

Chapter 11

AI-Enhanced Fraud Detection in Banking and E-Commerce

Ashok Koujalag

Shri Vishnu Engineering College for Women, India

T. Eswaran

T.S.M. Jain College of Technology, India

Amit Subramanyam

Rani Channamma University, India


Isa Bayhan

Bolu Abant Izzet Baysal University, Turkey


Varun Tiwari

Don Bosco Institute of Technology, India

Trinkul Kalita

 <http://orcid.org/0009-0006-4996-9738>
Assam Down Town University, India

S. Bala Krishnan

 <http://orcid.org/0009-0000-9391-4458>
Vaagai International Publishing House, India

ABSTRACT

The study proposes ways that businesses might integrate AI with their fraud detection systems, as well as future improvements that can be made to these solutions. This study shows how AI can affect the industry's future and contributes to what is already known about AI's effects on banking and security. When faced with the sheer magnitude and complexity of today's challenges, traditional rule-based fraud detection systems frequently fall short. One game-changing strategy for fighting fraud is AI which uses cutting-edge ML, DL and NLP approaches. This section delves into the function of AI in detecting fraud, how it improves monitoring and decision-making in real-time, and the ways it has been applied in e-commerce and

DOI: 10.4018/979-8-3373-5223-7.ch011

banking. Emerging technologies such as FL graph NN and blockchain-integrated AI systems are discussed towards the conclusion, after issues like explainability, data privacy and adversarial attacks have been addressed.

1. INTRODUCTION

Web-based methods are gradually replacing the more conventional method of paying with cash in business transactions due to the proliferation of e-commerce platforms. Online shopping, in contrast to the entity economy, has been relatively unscathed by the COVID-19 pandemic which has contributed to the industry's consistent development. By 2023, the predicted sales volume of business-to-consumer (B2C) e-commerce is \$6.50 trillion. New security risks have arisen in recent years, despite the fact that e-commerce and contemporary technology are growing and providing improved chances for online firms. Online fraud has reportedly increased at an alarming rate, costing billions of dollars annually around the world year. To guarantee the safety of online transactions, anti-fraud measures are essential due to the decentralised and ever-changing structure of the Internet (Rana, 2019). In the face of new security risks, current fraud detection systems that rely on user behaviour anomalies still have holes. Lack of effective process control throughout the trading process is a major flaw in current fraud detection systems. One of the most pressing problems that requires fixing is the flawed monitoring feature. Because current work does not incorporate process capture, the detection perspective is often insufficient. It offers a process-based approach that records and analyses user actions in real-time and turns past data into controllable data to achieve this goal. Furthermore, it integrate a multi-view anomaly detection system (Poudel & Dhungana, 2022).

2. TYPES OF FRAUD

The telecommunications, credit card, computer, bankruptcy, theft, counterfeit, application, and behavioural fraud types all come into play when it comes to e-commerce fraud (Prabin Adhikari et al., 2024)V.

Credit Card Fraud: There are two main categories of credit card fraud: offline and online.

- **Offline Fraud:** The use of a counterfeit or stolen physical card in any setting is offline fraud.
- **Online Fraud:** It occurs when a person does a fraudulent act through the use of the internet, phone or web (P. Kamuangu, 2024).

28 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/ai-enhanced-fraud-detection-in-banking-and-e-commerce/407731

Related Content

Identification and Prevention of Joint Gray Hole and Black Hole Attacks

Munesh C. Trivedi and Sachin Malhotra (2019). *International Journal of Ambient Computing and Intelligence* (pp. 80-90).

www.irma-international.org/article/identification-and-prevention-of-joint-gray-hole-and-black-hole-attacks/225772

Privacy-Preserving Aggregation in the Smart Grid

Georgios Karopoulos, Christoforos Ntantogian and Christos Xenakis (2017). *Security Solutions and Applied Cryptography in Smart Grid Communications* (pp. 80-97).

www.irma-international.org/chapter/privacy-preserving-aggregation-in-the-smart-grid/172673

Harnessing Blockchain for Human-Centric Transformation: Enhancing KPI Outcomes in Flexible Work Models During Recovery Phases

Heru Susanto, Alifya Kayla Shafa Susanto, Syafiq Rowii, Desi Setiana, Andri Saputra and Taufik Yuniartoro (2026). *Emerging AI, Governance, and Digital Innovations for Sustainable Organizations* (pp. 131-256).

www.irma-international.org/chapter/harnessing-blockchain-for-human-centric-transformation/399750

AI Corporate Governance and Legal Accountability: Comparative Indian–International Frameworks

Shashank Solanki, Kalpna Sharma, Vijaishree Dubey Pandey, Mayank Kapila, Rituraj Sinha, Sheetal Singha and Vijeta Verma (2026). *Legal Challenges of AI Across Interdisciplinary Sectors* (pp. 1-42).

www.irma-international.org/chapter/ai-corporate-governance-and-legal-accountability/400733

A Comparative Study on Adversarial Noise Generation for Single Image Classification

Rishabh Saxena, Amit Sanjay Adate and Don Sasikumar (2020). *International Journal of Intelligent Information Technologies* (pp. 75-87).

www.irma-international.org/article/a-comparative-study-on-adversarial-noise-generation-for-single-image-classification/243371