RADemics

E-Commerce Fraud Detection Using Behavioral Analytics and Deep Reinforcement Learning

Kavitha G, Yukti Varshney
St. Josephs College of Engineering,
Moradabad Institute of Technology

E-Commerce Fraud Detection Using Behavioral Analytics and Deep Reinforcement Learning

[1]Kavitha G, Assistant Professor, Department of Artificial Intelligence and Data Science, St. Josephs College of Engineering, Chennai, Tamil Nadu, India. kavitha@stjosephs.ac.in

[2]Yukti Varshney, Assistant Professor, Department of Computer Science and Engineering, Moradabad Institute of Technology, Moradabad, Uttar Pradesh, India. yuktivarshney16@gmail.com

Abstract

The exponential growth of e-commerce platforms has created unprecedented opportunities for digital commerce while simultaneously increasing exposure to sophisticated fraudulent activities. Traditional rule-based and static machine learning systems struggle to detect evolving fraud strategies due to limited adaptability, reliance on historical patterns, and high false-positive rates. Integration of behavioral analytics with deep reinforcement learning offers a transformative approach to address these challenges. Behavioral analytics captures multi-dimensional user interactions, temporal sequences, and device-contextual patterns, providing rich features for fraud assessment. Deep reinforcement learning enables adaptive learning and real-time decision-making, optimizing detection policies through continuous feedback from transactional environments. The hybrid framework supports early identification of anomalies, improves detection accuracy, and reduces operational risks without disrupting legitimate user experience. Practical considerations such as feature engineering, reward function design, class imbalance handling, and scalable deployment are essential for achieving effective and robust fraud detection. This chapter explores methodological frameworks, implementation strategies, and performance evaluation techniques, demonstrating the efficacy of combining behavioral intelligence with adaptive learning mechanisms. The proposed approach establishes a scalable and resilient foundation for next-generation e-commerce fraud prevention, capable of evolving alongside dynamic attack strategies.

Keywords: E-commerce fraud, Behavioral analytics, Deep reinforcement learning, Anomaly detection, Adaptive learning, Real-time monitoring.

Introduction

The rapid proliferation of e-commerce platforms has transformed global trade and consumer behavior by providing seamless access to products and services across geographical boundaries [1]. Online marketplaces, digital payment gateways, and mobile commerce applications have fueled this growth, creating unprecedented convenience for consumers and revenue streams for businesses [2]. This expansion has also exposed vulnerabilities, as fraudulent actors exploit technological and operational gaps in transactional ecosystems [3]. Fraud in e-commerce encompasses a wide range of activities, including payment card fraud, account takeovers, phishing, identity theft, and bot-driven manipulations. These activities impose significant financial losses, damage customer trust, and degrade platform integrity [4]. Traditional fraud detection mechanisms, primarily rule-based systems or static statistical models, often fail to capture the dynamic and evolving nature of such malicious activities. Fixed thresholds, historical patterns, and manual rules are unable to respond to sophisticated, adaptive fraud strategies. The emergence of data-driven and intelligent detection systems has become critical, requiring approaches capable of understanding complex behavioral signals, real-time adaptation, and multi-dimensional contextual analysis to effectively mitigate risks and maintain operational efficiency [5].

Behavioral analytics provides a structured approach for profiling user interactions, offering insights that extend beyond conventional transaction-level evaluation [6]. By analyzing sequences of actions, session characteristics, device usage patterns, and interaction timing, behavioral analytics captures the latent signatures of both legitimate and fraudulent behaviors [7]. Temporal patterns, navigation paths, clickstream data, and activity consistency create a multidimensional representation of user behavior, enabling the detection of anomalies that static rules fail to identify [8]. Sophisticated fraud operations attempt to replicate legitimate behavior, but subtle deviations in timing, sequencing, or device-context can be discerned through continuous behavioral monitoring. The adoption of behavioral analytics supports proactive risk assessment, allowing e-commerce systems to identify potential threats early and apply intervention strategies before substantial financial or operational impact occurs [9]. This analytic perspective also facilitates interpretability, providing insights into why specific actions are classified as suspicious, which assists in regulatory compliance and auditing processes. Behavioral profiling thus represents a foundational pillar for modern, intelligent fraud detection systems [10].