Dulgeridis, Marcel; Schubart, Constantin; Dulgeridis, Sabrina

Working Paper

Harnessing AI for accounting integrity: Innovations in fraud detection and prevention

IU Discussion Papers - Business & Management, No. 4 (July 2025)

Provided in Cooperation with:
IU International University of Applied Sciences

Suggested Citation: Dulgeridis, Marcel; Schubart, Constantin; Dulgeridis, Sabrina (2025) : Harnessing AI for accounting integrity: Innovations in fraud detection and prevention, IU Discussion Papers - Business & Management, No. 4 (July 2025), IU Internationale Hochschule, Erfurt, https://doi.org/10.56250/4065

This Version is available at:
https://hdl.handle.net/10419/321858

INTERNATIONALE HOCHSCHULE

www.iu.de

IU DISCUSSION PAPERS

Business & Management

Harnessing AI for Accounting Integrity: Innovations in Fraud Detection and Prevention

MARCEL DULGERIDIS
CONSTANTIN SCHUBART
SABRINA DULGERIDIS

IU Internationale Hochschule

Main Campus: Erfurt

Juri-Gagarin-Ring 152

99084 Erfurt

Telefon: +49 421.166985.23

Fax: +49 2224.9605.115

Contact: kerstin.janson@iu.org

Contact to the author(s):
Prof. Dr. Marcel Dulgeridis and Prof. Dr. Constantin Schubart

ORCID-ID: 0009-0009-4248-3067 (Open Researcher und Contributer ID)

IU Internationale Hochschule - Campus Regensburg

Johanna-Kinkel-Straße 3+4

93049 Regensburg

Email: marcel.dulgeridis@iu.org

Email: constantin.schubart@iu.org

IU Discussion Papers, Reihe: Business & Management, Vol. 6, No. 4 (JUL 2025)

ISSN: 2750-0683

DOI: https://doi.org/10.56250/4065

Website: https://repository.iu.org

HARNESSING AI FOR ACCOUNTING INTEGRITY: INNOVATIONS IN FRAUD DETECTION AND PREVENTION

Marcel Dulgeridis

Constantin Schubart

Sabrina Dulgeridis

ABSTRACT:

Accounting fraud poses significant financial and reputational risks for organizations. Traditional detection methods — such as manual audits and red-flag indicators — struggle to keep pace with the growing volume and complexity of financial data. In contrast, artificial intelligence technologies, including machine learning, anomaly detection, and natural language processing, offer scalable, real-time solutions to identify suspicious activity more efficiently.

This paper compares conventional fraud detection techniques with AI-driven approaches, highlighting their respective strengths and limitations in terms of accuracy, efficiency, scalability, and adaptability. While AI enables faster and more comprehensive analysis, it also raises challenges related to data quality, algorithmic bias, and transparency. Ethical and legal considerations, including data privacy and compliance with regulations, are crucial for responsible implementation.

The paper concludes with strategic recommendations for adopting AI-based fraud detection systems — emphasizing AI readiness, robust data governance, and human oversight. With a thoughtful approach, AI has the potential to significantly enhance the detection and prevention of accounting fraud.

KEYWORDS:

Artificial Intelligence, Fraud Detection, Machine Learning, Anomaly Detection, Natural Language Processing, Data Quality, Financial Fraud, Auditor Oversight, Transparency, AI Implementation.

AUTHORS

Marcel Dulgeridis *is a Professor of Business Administration at the Regensburg campus. With extensive academic experience and deep expertise across various business disciplines, he is passionately engaged in both teaching and research. Prior to his academic career, Marcel worked at Big Four firms and is now Head of Accounting at a regional bank.*

Constantin Schubart *is Professor of General Business Administration at IU Erfurt. His research interests lie in corporate and personnel development in the digital space. He is also the founder of the consulting company Schubart Consulting.*

Sabrina Dulgeridis *is Head of Department at VR TeilhaberBank. In addition to her managerial role, she works intensively on the optimization of processes in quality management and the design of customer-oriented communication strategies. In doing so, she develops recommendations for action that meet both internal requirements and the needs of customers.*

Rethinking Fraud Detection:

Why Traditional Methods No Longer Suffice

Accounting fraud is an issue in the global financial system, which causes serious economic, legal, and reputational repercussions to organizations, investors, and regulators. Falsification of accounts, asset misappropriation, and manipulation of earnings are all fraud and have caused immense losses and erosion of investor confidence. With the increasing complexity of financial flows and the growing volume of data, traditional methods for spotting fraud become less and less appropriate. The growing sophistication of fraud schemes, torrent of financial streams, and advancements of technology require a paradigm shift to predictive, scalable, and dependable fraud-detection solutions.

Manual audit and red-flag indicators have formed the essence of the accounting rules. Manual audits in reviewing financial records to check for anomalies or discrepancies typical of fraud are used in human judgment (Nabila et al.,2021, p. 50). These are typically laggard and retrospective approaches where the auditors are constrained by the size and breadth of data to examine. Red-flag indicators such as rare operations and document discrepancies also function as fraud-detection mechanisms but can only detect the presence of earlier fraud patterns or apparent schemes that conform to current fraud patterns.

Conversely, Artificial Intelligence (AI) offers a revolutionary answer to such challenges. AI systems like machine learning (ML), anomaly detection, and natural language processing (NLP) offer the means to scan huge volumes of data in real-time and spot unobvious patterns and inconsistencies likely to evade human auditors. These AI tools are unencumbered by the constraints of conventional methodologies and thus help organizations to identify fraud at an early stage, reduce the risk exposure, and enhance the overall efficiency of fiscal oversight.

The main reason for implementing AI in fraud detection systems is its ability to quickly process large datasets and recognize patterns they might ignore. Machine learning algorithms learn and become better at detecting fraud as they are shown more information over time (Ashtiani & Raahemi, 2021, p. 72505). Anomalies are detected by anomaly detection methods and flagged as unusual transactions or behaviors different from common patterns. Natural language processing is used to look at unstructured data like emails and contracts to pick up on suspicious language. This paper discusses how the role of AI in detecting accounting fraud has evolved compared to traditional methods.

RETHINKING FRAUD DETECTION: THE AI ADVANTAGE

To what extent can artificial intelligence enhance the early detection and prevention of accounting fraud compared to traditional audit methods, and how can its use be aligned with ethical, legal, and governance requirements in corporate practice?

Conceptual Cornerstones

Artificial Intelligence in fraud detection is more than a technological progression, but it is closely related to several theoretical frameworks that gives it application. These frameworks give some clarity regarding mechanisms behind AI tools, how AI helps humans in improving their capabilities and why these tools are critical to detection and prevention of accounting fraud.

DISTINCTION BETWEEN BALANCE SHEET OBFUSCATION AND BALANCE SHEET FRAUD

One of the main differences in detecting fraud is between obfuscation and fraud on the balance sheet. Obfuscation is the manipulation of financial records to conceal a firm's actual financial state but does so without falsification. A firm might utilize complicated accounting practices to conceal liabilities or even artificially inflate the revenue it has generated, making it hard to evaluate the firm's financial standing and condition using the standard methods. Obfuscation is both unethical and deceptive, but it is not necessarily fraud.

Conversely, fraud entails the intentional misstatement of financial data with the purpose of misleading stakeholders. Fraudulent activities involve overstating earnings, hiding liabilities, or creating fake assets to give a misleading impression of the firm's financial condition (Padmalosani and Balaji, 2024). AI facilitates the detection of obfuscation and fraud by finding discrepancies and inconsistencies in vast datasets that are difficult to identify using conventional methods. Anomaly detection algorithms and other AI tools are capable of highlighting inconsistencies in financial data and enabling the auditor to catch potential fraud or obfuscation early on (Hasan, 2022, p. 442).

APPLICATION OF DONALD CRESSEY'S FRAUD TRIANGLE

The Fraud Triangle, developed by Donald Cressey in 1953, is a popular and commonly accepted theory to describe the psychological causes of fraud. The model defines three essential elements in providing a setting to perpetrate fraud: pressure, opportunity, and rationalization.

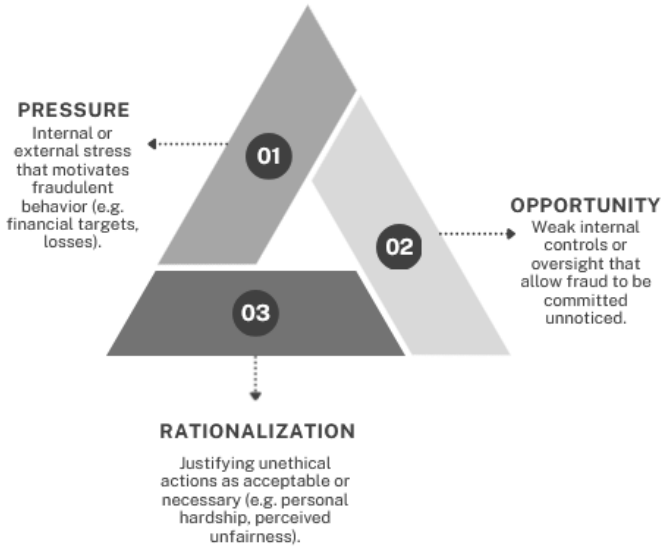


Figure 1: Fraud Triangle; Source: Own representation

Pressure: People might experience internal or external pressure to perpetrate fraud. In accounting terms, it could be pressure to achieve financial targets, keep share prices stable, or hide losses. AI systems can detect signs of pressure by scanning to identify anomalous financial patterns or behavior different from the expected (Supriadi, 2024, p. 50). For instance, AI might report on transactions signaling an effort to manipulate financial figures under pressure (Md Shakil Islam and Nayem Rahman, 2025, p. 101).

Opportunity: There is fraud when it is possible to falsify financial records without anyone noticing. Inadequate internal controls, insufficient oversight, or simple access to confidential information may give rise to such opportunities. AI takes care of the Opportunity component of the Fraud Triangle by monitoring all transactions in real-time and alerting any suspicious behavior indicative of fraud (Zhang et al., p.100619). For example, AI applications can identify anomalies in journal entries, transactions, or the behavior of certain employees and close any opportunities for fraud to go undetected (Odonkor et al., 2024, p. 172).

Rationalization: The third element of the fraud triangle is rationalization, whereby individuals rationalize their illegal activities. In accounting fraud, it might entail a person persuading themselves that the enterprise will not suffer harm or that they are entitled to manipulation because of difficulties in their life or perceived injustices. Although AI does not directly deal with rationalization, it does pick up on suspicious behavioral patterns indicative of fraud motives, which should be further inspected by accountants (Bhowte et al., 2024).

INCLUSION OF ADAMS' EQUITY THEORY

Another theoretical model accounting for financial fraud is Adams' Equity Theory, which proposes individuals are most likely to cheat when they perceive a discrepancy between their contributions (effort, time, and resources) and their payoff (rewards in terms of pay and appreciation) relative to others (Adams, 1965). In accounting fraud settings, if they do not believe they are paid equitably relative to others for their work, they might justify fraudulent actions like overstating revenues or diverting cash.

AI will assist in identifying rationalization by observing behavior patterns that could signify perceived injustices. The example of an underpaid worker rationalizing or falsifying financial records to "even out" a perceived system of injustice is a typical case. While AI will itself do nothing to address the psychological motives, it will alert to patterns of behavior like suspicious transaction patterns or account modifications, which could indicate fraud driven by perceived injustices (Hasan, 2022, p. 445).

Conventional Methods for Account Fraud Detection

MANUAL AUDITS AND RED-FLAG INDICATORS

Manually conducted audits have been the most common means of detecting and even preventing accounting fraud for decades. Auditors examine financial records, internal controls, and transaction data to identify discrepancies, irregularities, or suspicious activity that indicates fraud. Manual audits rely on human experience and judgment to ascertain the validity and veracity of fiscal data.

They typically consist of meticulously checking account balances, transaction history, and conformance with accounting rules (Bhowte et al., 2024, p. 1). Although applicable to a certain degree, the process is labor-intensive and subject to human error when dealing with datasets or financial dealings with huge data sizes or complicated schemes.

Another tool found in conventional fraud identification is the determination of red-flag indicators, which are symptoms or warning signs reflecting possible fraudulent activity. Irregularities such as

increases in unforeseen surges in revenue, differences between multiple financial reports, or dramatic changes in ratios of finances in contrast to general industry patterns are some examples of red-flag indicators (Hasan, 2022, p. 442). Red-flag indicators are typically reactive and pick up on issues after the fact and are not as adept at detecting more advanced or up-and-coming fraud schemes.

Along with red-flag indicators, whistleblower mechanisms are now part of fraud management in organizations. The mechanisms permit stakeholders or employees to report suspected irregularities anonymously, encouraging employees to report unethical practices occurring in the workplace. Although whistleblowing is a useful means to manage fraud, it depends on individuals observing anomalies and having the willingness to report the same, which may or may not happen (Shbail et al., 2023, p. 285).

THE STRENGTHS AND WEAKNESSES OF TRADITIONAL APPROACHES

Traditional fraud identification techniques have several benefits, including using the expertise and professional skepticism of individuals to analyze difficult financial information. Red-flag systems and hands-on audits are beneficial when fraud is blatant or straightforward. Human auditors are also better positioned to tell the story around anomalous transactions and use professional judgment to ascertain if the anomalous transaction is legitimate or fraudulent (Sarma and Dey, 2021).

Nonetheless, conventional approaches have some shortcomings, particularly in the data-intensive and fast-moving financial world of today. Manually conducted audits are necessarily time and resource intensive. In the case of vast data production daily by large conglomerates and global organizations, it is no longer tractable for manual auditors to check every transaction or accounting record in detail. Consequently, manually conducted audits end up using sample methods whereby a tiny fraction of the transactions are checked, which leaves a risk of failing to identify fraud (Odonkor et al., 2024, p. 172). The problem is exacerbated by cognitive biases that might affect the capacity of the auditors to identify fraud. For example, fraud schemes following a standard pattern might go unnoticed by the auditors or the auditors might shy away from marking out certain schemes if they are aligned with the overall objectives of the organization (Max et al., 2021, p. 578).

Another main drawback of conventional methods is non-scalability. As organizations grow and the sophistication of financial operations rises, manual audits are less efficient in giving real-time insights. Traditional methods are quite difficult to use in identifying fraud in real-time because they are often used to review financial data retrospectively. The delay in fraud identification exposes organizations to substantial financial losses and damage to their reputation before the time corrective action could be undertaken (Hilal et al., 2021, p. 116429).

In addition, fraud detection using red-flag indicators is less than adequate in detecting novel or sophisticated schemes of fraud. Red-flag indicators are typically evaded by fraudsters through evasive acts and leaves it difficult for fraud to be detected by auditors using conventional risk indicators. Conventional fraud methodologies thus do not possess the ability to regularly maintain and learn from experiences as it relates to fraud tactics, and it severely detracts from their usefulness in the dynamic financial landscape today (Kushwaha, 2023, p. 15).

Artificial Intelligence in Accounting: A New Era

Artificial Intelligence has been a revolutionary technology in accounting and fraud detection. Building on advancements in natural language processing (NLP), anomaly detection, and machine learning, AI can sift through vast amounts of financial data and learn to recognize suspicious patterns swiftly and efficiently. Unlike traditional methods of manual verification and judgment by humans, AI products are designed to scale and scale up as the need arises, enabling the ability to spot fraud in real time and to provide auditors with insights previously out of reach.

OVERVIEW OF AI TOOLS: MACHINE LEARNING, NLP, AND ANOMALY DETECTION

Machine learning is widely used among AI methods to detect fraud. ML algorithms gain knowledge from existing data sets and use that knowledge to dynamically forecast results or spot unusual activities as they occur in real situations (Ashtiani & Raahemi, 2021, p. 72505). In financial fraud detection, ML approaches learn how to identify warnings of fraud by analyzing previous fraud experiences. An ML model could, in practice, be trained to recognize out-of-the-ordinary vendor payment patterns, such as large or infrequent claims, and instantly alert accountants to possible fraud.

Natural Language Processing (NLP) is another significant AI method used to help recognize fraud. Unstructured information, such as audit reports, emails, contracts, and financial records, is examined by NLP to look out for signs of fraud. NLP software can recognize irregularities in dates and signatures, as well as other questionable word choices in financial accounts, and these types of abnormalities are hard for people to spot by hand (Hilal et al., 2021, p. 116429). The use of NLP software to automate text evaluation improves both the speed and precision with which fraud is found in financial paperwork that would typically be missed.

Anomaly Detection is a technique used by AI to identify abnormal patterns of behavior or transactions that fail to fit in normal patterns. An example is how anomaly detection software can identify irregular patterns of change in expenditures, like a sudden increase in expenses or unusually large payments to a particular vendor. The algorithms scan on an ongoing basis in real time and alert immediately when a discrepancy is found (Md Shakil Islam & Nayem Rahman, 2025, p. 110). While conventional methods may count on red-flag indicators or sample reviews, AI-based anomaly detection can review each transaction and thus is much better at detecting fraud early on.

TECHNOLOGICAL FOUNDATIONS AND FUNDAMENTAL CAPABILITIES

The speed and precision with which large data sets are analyzed by AI are two of its biggest strengths when compared to conventional methods of detecting fraud. Supplied learning algorithms are used to identify a transaction as fraudulent or legitimate and are a common technique used in fraud identification (Ashtiani & Raahemi, 2021, p. 72505).

The algorithms are trained on data related to past fraud and are henceforth able to recognize patterns of fraud and mark the same patterns in subsequent data. The same process is refined on a continuous basis as additional data becomes available, and thus models become more precise as time goes on.

Conversely, unsupervised learning is applied when there is inadequate labeled data to train. The algorithm is required to learn patterns or groups of data on its own in such scenarios. Unsupervised anomaly identification is especially helpful to identify fresh or innovative fraud methods unaccounted for in the past. Through learning natural patterns in data, unsupervised learning algorithms can detect fraud deviating from past patterns (Bhowte et al., 2024).

Another essential AI function is Robotic Process Automation (RPA), which may be used together with AI tools to automate preprocessing of financial data. RPA may capture and classify financial information from different sources like invoices or bank statements and pump it into AI models to be analyzed further. RPA reduces the amount of manual work to do fraud detection and enhances the general efficiency of the process by automating these mundane tasks (Odonkor et al., 2024, p. 172).

MAJOR AI VENDORS AND TOOLS AVAILABLE IN THE MARKET

Several prominent vendors and products have surfaced in AI-assisted fraud detection. MindBridge AI, for instance, applies machine learning models to automatically mark suspicious-looking transactions and identify discrepancies in financial accounts. Their product offers an auditor a fraud risk score to aid in the prioritization of high-risk transactions to investigate (Hilal et al., 2021, p. 116429). CaseWare is another vendor providing accounting fraud-detection solutions using AI. Their AI product identifies discrepancies and red flags in financial statements and audit data in real-time.

Deloitte AI also leads the way in AI implementations in fraud prevention, combining machine learning and anomaly identification to track financial activities around the clock. Deloitte's solutions are meant to identify outliers, out-of-pattern expenditures, and illegal alterations to financial data, which diminish by a considerable margin the probability of undetected fraud (Bhowte et al., 2024).

INTEGRATION WITH ENTERPRISE SYSTEMS

Fraud detection tools with artificial intelligence are now being implemented in Enterprise Resource Planning systems like SAP and Oracle. Fraud detection tools are directly accessing financial data in the core systems of the organization, which facilitates real-time fraud detection. AI models are able to review financial transactions directly as and when they are posted in ERP systems and mark any untoward behavior immediately and send alerts to auditors to investigate further (Bao et al.,2022, p. 240). The fraud detection process becomes much easier and efficient with the integration and improves AI tool effectiveness to identify fraud in the organization (Hasan, 2022, p. 44).

Comparative Analysis: Traditional vs. AI-Based Methods

Detection and prevention of accounting fraud have always been maintained through a blend of manual audits, red-flag identification, and forensic accounting. Although such methods have been central to upholding financial integrity, the fast progress of Artificial Intelligence technologies has brought in newer tools with the promise to make fraud detection much faster, more precise, and efficient. The following section contrasts the efficacy of conventional fraud-detection methods against AI-based tools based on parameters like precision, efficiency, scalability, and flexibility.

ACCURACY AND EFFICIENCY

One of the main strengths of AI fraud detection systems is their ability to accurately detect fraud. Conventional systems, like manual audits, are based on the expertise of individuals to identify inconsistencies in financial data. Although to some extent efficient, manual audits are subject to the imperfections of human judgment when dealing with huge datasets or complicated financial operations. Auditors might fail to identify fraud, skip over anomalies or misread data because of cognitive biases (Sarma and Dey, 2021, p. 9).

Conversely, AI systems like ML and anomaly detection algorithms are meant to scan huge volumes of data in a swift and precise manner. AI models learn to recognize patterns of fraudulent activities with higher accuracy by learning from past experiences of fraud cases. Over a period, AI models get better and better at fraud detection. AI's capability to scan huge volumes of data enhances fraud-detection efficiency compared to conventional means, hampered by human constraints (Hasan, 2022, p. 450).

SCALABILITY

Conventional fraud detection mechanisms are hampered by scalability challenges. Sample-based audits and red-flag indicators are insufficient to deal with the considerable amount of data that large organizations produce by their very scale. The more a firm expands and makes more financial data, the less efficient conventional fraud detection becomes. Manual audits, which involve checking a subset of transactions, risk missing fraud that happens in non-sample data (Hilal et al., 2021, p. 116429).

AI fraud detection systems are constructed to scale with ease. The systems can check all transactions in real-time and do not require manual intervention. AI tools can also monitor all datasets and pick up on anomalies in all financial records to deliver an all-encompassing service to large organizations. The scalability is especially useful for multinational organizations conducting complicated and high-volume transactions. It allows AI to achieve real-time fraud monitoring and detection in numerous business units or geographic locations (Odonkor et al., 2024, p. 172).

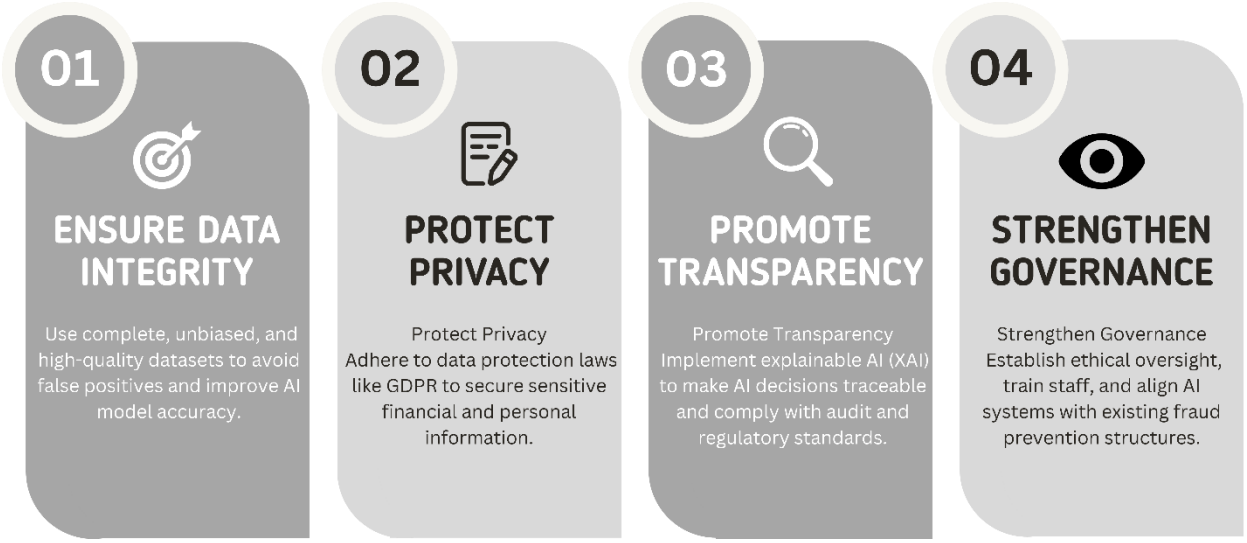
ADAPTABILITY

Another inherent strength of AI is its ability to adapt. Fraudsters themselves evolve continually and keep changing their methods of operation. Hence, fraud-detection systems also need to adjust accordingly. Conventional methods like red-flag identification are based on established patterns and parameters and may work to identify known schemes of fraud but cannot capture newer or more advanced schemes of fraud that do not fall into established patterns. AI, and especially machine learning models, are much more responsive. These models learn from new information and identify emerging patterns of fraud. The system becomes better at detecting new fraud methods that might not have been identified before as it becomes exposed to more fraud occurrences. Unsupervised learning, which does not involve labeled data, makes it possible for AI to identify anomalies other than known fraud patterns and thereby makes AI tools more responsive to newer types of fraud attempts (Ashtiani & Raahemi, 2021, p. 72505).

Limitations and Risks of AI

Although AI has numerous benefits, it also has several shortcomings. One of the main problems lies in the data quality needed to perform fraud detection efficiently. If data used to train the AI models is biased, incomplete, or uncorrected, the AI system will yield false positives (identifying legitimate transactions as fraudulent) or false negatives (missing fraudulent actions). Data quality plays a central role in ensuring the correctness of AI fraud detection systems (Shbail et al., 2023, p. 290).

Figure 2: Limitations and Risks of AI



Source: Own representation

Furthermore, AI also has a transparency problem in decision-making, known as the black-box problem. Most machine learning algorithms learn in ways that are not transparent to the analyst, and as a result, it becomes hard to tell why a specific alert or decision was generated. Lack of transparency has issues when it comes to legal or regulatory compliance (Max et al., 2021, p. 590).

ETHICAL, LEGAL, AND ORGANIZATIONAL CONSIDERATIONS

Even with the significant advances in fraud detection, enabled by AI, the introduction of AI also poses substantial ethical, legal, and organizational challenges that need to be addressed. Ethical, legal, and managerial issues are carried over to data privacy, algorithmic fairness, call for transparency, requirement of regulation, and sound governance. The solution to these challenges is crucial to enable the maximization of the reliability and trustworthiness of AI in financial vigilance.

DATA PRIVACY AND PROTECTION

Data privacy takes on the role of a significant ethical problem when AI is used in fraud detection processes. To spot patterns and unearth fraud, AI tools often must look at vast amounts of confidential financial data. Personal identifiable information (PII), a list of financial transactions, and confidential documentation on businesses are some possible data that such information may include. Although AI still has a place to play in financial oversight, companies need to be compliant with the data protection norms.

The General Data Protection Regulation imposes strict rules on how personal data should be managed, including the need to encrypt data, the ability to ask for deletion of data, and acceptance of consent before processing any data. Practices of AI in detecting fraud necessitate that organizations operate within these legal standards to protect privacy rights and to protect confidential financial information from unauthorized access. In addition, organizations should communicate to stakeholders how personal data is used and prove that individual privacy rights are respected (Max et al, 2021, p. 587).

ALGORITHMIC BIAS

Algorithmic bias is one of the main challenges faced by organizations. AI systems, especially those created using machine learning, obtain insights from existing data. If the data has biases like racial, gender, socio-economic, then such biases can be amplified by the AI model by accident, leading to discriminatory outputs. Consider, for example, a biased training dataset.

Any attempt to limit the bias risk in AI systems requires organizations to subject the data in their AI models to thorough inspection. The accuracy of fraud detection depends on the availability of representative and bias-free training data from the whole model development process. Moreover, applying explainable AI (XAI) techniques may increase transparency because it will be easier to conclude how AI systems make their decisions. Therefore, auditors and stakeholders will have a clear understanding of the AI decisions' foundation, which makes the system fair (Shbail et al., 2023, p. 290).

TRANSPARENCY AND EXPLAINABILITY

With the use of AI, there is also the tendency for AI systems to act in a way that the steps in the decision-making process are secretive, thus depriving the people responsible for auditing of an understanding. Such an absence of forward clarity often contradicts regulatory demands. Auditors and regulators must see that when AI systems fail to inform us about their decisions, organizations struggle to justify them legally and fulfill the stipulations in money rules.

Explainable Artificial Intelligence (XAI) has been created to solve this problem. These models enable transparency since it is now possible to explain clearly how AI tools reach their judgments. In fraud detection, this means showing how specific financial patterns detected by the system led to the classification of specific transactions as suspicious. If AI systems are designed to be interpretable, organizations are in better shape to develop customer confidence while staying within legal and regulatory limits (Qatawneh, 2024, p. 4380).

REGULATORY COMPLIANCE

The rapid advancements in AI are forcing regulators to deal with how they can best control such systems; the areas of focus, such as fiscal auditing and preventing fraud, are paramount. Although ISA 240, SOX, and other regulations provide directions to auditors and accountants for AI applications, they may not be sufficient for dealing with the peculiar challenges that AI applications create (Adetunji and Chinonso, 2025, p. 1228). For example, the problem of AI black-boxes introduces additional frictions that complicate the compliance of the fraud detection system with audit standards, which often require clear documentation and reasons for decisions (Hasan, 2022, p. 442).

To fill this gap, the business must work with regulating bodies to ensure that fraud detection AI tools comply with existing legal and ethical guidelines. In addition, organizations must have governance frameworks that ensure that AI tools have ethical usage protocols and put in place governance arrangements in terms of oversight and accountability.

GOVERNANCE AND ORGANIZATIONAL CHALLENGES

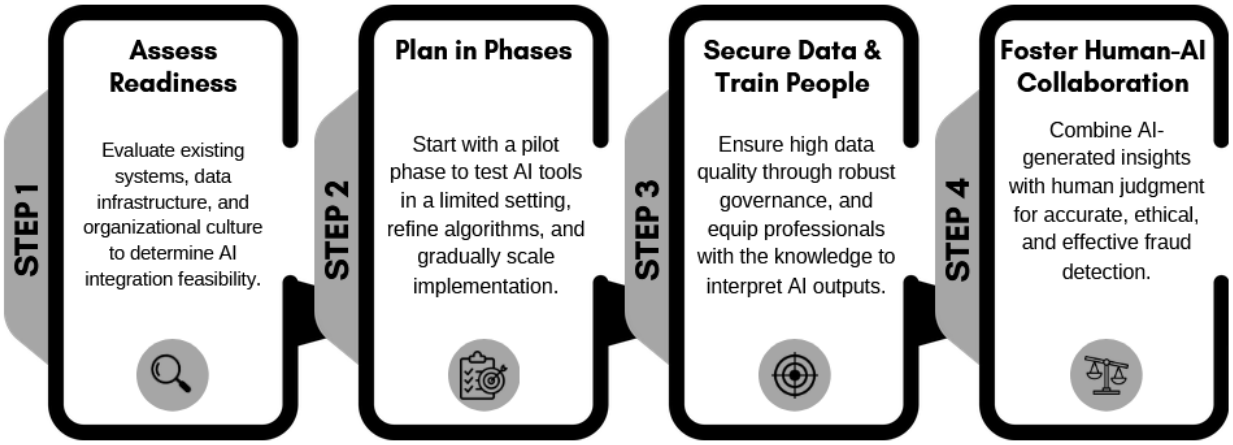
As such, using AI in fraud detection also has organizational challenges in governance, implementation, and adapting to change. Adopting AI technologies in organizations should connect with the existing fraud prevention systems. Data governing must be adopted to ensure that the financial data on which AI algorithms work is reliable and safe (Bhowte et al.,2024). Organizations should proactively limit any employee resistance caused by fear of AI or a lack of familiarity with its operations in their work.

The effectiveness of AI implementation within an organization depends on robust leadership and support from seniors, and training for auditors and staff on AI tools. Managers must formulate well-thought-out change management plans to facilitate a smooth transition to AI-assisted fraud detection, while transparently communicating the strengths, limitations, and ethical implications of these technologies to foster trust and acceptance among staff.

Strategic Recommendations for Implementation

Integrating AI into fraud detection systems requires a systematic approach and strategy to ensure that AI raises effectiveness and helps them serve organizational objectives. While progress in AI allows increasing speed, precision, and scale, the realization of a successful implementation requires consideration of the critical components, including data quality, governance, where people are involved, and responsiveness to legal and ethical norms.

Figure 3: Strategic Recommendations for Implementation



Source: Own representation

ASSESSING AI READINESS AND ORGANIZATIONAL ALIGNMENT

Before the introduction of AI to organizations for fraud detection, it is necessary to decide and consider whether they are prepared to utilize the technologies fully. Inclusion of a review of data systems, organizational technology, and culture, to see the likelihood of success of AI integration into the present framework (Bejjar et al.,2024).

For the AI fraud detection to be accurate, there is a need for datasets that are of high quality, which are not full of errors and are also uniformly formatted. To fully benefit from AI-based fraud detection, organizations must establish and handle broad-range, consistent financial data that is constantly updated (Sarma & Dey, 2021, p

Organizations need also to ensure that any AI implementation complements their current approach to fraud prevention. Adaptation of existing internal control systems to include AI tools, and development of a structured roadmap for implementing the AI tools are necessary measures.

PHASED IMPLEMENTATION APPROACH

The AI Tool deployment ought to be oriented through consecutive stepwise approach. Organizations may begin their AI deployment by performing a proof-of concept phase between a limited data selection. Such testing allows organizations to register potential barriers, evaluate the effectiveness of the model, and modify algorithms to augment the system's effectiveness. With a successful completion of piloting, then the organization can go to full implementation ensuring that AI tools are appropriately integrated into the overall fraud detection and auditing framework (Odonkor et al., 2024, p. 172).

DATA GOVERNANCE AND TRAINING

Effective AI tools deployment is not possible without effective data governance. Organizations have to establish adequate data management processes with a view to protecting the accuracy and privacy of financial information among other things. The efficiency of AI models relies on large and high-quality data launch, as the quality of the data has a huge impact on the efficiency of fraud detection systems (Bhowte et al, 2024).

Training is another essential component. The auditors and other professionals must be educated so that they can use the AI systems, interpret the results offered, and mix this information with their professional judgment. Any conduct review and monitoring process ensure continuous effectiveness and ability to adapt to evolving fraudulent habits from the AI systems (Shbail et al., 2023, p. 290).

HUMAN-AI COLLABORATION

Moreover, the use of AI should be treated as an aid, not a replacement for human auditors' skills and knowledge, which will improve the efficiency of the whole. There is high dependence on cooperation between human beings and AI systems to use AI driven insights effectively. The use of professional skepticism and judgment by the auditors to confirm the validity of the AI generated findings in confirming validity is conducive to more efficient and reliable fraud detection techniques (Hasan, 2022, p. 449).

The Road Ahead

As the complexity of fraudulent acts increases, there is an overwhelming need for effective fraudulent detection systems. Manual audits and reliance on red-flag indicators have been holding fraud detection mechanisms adopted by financial institutions since their inception. However, traditional methods find it difficult to cope up with the complexity and mass of financial data nowadays. Considering the complexities brought about by sophisticated approaches to fraud, the use of AI clearly promotes a huge advancement in fraud detection, which is faster, more reliable and capable of dealing with more data.

Technological advances in AI like machine learning, anomaly detections mechanisms and natural language processing equip organizations with greater capabilities to detect fraudulent conduct with high speed and in high accuracy in their actions of prevention of fraud. Using AI, organizations will be able to use a forward-looking strategy in discouraging fraud while past strategies focused almost entirely on fraud detection after the fact. Auditors using AI can put through massive amounts of data will find hidden patterns and anomalies that might go unnoticed which speeds up the process of detecting fraud and protects them from massive financial loss.

Although the application of AI can improve fraud detection significantly, the implementation of such an application relies on intensive planning. To ensure proper use of A in the current fraud detection frameworks, their organizations need to plan carefully to ensure data integrity, governance structures and regulatory compliance are properly adhered to. Organizations also need to explain the ethical consequences of using AI to prevent fraud, including issues of data confidentiality, equity of algorithms, and the openness of paths to decision making. The responsible use of AI tools is essential for building stakeholder trust and meeting obligations under data protection regulations.

Furthermore, successful use of AI in fraud detection requires active human over-sight. Artificial Intelligence should complement the attempt of human auditors instead of replacing them. Human and AI collaboration play a key role in revising the AI driven findings and maintaining ethical, legal and criteria for governance. The use of the strengths of both AI and human professionals enables organizations to design a fraud detection system that is both fast and accountable. The shift towards AI in accounting fraud detection is a move from the account-based approach to the data-based, forward-looking approach to fraud prevention. By constant improvement and plasticity, AI technologies may become important for fraud detection and prevention and consequently ensure the stability of finance and strengthen organizational barriers against fraudulent practices.

References:

Adetunji Paul Adejumo and Chinonso Peter Ogburie (2025). Forensic accounting in financial fraud detection: Trends and challenges. International Journal of Science and Research Archive, [online] 14(3), pp.1219–1232. doi: https://doi.org/10.30574/ijsra.2025.14.3.0815.

Ashtiani, M.N. and Raahemi, B. (2021). Intelligent Fraud Detection in Financial Statements using Machine Learning and Data Mining: A Systematic Literature Review. IEEE Access, 10, pp.72504–72525. Doi: https://doi.org/10.1109/access.2021.3096799.

Bao, Y., Hilary, G. and Ke, B. (2022). Artificial intelligence and fraud detection. Innovative Technology at the Interface of Finance and Operations, [online] 11, pp.223–247. doi: https://doi.org/10.1007/978-3-030-75729-8_8.

Bejjar, M.A. and Siala, Y. (2024). Machine Learning: A Revolution in Accounting. [online] www.igi-global.com. Available at: https://www.igi-global.com/chapter/machine-learning/343356.

Bhowte, Y.W., Roy, A., K. Bhavana Raj, Sharma, M., Devi, K. and Prem Latha Soundarraj (2024). Advanced Fraud Detection Using Machine Learning Techniques in Accounting and Finance Sector. [online] doi: https://doi.org/10.1109/iconstem60960.2024.10568756.

Hasan, A.R. (2022). Artificial Intelligence (AI) in Accounting & Auditing: A Literature Review. Open Journal of Business and Management, [online] 10(01), pp.440–465. doi: https://doi.org/10.4236/ojbm.2022.101026.

Hilal, W., Gadsden, S.A. and Yawney, J. (2021). A Review of Anomaly Detection Techniques and Applications in Financial Fraud. Expert Systems with Applications, [online] 193(1), p.116429. Available at: https://www.sciencedirect.com/science/article/pii/S0957417421017164.

Kushwaha, N.S., 2023. Application of Artificial Intelligence Methods to the Prevention of Cybercrime. Karnavati Journal of Multidisciplinary Studies, 1(2), pp.1-32.

Max, R., Kriebitz, A. and Von Websky, C., 2021. Ethical considerations about the implications of artificial intelligence in finance. Handbook on ethics in finance, pp.577-592.

Md Shakil Islam and Nayem Rahman (2025). AI-Driven Fraud Detections in Financial Institutions: A Comprehensive Study. Journal of Computer Science and Technology Studies, 7(1), pp.100–112. Doi: https://doi.org/10.32996/jcsts.2025.7.1.8.

Nabila, E.A., Santoso, S., Muhtadi, Y. and Tjahjono, B., 2021. Artificial intelligence robots and revolutionizing society in terms of technology, innovation, work and power. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 3(1), pp.46-52.

Odonkor, B., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Farayola, O.A. (2024). The Impact of AI on Accounting practices: a review: Exploring How Artificial Intelligence Is Transforming Traditional Accounting Methods and Financial Reporting. World Journal Of Advanced Research and Reviews, 21(1), pp.172–188. Doi: https://doi.org/10.30574/wjarr.2024.21.1.2721.

Padmalosani Dayalan and Balaji Sundaramurthy (2024). Exploring the Implementation and Challenges of AI-Based Fraud Detection Systems in Financial Institutions. Advances in

business information systems and analytics book series, [online] pp.25–38. Doi: https://doi.org/10.4018/979-8-3693-4187-2.ch002.

Qatawneh, A.M. (2024). The role of artificial intelligence in auditing and fraud detection in accounting information systems: moderating role of natural language processing. International journal of organizational analysis. [online] Doi: https://doi.org/10.1108/ijoa-03-2024-4389.

Sarma, W. and Dey, S. (2021). AI and Machine Learning in Fraud Detection for Finance and E-Commerce. International Journal of Innovative Research in Computer and Communication Engineering, 09(10). doi: https://doi.org/10.15680/ijircce.2021.0910040.

Shbail, A., Tareq Bani-Khalid, Husam Ananzeh, Huthaifa Al-Hazaima and Awn Al Shbail (2023). Technostress impact on the intention to adopt blockchain technology in auditing companies. Journal of Governance and Regulation, 12(3, special issue), pp.285–294. Doi: https://doi.org/10.22495/jgrv12i3siart10.

Supriadi, N.I. (2024). The audit revolution: Integrating artificial intelligence in detecting accounting fraud. Akuntansi dan Teknologi Informasi, 17(1), pp.48–61. doi: https://doi.org/10.24123/jati.v17i1.6279.

Zhang, C., Zhu, W., Dai, J., Wu, Y. and Chen, X. (2023). Ethical impact of artificial intelligence in managerial accounting. International Journal of Accounting Information Systems, 49(49), p.100619. Doi: https://doi.org/10.1016/j.accinf.2023.100619.