

Original Research Article

Role of Artificial Intelligence in Fraud Detection and Prevention in Accounting

Ms. Kaleeswari Soundrapandi

Asst. Prof., Department of Accounting and Finance, Guru Nanak College of Arts, Science and Commerce, G.T.B. Nagar, Sion East, Mumbai 400037 India

Corresponding author E-mail: kaleshwari@gncasc.org

Received: 10 September, 2026 | Accepted: 24 September, 2026 | Published: 17 October, 2026

Abstract

Fraud is one of the major challenges faced by organizations, as fraudulent activities can result in financial losses, reputational damage, regulatory penalties and loss of stakeholder confidence. The emergence of Artificial Intelligence (AI) has created new opportunities for improving fraud detection and prevention in accounting.

This research paper examines the role of Artificial Intelligence in fraud detection and prevention in accounting. The study focuses on the applications of machine learning, anomaly detection, natural language processing and predictive analytics in identifying fraudulent activities. It also discusses the benefits, limitations and ethical challenges associated with the use of AI. The study is based on secondary data collected from professional reports, research literature and authoritative publications. The findings indicate that AI can significantly strengthen fraud-risk monitoring by improving the speed, scale and consistency of transaction analysis. However, AI should not completely replace human judgment. Effective fraud prevention requires a combination of AI-based systems, internal controls, professional skepticism, employee awareness and human oversight.

Keywords: Artificial Intelligence, Accounting, Fraud Detection, Fraud Prevention, Machine Learning, Auditing, Financial Fraud, Anomaly Detection

1. Introduction

Accounting information plays an important role in business decision-making. Financial statements and accounting records help management, investors, creditors and other stakeholders evaluate an organization's financial position and performance. Therefore, accurate and reliable accounting information is essential.

Fraudulent activities such as financial statement manipulation, fictitious transactions, unauthorized payments, asset misappropriation and false expense claims can affect the reliability of accounting information. According to the ACFE's 2024 *Report to the Nations*, asset misappropriation occurred in 86% of the fraud cases studied, while financial statement fraud accounted for 5% but resulted in the highest median losses.

Traditional accounting and auditing methods remain important, but manually examining large volumes of transactions can be time-consuming. Artificial Intelligence (AI) can help overcome this challenge by analyzing large amounts of data, identifying unusual patterns and detecting suspicious transactions.

AI can support continuous fraud monitoring and provide timely alerts to accountants and auditors. However, technology should complement rather than replace human judgment, internal controls and reporting mechanisms. The ACFE also found that tips were the most common method of fraud detection, accounting for 43% of cases studied. Thus, an effective fraud-detection system requires a combination of AI, strong internal controls and human expertise.

2. Review of Literature

Kassar (2026) conducted a systematic literature review on the application of Artificial Intelligence (AI) and Robotic Process Automation in accounting and auditing. The study highlights that AI is transforming accounting and auditing by improving automation, data analysis and professional efficiency. AI technologies such as machine learning, deep learning and predictive analytics can assist professionals in identifying unusual transactions and potentially fraudulent activities. Similarly, research on financial statement fraud detection indicates that machine-learning techniques are increasingly being explored as a complement to traditional fraud-detection methods, particularly for analyzing large volumes of financial information (Journal of Financial Crime, 2023).

The literature also highlights that the effective use of AI requires appropriate governance and human oversight. The National Institute of Standards and Technology (NIST) states that trustworthy AI should be valid and reliable, secure, transparent, explainable, privacy-enhanced and fair, with harmful bias managed. These factors are particularly important when AI is used to identify financial fraud because incorrect or unexplained AI decisions may affect investigations and professional judgments. Therefore, existing literature suggests that AI has considerable potential to strengthen fraud detection and prevention, but it should complement rather than replace accountants, auditors and established internal-control mechanisms.

3. Objectives of the Study

The major objectives of the study are:

1. To examine the role of Artificial Intelligence in fraud detection and prevention in accounting.
2. To identify the major AI technologies used for detecting fraudulent financial activities.
3. To examine how AI improves the efficiency and effectiveness of accounting and auditing processes.
4. To understand the benefits of using AI for continuous monitoring of financial transactions.
5. To identify the challenges and limitations associated with AI-based fraud detection.

6. To suggest measures for effective and responsible implementation of AI in fraud-risk management.

4. Research Methodology

The present study is based on secondary data. Information has been collected from research literature, professional reports, institutional publications and authoritative online sources relating to Artificial Intelligence, accounting, auditing and fraud detection.

The study follows a descriptive and conceptual research design. It examines the applications of AI in fraud detection and prevention and evaluates its potential benefits and limitations.

Sources of Data

The major sources include:

- Association of Certified Fraud Examiners (ACFE) reports
- National Institute of Standards and Technology (NIST) publications
- Academic research papers and journals
- Professional accounting and auditing literature
- Reports and publications relating to AI and financial technology

The information collected has been analyzed thematically to understand how AI can be incorporated into accounting fraud-risk management.

5. Role of AI in Fraud Detection and Prevention

5.1 Transaction Monitoring

One of the most important applications of AI is continuous transaction monitoring. Accounting systems may contain thousands or millions of transactions. AI can examine these transactions and identify those that appear unusual.

For example, an AI system may identify:

- unusually large payments;
- duplicate invoices;
- transactions outside normal business hours;
- unusual vendor payments;
- repeated transactions involving the same account;
- transactions exceeding normal limits; and
- unusual changes in customer or supplier behaviour.

Such transactions can be automatically flagged for further investigation.

5.2 Anomaly Detection

Fraud does not always follow a predictable pattern. Criminals may change their methods to avoid traditional controls. AI-based anomaly detection can help identify unusual activities without requiring every possible fraud pattern to be predefined.

For example, suppose an organization normally makes supplier payments between ₹20,000 and ₹2,00,000. If a transaction of ₹9,50,000 is suddenly recorded for a relatively new supplier, the AI system can identify the transaction as an anomaly.

The system does not automatically conclude that the transaction is fraudulent. Instead, it generates an alert so that an accountant or auditor can investigate it.

5.3 Machine Learning

Machine learning enables computer systems to learn from data and improve their ability to identify patterns.

In accounting, machine-learning models can be trained using historical transaction data. Transactions can be classified based on characteristics such as amount, date, vendor, frequency, location and transaction type.

The model can subsequently assign a risk score to new transactions. High-risk transactions can receive greater attention from auditors.

This can improve the allocation of audit resources because auditors can focus more attention on transactions with a higher probability of fraud rather than examining every transaction with equal intensity.

5.4 Detection of Duplicate and False Invoices

Invoice fraud is a significant concern for organizations. Fraudulent invoices may involve duplicate billing, fictitious suppliers, inflated amounts or services that were never provided.

AI can compare invoices using multiple characteristics, including:

- supplier details;
- invoice numbers;
- dates;
- amounts;
- purchase orders;
- bank account details; and
- descriptions of goods or services.

AI can identify similarities between invoices that may not be immediately apparent to human reviewers.

5.5 Continuous Auditing

Traditional auditing is generally conducted periodically. AI can support continuous auditing by monitoring financial transactions on an ongoing basis.

Instead of identifying a problem several months after it occurs, organizations can receive alerts closer to the time of the transaction.

Continuous monitoring may therefore help organizations respond to suspicious activity more quickly and potentially reduce the financial impact of fraud.

5.6 Predictive Analytics

AI-based predictive analytics can be used to identify areas where fraud risk may be relatively high.

For example, an organization can analyze historical information to determine whether certain vendors, departments, transaction types or locations have experienced a higher frequency of irregularities.

The results can be used to prioritize internal audit activities and strengthen controls in high-risk areas.

5.7 Natural Language Processing

Accounting fraud may not be limited to numerical transactions. Important information may also be present in emails, contracts, invoices, reports and other documents.

Natural Language Processing (NLP), a branch of AI, can analyze large quantities of textual information. It can assist in identifying unusual language, inconsistencies or relationships between documents.

For example, an AI system could compare information contained in an invoice with the related purchase order and contract to identify potential inconsistencies.

6. Benefits of AI in Fraud Detection

6.1 Faster Detection

AI can analyze financial data much faster than manual examination. This enables organizations to identify suspicious transactions quickly.

6.2 Analysis of Large Volumes of Data

AI can examine large datasets and identify patterns across thousands or millions of transactions.

6.3 Improved Accuracy

Automated analysis can reduce certain forms of human error, particularly in repetitive transaction-review activities.

6.4 Better Allocation of Audit Resources

AI can identify high-risk transactions and allow auditors to focus their time and expertise on areas requiring investigation.

6.5 Early Warning Mechanism

AI-generated alerts can provide early warnings about potentially suspicious transactions and unusual activities.

7. Challenges and Limitations of AI

Despite its advantages, AI is not a complete solution to accounting fraud.

7.1 Data Quality

AI models depend heavily on the quality of the data used to train and operate them. Incorrect, incomplete or biased data can produce unreliable results.

7.2 False Positives

AI may sometimes classify legitimate transactions as suspicious. Excessive false alerts can increase the workload of accountants and auditors.

7.3 False Negatives

An AI system may also fail to detect sophisticated fraud. Therefore, organizations cannot assume that transactions not flagged by AI are automatically legitimate.

7.4 Lack of Explainability

Some advanced AI models may produce results that are difficult for users to understand. In accounting and auditing, explainability is important because auditors may need to justify why a transaction was considered suspicious.

7.5 Privacy and Data Security

Accounting systems contain sensitive financial and personal information. Organizations must ensure that AI systems protect this information from unauthorized access.

7.6 Implementation Cost

Developing or purchasing AI systems, integrating them with existing accounting software and training employees can require significant investment.

7.7 Changing Fraud Techniques

Fraudsters may change their methods in response to new controls. AI systems therefore need regular monitoring, testing and updating.

NIST's AI Risk Management Framework emphasizes that AI systems should be managed throughout their lifecycle and should incorporate appropriate considerations relating to reliability, security, transparency, privacy and fairness.

8. Human Role in AI-Based Fraud Detection

AI should be viewed as a tool that supports accountants and auditors rather than as a complete replacement for them.

An AI system may identify a suspicious transaction, but a qualified professional must determine why the transaction occurred and whether it represents genuine fraud.

For example, an unusually high payment may be flagged by AI. However, the payment may be legitimate if it relates to the purchase of new machinery. The auditor must examine supporting documents and business circumstances before reaching a conclusion.

Human professionals provide:

- professional judgment;
- contextual understanding;
- ethical reasoning;
- communication with management;
- interpretation of evidence; and
- final investigation and decision-making.

This human-AI combination is particularly important because fraud detection involves both quantitative patterns and qualitative information.

The ACFE's findings also demonstrate the continuing importance of human reporting mechanisms. In its 2024 study, tips accounted for 43% of initial fraud detections, making them the most common detection method.

9. Findings of the Study

Based on the review of available literature and professional sources, the following major findings emerge:

1. AI has significant potential for improving fraud detection because it can analyze large volumes of financial transactions rapidly.
2. Machine learning and anomaly detection can help organizations identify unusual transactions and patterns.
3. Continuous monitoring can improve the timeliness of fraud detection compared with relying exclusively on periodic manual reviews.
4. AI can improve audit efficiency by helping auditors prioritize high-risk transactions.
5. AI cannot eliminate fraud completely. Fraudsters can change their behavior and sophisticated fraud may remain difficult to identify.
6. Human judgment remains essential. AI alerts require investigation and professional interpretation.
7. Data quality is critical. Poor-quality or biased data can reduce the reliability of AI outputs.
8. Ethical and governance issues require attention. Organizations need appropriate controls relating to privacy, security, explainability and accountability.
9. Traditional fraud-prevention mechanisms remain important. Internal controls, segregation of duties, whistleblower systems and employee awareness should operate alongside AI.
10. The future of fraud detection is likely to involve human-AI collaboration, where technology performs large-scale analysis and professionals provide judgment and decision-making.

10. Suggestions and Recommendations

Based on the study, the following recommendations are proposed:

1. Organizations should gradually integrate AI-based fraud-monitoring systems with existing accounting and ERP systems.
2. AI models should be regularly tested and updated to respond to changing fraud patterns.
3. Organizations should establish strong data-governance policies to ensure data accuracy and security.
4. Accountants and auditors should receive training in AI, data analytics and interpretation of AI-generated alerts.
5. AI-generated alerts should be reviewed by qualified professionals before any major action is taken.
6. Organizations should maintain effective whistleblower and fraud-reporting mechanisms.
7. Internal controls should continue to be strengthened even after adopting AI technology.
8. Organizations should establish clear accountability for AI-based fraud detection systems.
9. AI systems should be evaluated for bias, reliability, security and explainability.
10. Small and medium-sized organizations should consider cost-effective AI-enabled accounting and audit solutions rather than relying only on expensive customized systems.

12. Conclusion

Artificial Intelligence is transforming accounting, auditing and fraud-risk management. Its ability to analyze large volumes of financial data, identify anomalies, monitor transactions and generate alerts makes it an effective tool for fraud detection and prevention.

The study indicates that AI can improve the speed and efficiency of fraud detection. Technologies such as machine learning, anomaly detection, predictive analytics and natural language processing can help accountants and auditors identify suspicious activities that may be difficult to detect through traditional methods.

However, AI cannot replace accountants, auditors or internal controls. Its effectiveness depends on data quality, proper implementation, continuous monitoring and human oversight. Issues such as privacy, bias, cybersecurity and accountability must also be addressed.

Therefore, effective fraud management should combine AI, human expertise and strong internal controls. AI can identify potential risks, while accountants and auditors investigate them and apply professional judgment.

The future of fraud detection is likely to focus on human-AI collaboration, enabling organizations to detect fraud earlier and improve the reliability of financial information

References

1. Association of Certified Fraud Examiners (ACFE). (2024). *Occupational Fraud 2024: A Report to the Nations*. ACFE.
2. Association of Certified Fraud Examiners (ACFE). (2024). *First Look at Occupational Fraud 2024: A Report to the Nations*. Fraud Magazine.
3. National Institute of Standards and Technology (NIST). (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. U.S. Department of Commerce.
4. National Institute of Standards and Technology (NIST). (2024). *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*. U.S. Department of Commerce.
5. National Institute of Standards and Technology (NIST). (2026). *AI Risk Management Framework Playbook*. U.S. Department of Commerce.
6. Association of Certified Fraud Examiners. *Report to the Nations Archive*.