



RADemics

# Machine Learning for Banking Risk, Fraud Detection, and Transaction Intelligence



A.Kiruthika, B. Seenivasan

Velalar College of Engineering and Technology,  
Sacred Heart College

# Machine Learning for Banking Risk, Fraud Detection, and Transaction Intelligence

<sup>1</sup>A.Kiruthika, Assistant Professor, Department of CSE (Artificial Intelligence and Machine Learning), Velalar College of Engineering and Technology, Erode, Tamil Nadu, India. [kiruthikavcet13@gmail.com](mailto:kiruthikavcet13@gmail.com)

<sup>2</sup>B. Seenivasan, Assistant Professor and Head, Department of Commerce (Banking and Finance), Sacred Heart College, Tirupattur, Tamil Nadu, India. [seejet80@gmail.com](mailto:seejet80@gmail.com)

## Abstract

Rapid digital transformation across global banking ecosystems has intensified exposure to credit risk, systemic instability, cyber-enabled fraud, and complex financial crime networks. Escalating transaction volumes, real-time payment infrastructures, and interconnected financial platforms demand intelligent analytical frameworks capable of detecting nonlinear patterns, behavioral deviations, and network-driven risk propagation. Machine learning has emerged as a transformative enabler for modern banking analytics, offering advanced predictive modeling, anomaly detection, and adaptive decision intelligence beyond traditional rule-based systems.

This chapter presents a comprehensive and integrated perspective on machine learning applications for banking risk management, fraud detection, anti-money laundering, and transaction intelligence. Advanced methodologies including ensemble learning, deep neural architectures, graph neural networks, and streaming analytics frameworks are examined in the context of credit risk estimation, systemic early warning systems, real-time transaction risk scoring, and network-based financial crime detection. Emphasis is placed on feature engineering strategies, temporal and relational modeling, and scalable deployment architectures designed for high-velocity financial data environments.

Regulatory compliance and governance considerations receive focused attention through the integration of explainable artificial intelligence techniques, fairness auditing mechanisms, and model risk management frameworks aligned with prudential standards. The chapter further addresses challenges related to class imbalance, concept drift, adversarial adaptation, and cross-institution intelligence sharing through privacy-preserving learning paradigms. By synthesizing predictive accuracy, interpretability, and operational resilience, the proposed analytical foundations contribute toward the development of secure, transparent, and adaptive banking intelligence systems suitable for regulated financial ecosystems.

Keywords: Machine Learning, Credit Risk Modeling, Fraud Detection, Graph Neural Networks, Explainable AI, Transaction Intelligence

## Introduction

Digital transformation within the global banking sector has redefined financial intermediation, risk exposure, and transactional complexity [1]. Expansion of online banking platforms, mobile

payment ecosystems, real-time gross settlement systems, and cross-border digital finance channels has generated unprecedented volumes of structured and unstructured financial data [2]. Transaction streams now flow continuously across interconnected institutions, creating intricate dependencies among customers, counterparties, markets, and payment infrastructures. This transformation enhances operational efficiency and financial inclusion, yet simultaneously amplifies vulnerabilities related to credit defaults, liquidity disruptions, cyber intrusions, identity fraud, and coordinated financial crime [3]. Traditional statistical risk assessment models and rule-based monitoring systems, originally designed for periodic reporting environments, struggle to capture nonlinear interactions, high-dimensional dependencies, and rapidly evolving behavioral patterns embedded within modern transaction ecosystems. As adversarial actors employ increasingly sophisticated techniques such as synthetic identities, mule networks, and algorithmic laundering strategies, financial institutions require adaptive intelligence systems capable of identifying subtle anomalies in real time [4]. The growing convergence of financial technology, regulatory oversight, and data science has therefore positioned machine learning at the center of contemporary banking analytics. Advanced computational models now serve not only as predictive instruments but also as strategic infrastructure supporting resilience, transparency, and competitive advantage in highly regulated financial markets [5].

Machine learning methodologies provide the analytical foundation necessary to process large-scale financial datasets characterized by heterogeneity, velocity, and structural interdependence [6]. Supervised learning frameworks enhance credit risk estimation through nonlinear modeling of borrower characteristics, transactional histories, and macroeconomic indicators, enabling refined probability of default and loss forecasting [7]. Unsupervised and semi-supervised techniques facilitate anomaly detection within massive transaction streams, uncovering irregular patterns that escape deterministic rule thresholds. Deep learning architectures capture complex temporal sequences and high-order feature interactions, strengthening predictive discrimination in volatile financial conditions [8]. Beyond tabular representations, graph-based learning approaches incorporate relational intelligence derived from account linkages, shared devices, transaction chains, and ownership structures, offering powerful tools for identifying coordinated fraud rings and systemic contagion channels [9]. Integration of streaming analytics platforms with optimized inference engines enables instantaneous risk evaluation during payment authorization processes, reducing latency between anomaly detection and intervention. Such computational capabilities mark a decisive shift from reactive post-event investigation toward proactive and continuous financial surveillance, reinforcing operational stability in dynamic digital economies [10].