine and healthcare. Critical Reviews in Clinical Laboratory Sciences, 61(2), 140-163.

[28] Huang, A. H., Wang, H., & Yang, Y. (2023). FinBERT: A large language model for extracting information from financial text. Contemporary Accounting Research, 40(2), 806-841.

[29] Duane, J., Morgan, A., & Carter, E. (2025). A Review of Financial Data Analysis Techniques for Unstructured Data in the Deep Learning Era: Methods, Challenges, and Applications. OSF Preprints, (gdvbj_v1)..

[30] Ning, J., Tao, L., Mi, B., & Zhang, L. (2025). The use of managerial tone in corporate disclosure: a literature review in accounting and finance. Journal of Accounting Literature, 1-88.

[31] Maxima, A. (2024). Integration and analysis of unstructured data towards database optimization and decision making using deep learning techniques (Doctoral dissertation, Kampala International University).

[32] Rane, N., Choudhary, S. P., & Rane, J. (2024). Ensemble deep learning and machine learning: applications, opportunities, challenges, and future directions. Studies in Medical and Health Sciences, 1(2), 18-41.

[33] Kalideen, M. R. (2025). Detection of Fraudulent Transaction Issues in the Payment Card Industry using Machine Learning: A Comprehensive Survey.

[34] Chalapathy R, Chawla S. Deep learning for anomaly detection: A survey. arXiv preprint arXiv:1901.03407; 2019.

[35] Wang, L., Li, P., Xiong, K., Zhao, J., & Lin, R. (2021, October). Modeling heterogeneous graph network on fraud detection: A community-based framework with attention mechanism. In Proceedings of the 30th ACM international conference on information & knowledge management (pp. 1959-1968).

[36] Weber M, Domeniconi G, Chen J, et al. Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics. ACM SIGKDD Workshop Anomaly Detect Finance. 2019;2019:1-9.

[37] Pumsirirat A, Yan L. Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine. Int J Adv Comput Sci Appl. 2019;9(1):18-25.

[38] Ajibade, S. S. M., Jasser, M. B., Alebiosu, D. O., Al-Hadi, I. A. A. Q., Al-Dharhani, G. S., Hassan, F., & Bright, A. G. (2024). Uncovering the dynamics in the application of machine learning in computational finance: a bibliometric and social network analysis. International Journal of Economics and Financial Issues, 14(4), 299.

[39] Sharma, N., & Shambharkar, P. G. (2025). Multi-attention DeepCRNN: an efficient and explainable intrusion detection framework for Internet of Medical Things environments. Knowledge and Information Systems, 1-67.

[40] van Tilburg, D. H. C. (2025). AUDIT AUTOMATION: LEVERAGING NLP AND MACHINE LEARNING TO ENHANCE MD&A COMPLIANCE VERIFICATION (Doctoral dissertation, Tilburg University).

[41] Ünver, A. (2023). Emerging technologies and automated fact-checking: Tools, techniques and algorithms. Techniques and Algorithms (August 29, 2023).

ISSN: 3079-6342

[42] Schmitz J, Leoni G. Accounting and auditing at the time of blockchain technology: A research agenda. Aust Account Rev. 2019;29(2):331-342.

[43] Yue W, Wang Z, Chen H, et al. Machine learning with applications in breast cancer diagnosis and prognosis. Des Autom Embed Syst. 2019;23(3):105-130.

[44] Arrieta AB, Díaz-Rodríguez N, Del Ser J, et al. Explainable artificial intelligence: Concepts, taxonomies, opportunities and challenges toward responsible AI. Inf Fusion. 2020;58:82-115.

[45] Setzu M, Guidotti R, Monreale A, et al. GLocalX: From local to global explanations of black box AI models. Artif Intell. 2021;294:103457.

[46] Owoade, A. A. (2025). Improved Stock Price Prediction Model in the Nigeria Bank Sector Using Ensemble Machine Learning Models. University of Ibadan Journal of Science and Logics in ICT Research, 13(1), 38-51.

[47] Goodell JW, Kumar S, Lim WM, Pattnaik D. Artificial intelligence and machine learning in finance: Identifying foundations, themes, and research clusters from bibliometric analysis. J Behav Exp Finance. 2021;32:100577.

[48] Huang, C., Zhou, J., Chen, J., Yang, J., Clawson, K., & Peng, Y. (2023). A feature weighted support vector machine and artificial neural network algorithm for academic course performance prediction. Neural Computing and Applications, 35(16), 11517-11529.

[49] Gotthardt, M., Koivulaakso, D., Paksoy, O., Saramo, C., Martikainen, M., & Lehner, O. (2020). Current state and challenges in the implementation of smart robotic process automation in accounting and auditing. ACRN Journal of Finance and Risk Perspectives.

[50] Yu, J., & Hwang, Y. S. (2024). The interaction effects of board independence and digital transformation on environmental, social, and governance performance: complementary or substitutive?. Sustainability, 16(20), 9098.

[51] Rudin C, Radin J. Why are we using black box models in AI when we don't need to? Harvard Data Sci Rev. 2019;1(2):1-10.

[52] Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., ... & Rahmani, A. M. (2021). Deep learning-based intrusion detection systems: a systematic review. IEEE Access, 9, 101574-101599.

[53] Trinh, T. K., & Zhang, D. (2024). Algorithmic fairness in financial decision-making: Detection and mitigation of bias in credit scoring applications. Journal of Advanced Computing Systems, 4(2), 36-49.

[54] Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). A survey on federated learning. Knowledge-Based Systems, 216, 106775.

[55] Jourdan, N. (2024). Addressing Concept Drift in Machine Learning-Based Monitoring of Manufacturing Processes.

[56] Hasan, L., Hossain, M. Z., Johora, F. T., & Hasan, M. H. (2024). Cybersecurity in accounting: Protecting financial data in the digital age. European Journal of Applied Science, Engineering and Technology, 2(6), 64-80.

[57] veria Hoseini, S., Suutala, J., Partala, J., & Halunen, K. (2024). Threat modeling AI/ML with the Attack Tree. IEEE Access.

[58] Xie, Y., Shan, J., Wei, L., Yao, J., & Zhou, M. (2025). GAN-based Hybrid Sampling Method for Transaction Fraud Detection. IEEE Transactions on Knowledge and Data Engineering.

[59] Tavares, M. C., Azevedo, G., Marques, R. P., & Bastos, M. A. (2023). Challenges of education in the accounting profession in the Era 5.0: A systematic review. Cogent Business & Management, 10(2), 2220198.

[60] Lamsaf, A., Carrilho, R., Neves, J. C., & Proença, H. (2025). Causality, machine learning, and feature selection: a survey. Sensors, 25(8), 2373.