Machine Learning for Financial Fraud Detection

Muhammad Sarfraz Arshad, FCMA
Chief Financial Officer
Craft Industrial Co., Saudi Arabia

History shows that financial fraud remains a significant and growing problem in today's world, causing billions of dollars in losses for businesses, governments, and individuals every year. The complicated structure of modern financial systems, combined with increasingly sophisticated fraud tactics, means that traditional methods of detecting fraud through simple rules are no longer enough and require out-of-the-box solutions to detect financial fraud and enable remedial actions.

Machine Learning (ML) stands out as a revolutionary approach, offering the capability to identify concealed patterns, adapt to emerging fraud techniques, and provide immediate analysis. This discussion examines how ML is utilized in financial fraud detection, emphasizing important methodologies, obstacles, and the future of advanced fraud prevention systems.

Machine learning functions as a very powerful method for addressing monetary fraud in recent times. Its capability to process huge volumes of data and recognize complex patterns provides significant advantages over traditional rule-based approaches.

Machine learning in finance is a type of artificial intelligence (AI) that has recently gained popularity. It allows computing algorithms to work with vast amounts of data efficiently and at low cost. *(Source: https://unthinkable.fm/how-does-machine-learning-guide-in-finance/)*

How Machine Learning Contributes to Reducing Financial Fraud

(1) Detecting Patterns and Unusual Activity

Conventional fraud detection relies on fixed rules, including "alert for transactions exceeding $1,000" or "prevent purchases from international locations." However, criminals continuously modify their approaches. Machine learning addresses this constraint through:

a) **Unusual Activity Detection:** ML systems learn from extensive historical data to establish typical behavior patterns for individuals or organizations. This encompasses purchasing behaviors, transaction locations, timing, and purchase categories. When transactions significantly differ from established patterns—such as a minor purchase in one location immediately followed by a major purchase across the globe— the system identifies it as questionable. This represents unsupervised learning, where models detect irregular patterns without pre-categorized information.

b) **Pattern Identification:** ML systems can discover very subtle and complex relationships that remain hidden from human observation. They can identify fraudulent account networks by examining connections between various entities, including shared contact information, IP addresses, or telephone numbers. This approach is referred to as network or graph analysis.

(2) Immediate Processing and Action

The rapid pace of financial transactions demands fraud detection systems capable of real-time operation. ML models can evaluate hundreds of thousands of transactions within milliseconds, assigning risk ratings to each. This enables financial organizations to:

a) **Prompt Transaction Obstructing/Blocking:** When transactions receive elevated financial risk ratings, the systems can automatically prevent completion before fraudulent activities occur. This blocks the transaction in real time and prevents losses of billions of dollars.

b) **Request Additional Authentication:** For moderately risky transactions, systems can initiate additional verification requests, including one-time codes or confirmation messages to cardholders.

(3) Continuous Learning for Changing Threats

Fraudulent methods constantly evolve. ML models are capable of continuously learning and adjusting to new schemes by automatically processing fresh data. This represents a significant benefit over static rule-based systems requiring manual modifications. Through reinforcement or adaptive learning processes, ML models can modify their algorithms for improved effectiveness over time, even against previously unknown threats.

(4) Minimized Incorrect Alerts

It is generally observed that traditional fraud detection methods face the most significant challenges with "incorrect alerts," where legitimate transactions are mistakenly identified as fraudulent. This creates frustrating customer experiences and business losses. Machine learning addresses this through:

a) **Enhanced Precision:** By examining broader ranges of characteristics and behavioral data, ML models better differentiate between genuinely suspicious transactions and unusual but legitimate activities (such as vacation purchases in new locations).

b) **Risk Assessment:** Rather than simple "fraud/legitimate" classifications, ML models typically provide risk ratings. This allows financial institutions to make more sophisticated decisions and focus resources on investigating the highest-risk transactions.

(5) Diverse Financial Service Applications

Machine learning is applied across a wide range of financial fraud scenarios:

- **Credit Card Fraud:** ML examines transaction details such as amount, location, merchant, and timing to promptly identify and flag suspicious activities, preventing unauthorized usage or withdrawals.
- **Financial Statements:** ML can code accounting entries, enhancing the accuracy of rules-based approaches and enabling greater automation, while predictive models can also forecast revenues.
- **Account Security:** ML monitors user access patterns to detect unusual activities, such as repeated failed login attempts or access from unfamiliar devices or locations.
- **Documentation and Internal Fraud:** ML analyzes invoices and related documents for inconsistencies, including duplicate billing or questionable vendor information.
- **Insurance Fraud:** ML identifies fraudulent claims, billing irregularities, and excessive service utilization.

Standard Machine Learning Methods in Fraud Detection

Various algorithms support fraud detection and are typically divided into supervised, unsupervised, and reinforcement learning approaches.

1) Supervised Learning

Supervised learning uses categorized data (transactions already classified as fraudulent or legitimate) to train models for classifying new transactions. Common algorithms include:

- **Logistic Regression:** A straightforward yet effective classification method for binary outcomes (fraud/legitimate).
- **Decision Trees and Random Forests:** These create rule sets for data classification, often providing clear interpretations.
- **Support Vector Machines (SVM):** This method identifies optimal boundaries separating fraudulent from legitimate transactions.

2) Unsupervised Learning

Unsupervised learning detects irregularities in uncategorized data, making it effective for identifying new fraud types.

3) Reinforcement Learning

Reinforcement learning can be used when there isn't a lot of training data available, the ideal end state cannot be clearly defined, or the only way to learn about the environment is to interact with it.

A. Primary Machine Learning Methods

Method	Purpose
Decision Trees & Random Forests	Transaction type classification
Logistic Regression	Binary fraud/legitimate classification
Neural Networks	Complex fraud pattern recognition
K-Means Clustering	Grouping similar behaviors to identify outliers
Autoencoders	Input reconstruction to detect unusual variations

B. Data-Related Obstacles in Fraud Detection

Several data challenges complicate ML fraud detection:

- **Class imbalance:** Fraudulent cases occur less frequently than legitimate ones.
- **Data privacy:** Sharing financial information for model development creates legal issues.
- **Feature development:** Extracting valuable features from raw data is essential.
- **Classification difficulties:** Accurate and proper data labeling can be lengthy and prone to errors/mistakes.

C. Real-World Examples and Industry Uses

Multiple organizations have successfully implemented ML for fraud detection:

- **PayPal:** Utilizes deep learning and combined methods to identify suspicious transactions.
- **Mastercard:** Applies decision intelligence for monitoring billions of transactions.
- **Banks and FinTechs:** Employ ML for immediate AML screening, transaction monitoring, and customer verification.

About the Author: *The writer is a Fellow member of ICMA and an ACCA member with over 22 years of experience in public and private sectors, including a tenure as acting CEO in a public sector company. He is currently CFO at Craft Industrial Co., Saudi Arabia. His expertise spans strategic financial planning, regulatory compliance, business development, and international financial reporting. He also mentors emerging professionals and serves as an ACCA IPSAS Trainer and Corporate Trainer at the Pakistan Audit & Accounts Academy.*