RADemics

Intelligent Fraud Detection in E-Commerce Platforms Using Behavioral Analytics

Ruchi Pandey, Kathiravan Ravichandran
The ICFAI University, Dhaanish Ahmed Institute of Technology

Intelligent Fraud Detection in E-Commerce Platforms Using Behavioral Analytics

[1]Ruchi Pandey, Assistant Professor, Faculty of Commerce, The ICFAI University, Raipur, Durg, India. ruchip_27@yahoo.in

[2]Kathiravan Ravichandran, Assistant Professor, Department of Science and Humanities - English, Dhaanish Ahmed Institute of Technology, Coimbatore, Tamil Nadu, India. fredrickjohnpaul@gmail.com

Abstract

Rapid expansion of digital commerce ecosystems and online financial transactions created critical security challenges associated with sophisticated fraud attacks, account takeover incidents, synthetic identity exploitation, payment manipulation, and automated cybercrime operations across e-commerce platforms. Conventional rule-based fraud prevention mechanisms demonstrate limited adaptability against evolving attack strategies, dynamic transaction behaviors, and large-scale anomalous activities within modern digital payment infrastructures. Intelligent behavioral analytics integrated with machine learning and deep learning techniques provides advanced capabilities for real-time fraud detection, predictive risk assessment, anomaly recognition, and adaptive cybersecurity management in highly distributed e-commerce environments. This book chapter presents a comprehensive investigation of intelligent fraud detection frameworks using behavioral analytics for secure digital commerce applications. The study examines major categories of e-commerce fraud, behavioral monitoring techniques, transaction analysis mechanisms, feature engineering methodologies, and advanced artificial intelligence models for fraud classification and anomaly detection. Significant emphasis focuses upon deep learning architectures, behavioral biometrics, deep autoencoders, ensemble learning techniques, and scalable real-time fraud analytics systems capable of processing high-volume transactional data streams. Critical challenges involving noisy datasets, class imbalance, false-positive reduction, privacy preservation, adversarial attacks, and computational scalability receive detailed analytical discussion within the context of modern cybersecurity infrastructures. Emerging technologies including Explainable Artificial Intelligence, Federated Learning, Blockchain integration, and Graph Neural Networks receive exploration for strengthening intelligent fraud prevention capabilities across distributed e-commerce ecosystems. The chapter contributes a structured analytical perspective toward development of adaptive, scalable, and behavior-driven fraud detection architectures capable of enhancing transaction security, operational reliability, customer trust, and financial risk management within next-generation digital commerce platforms.

Keywords: Behavioral Analytics, Fraud Detection, E-Commerce Security, Deep Learning, Anomaly Detection, Machine Learning.

Introduction

Rapid advancement of digital technologies transformed traditional commercial activities into highly interconnected online business ecosystems supported through e-commerce platforms, mobile applications, cloud infrastructures, and electronic payment systems [1]. Increasing consumer dependence upon online shopping, digital banking, contactless transactions, and mobile commerce services accelerated transaction volumes across global digital marketplaces [2]. Large-scale digital transformation created substantial opportunities for businesses through improved operational efficiency, customer accessibility, and automated financial management [3]. Simultaneously, continuous growth of online financial activities attracted sophisticated cybercriminal operations targeting payment systems, customer accounts, transaction gateways, and digital authentication infrastructures [4]. Fraudulent activities involving payment manipulation, account takeover attacks, synthetic identity fraud, credential theft, phishing operations, and bot-driven transaction abuse generated severe financial and reputational consequences across modern e-commerce environments [5]. Growing complexity of cyber threats created urgent requirements for intelligent fraud detection systems capable of protecting digital commerce ecosystems against continuously evolving fraudulent strategies and organized cybercrime activities within highly distributed transactional environments.

Traditional fraud prevention frameworks primarily depend upon static rule-based mechanisms, predefined transaction thresholds, blacklist databases, and manual verification procedures for identifying suspicious financial activities within e-commerce systems [6]. Conventional security architectures evaluate transaction amount, geographic location, purchase frequency, IP address consistency, and customer authentication records for fraud classification purposes [7]. Such approaches provide limited adaptability toward emerging attack patterns because cybercriminals continuously modify behavioral strategies and exploit vulnerabilities within digital payment infrastructures [8]. Increasing use of automated bots, artificial intelligence-driven cyberattacks, credential stuffing techniques, and behavioral spoofing operations reduced effectiveness of conventional transaction monitoring systems across large-scale digital commerce platforms [9]. High false-positive rates generated through static analytical methods created operational inefficiencies, delayed payment processing, customer dissatisfaction, and increased verification costs for financial organizations [10]. Complex transaction environments therefore require adaptive analytical frameworks capable of recognizing hidden anomalies and behavioral irregularities associated with modern cyber fraud operations.