RADemics

AI-Powered Online Payment Security and Fraud Detection in Modern Finance

N. Anandha Priya, K. Boopalan
Nehru Institute of Information Technology and Management, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology

AI-Powered Online Payment Security and Fraud Detection in Modern Finance

[1]N. Anandha Priya, Assistant Professor, PG - Department of Computer Applications, Nehru Institute of Information Technology and Management, Coimbatore, Tamil Nadu, India. niitmanandhapriya@nehrucolleges.com

[2]K. Boopalan, Associate Professor, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi Chennai, India. erbookumar@gmail.com

Abstract

The exponential growth of digital payment ecosystems has transformed global financial transactions while simultaneously amplifying exposure to sophisticated cyber fraud. Conventional rule-based security frameworks struggle to address high-volume, real-time transaction streams characterized by evolving adversarial behavior, identity manipulation, and cross-platform fraud networks. Artificial Intelligence (AI) has emerged as a transformative enabler of intelligent, adaptive, and scalable payment security infrastructures. Advanced machine learning, deep learning, graph analytics, reinforcement learning, and encrypted computation techniques now support dynamic risk scoring, anomaly detection, fraud ring identification, and privacy-preserving collaborative intelligence across distributed financial systems.

This chapter critically examines the evolution of online payment security from static control mechanisms to autonomous self-learning defense architectures. Core discussions encompass explainable and ethical AI for regulatory-compliant fraud detection, privacy-preserving encrypted machine learning, adversarial robustness through game-theoretic modeling, blockchain–AI integration for secure transaction validation, and scalability considerations in high-frequency payment networks. Emerging paradigms such as federated learning, quantum-resistant cryptography, and adaptive real-time decision systems are analyzed to highlight future research trajectories in financial cybersecurity.

By synthesizing technological innovation with governance, transparency, and resilience principles, this work establishes a comprehensive framework for AI-powered fraud detection in modern finance. The chapter contributes a structured perspective that bridges algorithmic advancement, secure infrastructure design, and ethical oversight, providing a forward-looking foundation for scalable and trustworthy digital payment protection in increasingly complex financial ecosystems.

Keywords: Artificial Intelligence, Online Payment Security, Fraud Detection, Explainable AI, Blockchain Integration, Privacy-Preserving Machine Learning.

Introduction

The rapid expansion of digital payment infrastructures has fundamentally reshaped global financial ecosystems, enabling seamless cross-border transactions, instant settlements, and

platform-integrated commerce [1]. Mobile wallets, contactless cards, embedded finance solutions, and real-time payment gateways have accelerated the transition toward cashless economies across developed and emerging markets. This transformation has increased transaction velocity, diversified payment channels, and expanded access to financial services [2]. At the same time, the digitalization of monetary exchange has amplified systemic vulnerabilities within interconnected banking networks, third-party processors, and cloud-based financial platforms. Cybercriminal enterprises exploit these interconnected systems through automated attack vectors, credential harvesting, synthetic identity construction, and coordinated fraud rings operating across jurisdictions [3]. Financial losses associated with online fraud continue to escalate due to increasingly sophisticated evasion techniques designed to bypass static control mechanisms. Traditional security architectures, heavily reliant on deterministic rule sets and predefined risk thresholds, struggle to adapt to evolving adversarial behavior [4]. Escalating transaction complexity demands advanced analytical capabilities capable of identifying subtle anomalies hidden within high-dimensional datasets. As financial institutions pursue innovation and customer-centric digital transformation, the need for resilient, intelligent, and scalable fraud detection frameworks has become a strategic imperative within modern finance [5].

Artificial Intelligence has emerged as a transformative force within payment security, offering advanced capabilities that extend beyond conventional statistical monitoring systems [6]. Machine learning algorithms analyze historical transaction data to detect hidden correlations, behavioral irregularities, and probabilistic fraud indicators [7]. Deep learning architectures enhance detection precision by extracting complex, nonlinear feature representations from large-scale datasets encompassing transactional metadata, geospatial information, device fingerprints, and user interaction patterns [8]. Graph-based learning models introduce relational intelligence, enabling the identification of coordinated fraud networks and collusive transaction structures that evade isolated account-level monitoring. Reinforcement learning further strengthens adaptive defense mechanisms by optimizing dynamic authentication thresholds based on evolving risk environments. These AI-driven methodologies facilitate real-time transaction scoring within milliseconds, aligning security requirements with high-frequency digital payment infrastructures [9]. Continuous model retraining mechanisms address distributional shifts and concept drift, maintaining predictive robustness as fraud tactics evolve. The convergence of computational intelligence and financial cybersecurity establishes a paradigm shift from reactive control strategies toward predictive, adaptive, and data-driven security ecosystems capable of responding to complex adversarial threats [10].