



# INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

## ROLE OF ARTIFICIAL INTELLIGENCE IN DETECTING FINANCIAL FRAUD

**Dr. Muthaher Unnisa**

**Associate Professor**

**Department of Commerce**

**Government First Grade College Chikkaballapur**

### Abstract

Financial fraud has existed for as long as financial transactions themselves, but the way fraud is committed has changed significantly with digitalisation. Online banking, digital payments, mobile applications and technology-driven financial services have made transactions faster and more convenient, while also creating new opportunities for fraudulent activities. Traditional fraud-detection methods often depend on predefined rules, manual verification and investigation after suspicious activity has already occurred. These approaches remain important, but they may struggle to deal with the speed and volume of modern financial transactions.

Artificial Intelligence (AI) is increasingly being used to strengthen fraud detection by analysing large volumes of data, identifying unusual patterns and assessing suspicious transactions in near real time. Machine learning, predictive analytics, natural language processing and behavioural analytics can help financial institutions recognise patterns that may otherwise remain unnoticed. However, AI is not a complete replacement for human judgement. Concerns relating to data privacy, false alerts, algorithmic bias, transparency and the increasing use of AI by fraudsters themselves remain important.

This article examines the role of Artificial Intelligence in detecting financial fraud, discusses its major applications and advantages, identifies the challenges associated with its adoption and highlights the need for a balanced combination of technology, internal controls and human expertise.

**Keywords:** Artificial Intelligence, Financial Fraud, Fraud Detection, Machine Learning, Banking, Financial Technology, Data Analytics

### Introduction

Technology has changed the way people handle money. A customer can now transfer funds, invest, borrow money or make purchases within seconds using a mobile phone. Businesses also process thousands or even millions of transactions electronically every day. While this digital transformation has improved convenience and efficiency, it has also changed the nature of financial fraud.

Fraudsters no longer need to rely only on forged documents or physical theft. Financial crimes today can involve identity theft, phishing, account takeovers, payment fraud, money laundering, fraudulent loan applications, manipulation of financial information and the use of mule accounts to move illegally obtained funds.

One of the difficulties with financial fraud is that fraudulent transactions are often designed to look like genuine ones. A transaction may appear normal when viewed individually but become suspicious when compared with a customer's usual behaviour or with thousands of similar transactions.

This is where Artificial Intelligence can make a difference. Rather than examining every transaction manually, AI systems can analyse enormous amounts of financial data within a short period and identify transactions that deserve further investigation.

Artificial Intelligence should therefore not be viewed simply as another technology used by banks. It is gradually becoming part of the broader fraud-risk-management system.

### **Statement of the Problem**

Financial fraud has become a serious concern for banks, financial institutions, businesses and individuals due to the rapid growth of digital transactions. Traditional fraud-detection methods generally depend on manual verification, predefined rules and periodic monitoring. Although these methods are still useful, they may not always be sufficient to identify sophisticated fraud that occurs through rapidly changing digital channels.

Fraudsters are increasingly using advanced technologies, fake identities, phishing techniques, manipulated documents and complex transaction patterns to avoid detection. At the same time, financial institutions process enormous volumes of transactions every day, making it difficult for human investigators to examine each transaction individually.

Artificial Intelligence has emerged as an important tool that can analyse large volumes of financial data, identify unusual behaviour and detect suspicious patterns within a short period of time. Technologies such as machine learning, predictive analytics, behavioural analysis and natural language processing can support organisations in identifying possible fraud more effectively.

However, the use of AI also creates challenges such as data privacy concerns, false alerts, lack of transparency, high implementation costs and dependence on accurate data. Therefore, there is a need to understand how Artificial Intelligence contributes to financial fraud detection, its effectiveness, its limitations and the extent to which it can support traditional fraud-prevention methods.

The present study attempts to examine the role of Artificial Intelligence in detecting financial fraud and understand its growing importance in modern financial systems.

### **Objectives of the Study**

The major objectives of this study are:

1. To understand the role of Artificial Intelligence in detecting financial fraud.
2. To examine the major AI-based techniques used for fraud detection.
3. To identify the benefits of AI in preventing and detecting fraudulent financial activities.
4. To analyse the challenges associated with the adoption of AI-based fraud-detection systems.
5. To understand the growing relevance of AI in the Indian financial sector.
6. To suggest measures for improving the effectiveness and responsible use of AI in fraud management.

## Research Methodology

The present study follows a **descriptive and conceptual research design**.

The study is based mainly on **secondary data** obtained from published reports, regulatory publications, research literature and information issued by organisations concerned with financial fraud and financial-sector technology.

The research does not focus on a particular organisation or group of respondents. Instead, it examines existing knowledge, reports and studies related to the application of AI in fraud detection.

## Sources of Data

The study is based entirely on **secondary data**.

Information has been collected from sources such as:

- Research journals and academic articles
- Reports published by financial and professional organisations
- Publications of the Reserve Bank of India
- Publications of the Securities and Exchange Board of India
- Reports of the Association of Certified Fraud Examiners
- Books, websites and other reliable publications relating to Artificial Intelligence and fraud management

## Scope of the Study

The study mainly focuses on the application of Artificial Intelligence in detecting financial fraud in banking, digital payments and other financial activities.

It covers:

- AI-based transaction monitoring
- Machine learning in fraud detection
- Behavioural analytics
- Detection of unusual transaction patterns
- Identification of mule accounts
- Predictive fraud detection
- Challenges in AI adoption
- Importance of human judgement along with AI

The study does not evaluate the technical performance of any particular AI software or algorithm.

## Review of Literature

Several researchers and professional organisations have studied the growing role of Artificial Intelligence and data analytics in fraud prevention and detection.

**Bolton and Hand (2002)** examined statistical methods used for fraud detection and explained that unusual patterns in financial transactions can be identified by comparing current behaviour with past behaviour. Their study highlighted the importance of analytical techniques in identifying abnormal financial activities.

**Ngai et al. (2011)** reviewed the use of data-mining techniques in financial fraud detection. The study identified classification, clustering, regression and prediction as important techniques used in detecting fraudulent activities. The researchers concluded that data-driven methods could improve the efficiency of fraud identification.

**West and Bhattacharya (2016)** studied intelligent financial fraud-detection systems and observed that machine-learning techniques can improve the accuracy of fraud detection. The study also highlighted that combining different analytical methods can provide better results than depending on a single technique.

**Abdallah, Maarof and Zainal (2016)** examined various fraud-detection approaches and noted that financial fraud continues to evolve along with technology. Their research indicated that traditional fraud-detection systems may struggle to identify new fraud patterns and emphasised the need for adaptive analytical models.

**Ryman-Tubb, Krause and Garn (2018)** examined machine-learning methods used in credit-card fraud detection. Their work highlighted the potential of advanced analytical models in identifying fraudulent transactions while also noting challenges relating to highly imbalanced transaction data.

### Limitations of the Study

The present study has the following limitations:

1. The study is based mainly on **secondary data** collected from journals, reports, regulatory publications and other available sources. Therefore, the findings depend on the accuracy and reliability of the existing information.
2. The study does not include **primary data collection** from banks, financial institutions, fraud investigators or customers.
3. Artificial Intelligence is a rapidly developing technology. Hence, the tools, techniques and fraud-detection methods discussed in the study may continue to change over time.
4. The study provides a **general overview** of the role of AI in financial fraud detection and does not examine the performance of any specific AI software or algorithm.
5. The research does not focus on a particular bank, company or financial institution, which limits the possibility of making organisation-specific conclusions.
6. Access to confidential information relating to actual fraud cases and internal fraud-detection systems is limited because financial institutions generally do not disclose such sensitive information publicly.
7. The study does not provide a detailed technical evaluation of machine-learning models, coding methods or algorithmic accuracy

### Role of Artificial Intelligence in Financial Fraud Detection

#### Real-Time Transaction Monitoring

One of the most important advantages of AI is its ability to analyse transactions almost immediately.

Consider a customer who normally uses a bank account for relatively small transactions in Bengaluru. If the account suddenly records several high-value transactions from unfamiliar locations within a short period, an AI-based system can compare this activity with the customer's historical behaviour and assign the transactions a higher level of risk.

The institution can then request additional authentication, temporarily hold the transaction or send the case for investigation.

AI therefore helps organisations move from simply investigating fraud after it occurs towards identifying suspicious activity while it is happening.

## Pattern Recognition

Financial transactions generate enormous amounts of data. Within this data, fraudulent activities may leave patterns.

Machine-learning algorithms can analyse previous examples of legitimate and fraudulent transactions and identify relationships between variables such as:

- Transaction value
- Transaction frequency
- Geographic location
- Device information
- Login behaviour
- Time of transaction
- Merchant category
- Payment history
- Changes in customer behaviour

The system can then use these relationships to estimate whether a new transaction resembles previously identified fraudulent behaviour.

## Detection of Unusual Behaviour

AI is particularly useful when fraud does not match an already-known pattern.

For example, an employee may approve transactions that individually fall within authorised limits but repeatedly sends payments to the same newly created vendor. A traditional system examining only transaction limits might not identify a problem.

An AI system analysing relationships between employees, vendors, approval timings and transaction behaviour may identify the unusual pattern and generate an alert.

This ability to identify anomalies can help uncover sophisticated fraud that may otherwise remain hidden.

## Behavioural Analytics

People generally develop patterns in the way they use financial services. They may log in from similar devices, carry out transactions within certain value ranges and interact with applications in relatively consistent ways.

AI-powered behavioural analytics can create a profile of normal customer activity.

When behaviour suddenly differs from that profile, the system can investigate further. Behavioural signals can include typing patterns, device use, login location and transaction behaviour.

This approach can be particularly useful in detecting stolen credentials and account takeovers.

## Identification of Mule Accounts

Mule accounts are bank accounts used to receive and transfer funds generated through fraudulent activities. They can make it difficult to trace money back to the original fraudster.

In India, the Reserve Bank Innovation Hub developed **MuleHunter.ai**, an AI/ML-based system designed to identify suspected mule bank accounts. RBI has stated that the model uses machine-learning techniques for near-real-time identification of mule accounts and has been tested and deployed in some large public-sector banks.

This is a practical example of how AI can move beyond theoretical applications and become part of the financial system's defence against digital fraud.

### **Natural Language Processing**

Not all financial information exists as numbers. Fraud investigations can also involve emails, complaints, transaction descriptions, documents and communication between employees or customers.

Natural Language Processing (NLP), a branch of AI concerned with understanding human language, can assist in analysing large amounts of textual information.

This does not necessarily prove fraud, but it can help investigators identify cases that require closer attention.

### **Artificial Intelligence and Fraud Detection in India**

India provides an important environment for AI-based fraud detection because of the rapid growth of digital financial services.

The Reserve Bank of India has recognised AI and machine learning as technologies that can support fraud detection, transaction monitoring and financial-sector supervision. RBI has also highlighted the importance of responsible AI, including concerns surrounding privacy, transparency, accountability and explainability.

Similarly, SEBI is increasingly incorporating AI into securities-market surveillance.

In 2026, SEBI described AI-powered tools including **SEBI Sudarshan**, which is used to identify fraudsters posing as registered investment advisers or research analysts on social media, and **R(AI)DAR**, which analyses advertisements for possible regulatory violations. SEBI has also discussed AI-supported analysis of corporate announcements and cyber-risk information.

These initiatives demonstrate that AI is becoming relevant not only for private banks and financial companies but also for regulators responsible for maintaining the integrity of financial markets.

### **Benefits of Artificial Intelligence in Fraud Detection**

#### **Faster Detection**

AI can process large amounts of data considerably faster than manual investigation, allowing suspicious transactions to be identified quickly.

#### **Continuous Monitoring**

Unlike manual reviews conducted periodically, automated systems can continuously monitor financial activity.

#### **Ability to Handle Large Data Volumes**

Modern financial institutions process enormous numbers of transactions. AI makes it possible to analyse data at a scale that would be extremely difficult through human effort alone.

#### **Identification of Hidden Relationships**

AI can connect information across customers, devices, transactions, accounts and locations, helping investigators identify relationships that may not be immediately visible.

## Improved Prioritisation

Risk-scoring systems can help fraud investigators focus their time on cases with the greatest likelihood of suspicious activity.

## Learning Capability

Machine-learning systems can be retrained using new fraud cases and updated data, allowing detection models to adapt as fraud patterns change.

## Findings of the Study

Based on the review of secondary information, the study identifies the following major observations:

1. Artificial Intelligence is increasingly becoming an important tool in financial fraud detection.
2. Machine learning enables institutions to analyse historical transactions and recognise patterns associated with fraudulent activity.
3. AI allows suspicious transactions to be identified much faster than traditional manual approaches.
4. Behavioural analytics and anomaly detection can identify fraud even when transactions do not match predefined fraud rules.
5. AI can improve the detection of complex activities such as mule accounts, identity fraud, account takeover and unusual transaction networks.
6. Indian financial regulators are increasingly exploring and implementing AI-enabled supervisory and fraud-detection technologies.

## Suggestions

- **Combine AI with human expertise:** AI-generated fraud alerts should be supported by experienced investigators rather than relying entirely on automated decisions.
- **Regularly update fraud models:** Fraud patterns change continuously. AI models should therefore be reviewed and retrained using current information.
- **Improve data quality:** Financial institutions should establish strong data-management practices to ensure that the information used by AI systems is accurate and reliable.
- **Strengthen privacy and security:** Customer information used for fraud monitoring must be appropriately protected.
- **Improve explainability:** Organisations should prefer systems that allow investigators to understand why a transaction has been considered suspicious.
- **Develop employee skills:** Accountants, auditors, bankers and fraud investigators should be trained to understand AI-based tools and interpret their outputs.
- **Combine technology with internal controls:** AI should complement controls such as segregation of duties, authorisation procedures, reconciliations, audits and whistle-blower mechanisms.
- **Promote responsible AI:** Regulators and financial institutions should develop clear standards relating to transparency, accountability, privacy and ethical use of AI.
- **Increase customer awareness:** Since many digital frauds depend on social engineering rather than weaknesses in financial systems, customers should also be educated about phishing, impersonation and AI-generated scams.

## Conclusion

Financial fraud has become more sophisticated as financial services have become more digital. Traditional fraud controls continue to play an important role, but they cannot always analyse the speed, scale and complexity of modern financial activity on their own.

Artificial Intelligence offers an important opportunity to strengthen fraud detection. Through machine learning, anomaly detection, behavioural analysis, predictive analytics and natural

language processing, AI can identify suspicious patterns that may be difficult for humans to recognise manually.

At the same time, AI should not be seen as a magical solution to fraud. Its effectiveness depends on good-quality data, appropriate controls, trained professionals and responsible governance. There will also always be situations in which technology identifies an unusual pattern but human judgement is required to understand the reason behind it.

The future of financial fraud detection will therefore depend on cooperation between **technology and people**. AI can provide speed, scale and analytical capability, while human professionals provide judgement, experience and accountability.

As financial transactions continue to evolve, organisations that successfully combine these strengths will be better placed not only to detect fraud after it occurs but also to recognise warning signs earlier and prevent financial losses before they become significant.

## References

1. Association of Certified Fraud Examiners. (2024). *Occupational Fraud 2024: A Report to the Nations*. Association of Certified Fraud Examiners.
2. Association of Certified Fraud Examiners & SAS. (2024). *Anti-Fraud Technology Benchmarking Report*. ACFE and SAS.
3. Association of Certified Fraud Examiners. (2026). *Anti-Fraud Technology Benchmarking Report: Key Findings*. ACFE.
4. Reserve Bank of India. (2025). *Annual Report 2024–25*. Reserve Bank of India.
5. Reserve Bank of India. *Artificial Intelligence and Machine Learning in Financial Services*. RBI Bulletin.
6. Securities and Exchange Board of India. (2026). Publications and regulatory communications on responsible use of Artificial Intelligence and technology-driven market surveillance.
7. Securities and Exchange Board of India. (2026). *Master Circular on Surveillance of Securities Market*. SEBI.