RADemics

ML-Based Anomaly Detection in Payment Gateways, Digital Wallets, and Online Banking

S. Praveena, Neeti Misra
MAHATMA GANDHI INSTITUTE OF TECHNOLOGY (MGIT), SCHOOL OF BUSINESS UPES

ML-Based Anomaly Detection in Payment Gateways, Digital Wallets, and Online Banking

[1]S. Praveena, Associate Professor Department of ECE, Mahatma Gandhi Institute of Technology (MGIT), Hyderabad, India. spraveena_ece@mait.ac.in

[2]Neeti Misra, Assistant Professor, School of Business, UPES, Dehradun, Uttarakhand, India. neeti.cm@gmail.com

Abstract

The proliferation of digital financial platforms, including payment gateways, digital wallets, and online banking systems, has introduced significant efficiencies in financial transactions while simultaneously escalating the risk of sophisticated fraudulent activities. Traditional security mechanisms, such as rule-based systems and threshold monitoring, are increasingly inadequate in addressing high-frequency, evolving fraud patterns. Machine learning (ML) techniques have emerged as robust solutions for anomaly detection, capable of analyzing high-dimensional, heterogeneous, and real-time transactional data to identify suspicious behaviors effectively. By leveraging supervised, unsupervised, and semi-supervised approaches, ML models capture complex, nonlinear relationships among transaction features, enhancing detection accuracy and enabling proactive intervention in dynamic financial environments. Feature engineering and representation learning further strengthen model performance by processing behavioral patterns, device identifiers, geolocation signals, and transactional sequences. Real-time deployment frameworks, supported by adaptive algorithms and streaming analytics, ensure low-latency anomaly detection, facilitating timely alerts and minimizing financial losses. The integration of explainable AI (XAI) enhances interpretability, allowing institutions to justify automated decisions, comply with regulatory requirements, and maintain stakeholder trust, while ethical considerations, including privacy preservation, fairness, and accountability, ensure transparent and equitable system operation. Empirical studies demonstrate the practical application of ML-based systems in high-volume financial ecosystems, highlighting improved detection rates, operational efficiency, and risk management compared to conventional approaches. By addressing challenges such as imbalanced datasets, evolving fraud strategies, and regulatory compliance, ML-based anomaly detection frameworks offer scalable, adaptive, and responsible solutions. These systems represent a transformative approach to securing financial transactions, combining advanced algorithms, real-time processing, explainability, and ethical governance to achieve robust and accountable fraud prevention in complex digital financial landscapes.

Keywords: Machine Learning, Anomaly Detection, Digital Payments, Real-Time Fraud Detection, Explainable AI, Financial Security

Introduction

The rapid digitalization of financial services has fundamentally transformed how transactions are conducted, with payment gateways, digital wallets, and online banking platforms providing unprecedented convenience, speed, and accessibility [1]. These technologies have enabled users

to perform financial operations anytime and anywhere, fostering the expansion of global commerce and personal finance management [2]. This digital evolution has also introduced significant vulnerabilities, as cybercriminals increasingly exploit technological gaps to perpetrate fraudulent activities [3]. Financial institutions face heightened risks from sophisticated attack vectors, including account takeovers, transaction manipulation, synthetic identity fraud, and multi-channel coordinated attacks. The complexity of modern financial ecosystems, characterized by high transaction volumes, heterogeneous data streams, and diverse user behaviors, necessitates advanced approaches to detect anomalies in near real-time [4]. Traditional rule-based or threshold-monitoring mechanisms, while historically effective, are no longer sufficient to contend with these rapidly evolving threats. As a result, the integration of machine learning (ML) techniques into anomaly detection frameworks has emerged as a critical strategy for enhancing the security and resilience of digital payment systems [5].

Machine learning approaches provide a transformative solution to the challenges posed by dynamic, high-volume financial data [6]. Unlike conventional systems that rely on static rules or predefined thresholds, ML algorithms can learn complex patterns, adapt to emerging behaviors, and identify subtle deviations indicative of fraudulent activity [7]. Supervised learning models leverage historical labeled datasets to distinguish between legitimate and fraudulent transactions, employing methods such as decision trees, support vector machines, and gradient boosting for high-accuracy predictions [8]. Unsupervised approaches, including clustering, autoencoders, and isolation forests, facilitate the detection of previously unseen anomalies without explicit labeling, capturing irregularities that may elude traditional monitoring systems [9]. Semi-supervised and hybrid techniques combine the strengths of both paradigms, enabling effective identification of rare fraud instances in imbalanced datasets. ML models excel at handling high-dimensional transaction data that incorporate structured fields, behavioral metrics, device metadata, and geospatial information, providing a holistic understanding of transactional dynamics. These capabilities position ML as a pivotal enabler for proactive, data-driven fraud prevention in contemporary digital financial ecosystems [10].