RADemics

Intelligent Fraud Detection Systems for Banking, E-Commerce, and Cloud Payments

Himanshu Sahu, Suresh Kumar
Vivekananda Global University, MVN University
Palwal

Intelligent Fraud Detection Systems for Banking, E-Commerce, and Cloud Payments

[1]Himanshu Sahu, Assistant Professor, Department of Computer Science & Application, Vivekananda Global University, Jaipur, Rajasthan, India. himanshu.sahu.q7k@gmail.com

[2]Suresh Kumar, Associate Professor, Department of Law, MVN University Palwal, Haryana, India. lawsureshkr07@gmail.com

Abstract

The rapid expansion of digital banking, e-commerce platforms, and cloud-based payment infrastructures has intensified exposure to sophisticated and large-scale financial fraud. High transaction velocity, interconnected payment ecosystems, and API-driven service architectures have created complex environments in which traditional rule-based detection mechanisms fail to provide adequate protection. Intelligent Fraud Detection Systems (IFDS) have emerged as a transformative solution, integrating machine learning, deep learning, graph analytics, and real-time stream processing to detect evolving fraud patterns with greater accuracy and adaptability.This chapter presents a comprehensive examination of intelligent fraud detection frameworks across banking systems, e-commerce marketplaces, and cloud-native payment ecosystems. Advanced predictive modeling techniques, including ensemble learning, sequential deep neural networks, reinforcement learning, and graph neural networks, are analyzed for their capacity to capture temporal dependencies and relational fraud structures. Emphasis is placed on adaptive risk scoring mechanisms, real-time payment monitoring, Zero Trust security integration, and federated learning approaches that address data privacy and cross-institutional collaboration challenges.Critical issues such as class imbalance, concept drift, adversarial manipulation, regulatory compliance, and explainable artificial intelligence are examined to highlight operational and governance considerations in high-stakes financial environments. The chapter synthesizes emerging research directions and architectural best practices to establish a unified, scalable, and transparent fraud detection paradigm capable of strengthening resilience across modern digital financial systems.

Keywords: Fraud Detection, Machine Learning, Deep Learning, Graph Neural Networks, Risk Scoring, Cloud Payments.

Introduction

Digital payment systems have undergone a profound structural transformation driven by rapid advancements in Artificial Intelligence (AI), the Internet of Things (IoT), high-speed communication networks, and cloud-based financial infrastructures [1]. The global economy increasingly relies on contactless transactions, mobile wallets, biometric authentication platforms, and decentralized financial services that operate across interconnected digital ecosystems [2]. Payment terminals, wearable devices, smart ATMs, and embedded financial sensors continuously generate transactional and behavioral data streams that require real-time processing and secure

validation. Such expansion enhances convenience, operational efficiency, and financial inclusion, while simultaneously enlarging the cyber-attack surface within distributed payment architectures [3]. Sophisticated fraud schemes, identity manipulation techniques, and coordinated cyber intrusions target vulnerabilities across network layers, application interfaces, and device firmware. Traditional perimeter-based security frameworks prove inadequate in environments characterized by decentralized endpoints and continuous data exchange. Intelligent, adaptive, and context-aware protection mechanisms therefore become fundamental components of modern financial infrastructures [4]. The integration of AI-driven analytics with IoT-enabled transaction ecosystems provides a pathway toward proactive threat detection, automated risk mitigation, and dynamic authentication control. This convergence establishes the foundation for resilient digital payment networks capable of sustaining high transaction throughput while maintaining integrity, confidentiality, and regulatory compliance across heterogeneous operational environments [5].

Artificial Intelligence introduces advanced analytical capabilities that extend beyond conventional rule-based fraud detection systems [6]. Machine learning algorithms, deep neural networks, reinforcement learning models, and graph-based analytics enable dynamic evaluation of transaction patterns, user behavior, geospatial anomalies, and device fingerprinting attributes [7]. Continuous learning mechanisms facilitate adaptation to evolving fraud tactics, synthetic identity construction, and coordinated attack strategies. Predictive risk scoring models enhance transaction validation processes by balancing security enforcement with customer experience optimization [8]. Context-aware decision engines evaluate multifactor signals in milliseconds, reducing false positives and operational friction within high-volume payment ecosystems. The emergence of explainable AI techniques strengthens transparency in automated financial decisions, addressing regulatory requirements and governance standards that demand accountability in algorithmic processing [9]. Integration of AI within distributed financial infrastructures supports intelligent orchestration of authentication intensity, adaptive credit evaluation, and anti-money laundering analytics. Intelligent automation therefore transforms digital payment environments into self-monitoring systems capable of responding to dynamic financial threats while preserving transactional efficiency and consumer trust [10].