Serhii Haidenko
Candidate of Economic Sciences, Docent,
Associate Professor at the Department of Entrepreneurship
and Business Administration
O.M. Beketov National University of Urban Economy in Kharkiv

Гайденко С.М.
кандидат економічних наук, доцент,
доцент кафедри підприємництва та бізнес-адміністрування
Харківського національного університету міського господарства
імені О. М. Бекетова

DOI: https://doi.org/10.30525/978-9934-26-639-3-9

MANAGEMENT OF THE FINANCIAL RISK MODELING PROCESS AND DETECTION OF FRAUDULENT TRANSACTIONS USING DATA ANALYSIS

УПРАВЛІННЯ ПРОЦЕСОМ МОДЕЛЮВАННЯ ФІНАНСОВИХ РИЗИКІВ ТА ВИЯВЛЕННЯ ШАХРАЙСЬКИХ ОПЕРАЦІЙ ЗА ДОПОМОГОЮ АНАЛІЗУ ДАНИХ

The modern financial sector faces an unprecedented level of threats, with global losses from fraud and banking schemes exceeding hundreds of billions of dollars annually. This situation is exacerbated by rapid digitalization, the use of generative AI by fraudsters to create deepfakes and complex synthetic identity schemes, which account for over 80% of all identity fraud [5]. Traditional systems based on static rules are ineffective, as they react to incidents after the fact and generate a large number of false positives that overload operational departments [2]. In this environment, financial risk management and fraud detection are undergoing a paradigm shift – from a reactive to a proactive and predictive approach, based on advanced data analytics, machine learning and real-time behavioral analysis.

At the heart of modern systems is predictive analytics, which uses business statistical algorithms, machine learning, and data mining to analyze historical data to predict future events. This approach allows you to go beyond thresholds and detect subtle patterns that indicate fraud. The key is to move from after-the-fact detection to real-time intervention that prevents fraudulent transactions from being completed [1].

Machine learning's adaptability is crucial to combat fraudsters who are constantly changing their tactics. Algorithms continuously learn from new data, improving their accuracy and ability to detect new, previously unknown fraud schemes [1]. Instead of rigid rules, systems create a dynamic "norm" for each customer.

The effectiveness of the risk modeling system is assessed by the following key indicators:

– accuracy and recall: the ability to correctly identify the maximum number of fraudulent transactions;

– false positive rate: reducing this indicator directly improves the customer experience and reduces operational burden;

– financial losses from fraud: the ultimate performance indicator;

– detection speed: the time between the initiation of a suspicious transaction and its detection.

So, it is necessary to dwell on modern technologies and methods of analytics:

1) advanced behavioral biometrics and device analytics: authentication is evolving from passwords and devices to behavioral analysis; passive continuous authentication analyzes the rhythm of typing, mouse movements, gestures on touch screens, creating an individual behavioral profile that is difficult to fake; this allows you to detect attackers even with valid credentials, without creating additional "friction" for the client; device analytics creates a unique "fingerprint" of the device based on hardware and software attributes, which allows you to track it even when the IP address changes or cookies are deleted [2].

2) Network graphs for detecting organized fraud: one of the most powerful tools for combating complex, coordinated schemes, this technology maps connections between accounts, devices, transactions and individuals, revealing hidden patterns that are invisible when analyzing individual events [2]; community detection algorithms group related entities, which allows the detection of entire criminal networks, such as money laundering "mules" networks or coordinated attacks on account creation [5].

3) AML and fraud consolidation: the trend towards combining fraud detection and AML functions into a single platform; these systems centralize data, eliminate gaps between departments and allow the detection of more complex risk patterns. This not only increases efficiency, but also significantly reduces operational costs and simplifies regulatory compliance [2].

We emphasize that for a detailed comparison of AI-methods for fraud detection, it is worth using table 1.

Managing the process of modeling financial risks and detecting fraudulent transactions includes four key stages [1]:

I) data integration: collecting, cleaning and combining data from various sources (transaction systems, customer profiles, device telemetry, external threat sources) into a single analytical repository;

II) model development: creating algorithms specific to the business using selected machine learning methods, training them and testing them on historical data (data from past periods);

III) continuous monitoring: implementing real-time systems for analyzing transactions and constantly updating models to adapt to new fraudster tactics;

IV) feedback: creating a loop where the results of the investigation (real fraud / false positives) are used to refine and improve the models.

Table 1

Comparison of AI methods for fraud detection

Method / Algorithm	Best suited for	Key benefits	Limitations
gradient boosting (XGBoost, LightGBM)	structured tabular data (transactions)	high accuracy, speed, ability to work with different types of features	limited interpretability, may be prone to overtraining
deep learning (autoencoders, LSTM)	sequential data, behavioral anomalies, image processing (document verification)	ability to detect complex nonlinear patterns, efficient for sequence analysis	high complexity, need for large amounts of data, “black box”
graph network algorithms	detection of coordinated network attacks, analysis of connections	ability to detect complex collusions invisible to other methods	complexity of real-time integration, need for specialized data
adaptive isolation forests	fast anomaly detection in real-time data streams	efficient with small samples, speed	less efficient for detecting complex multidimensional patterns

It should also be noted that effective detection in the context of high-speed payments requires an architecture capable of making decisions in the sub-millisecond range [2], which can be achieved by using [5]:

– streaming data processors: Apache Kafka for integration and Apache Flink or Spark Structured Streaming for real-time analysis;

– in-memory computing: using Hazelcast or Redis to store data and models, providing instant access;

– microservice architecture: microservice-based APIs provide seamless integration with core banking systems without slowing down the transaction flow.

Implementing advanced analytics requires a robust data governance framework. This includes privacy controls such as encryption, pseudonymization, differential privacy protection, and federated learning, which allows data to be analyzed without sensitive information being exposed [5]. Clear data traceability is essential for auditing and compliance with regulations such as GDPR and PCI DSS [4].

Financial risk management and fraud detection using data analytics is thus transformed from a support function into a strategic asset that provides competitive advantage. Key areas of development will be [2]:

– hyper-personalization: creating dynamic risk profiles for each individual customer, not a segment;

– collaborative intelligence: participating in industry consortia to exchange anonymized threat signals in real time, as no institution can fight fraud alone;

– combating AI threats: developing methods for detecting attacks using generative AI, such as deep forgery detection and advanced pixel-level document validation;

– further automation: implementing AI-assisted investigation management systems that will automate routines, distribute alerts, and suggest next steps.

Refrerences:

1. Fraud Analytics: Identifying and Reducing Fraud Risks in 2025. Available at: https://www.getfocal.ai/blog/fraud-analytics (date of application: 20.10.2025).

2. Fraud Detection in Banking: 2025 Future Trends & Predictions. Available at: https://trustdecision.com/resources/blog/fraud-detection-in-banking-2025-future-trends-predictions (date of application: 20.10.2025).

3. Global economic outlook report McKinsey. Available at: https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/economic-conditions-outlook#/ (date of application: 20.10.2025).

4. How to Use Predictive Analytics for Risk Management & Fraud Detection. Available at: https://digitaldefynd.com/IQ/the-use-of-predictive-analytics-for-risk-management-and-fraud-detection/ (date of application: 20.10.2025).

5. Leveraging Data Analytics for Risk Management and Fraud Detection in Financial Services. Available at: https://www.matellio.com/blog/data-analytics-risk-management-fraud-detection/ (date of application: 20.10.2025).