Chapter 3
AI-Driven Fraud Analytics:
Proactive Strategies for Detecting Emerging Cybercrime Patterns

R. N. Ravikumar
https://orcid.org/0009-0009-3705-1681
Marwadi University, Rajkot, India

S. Aarthi
https://orcid.org/0009-0006-9064-2091
Marwadi University, Rajkot, India

ABSTRACT

Fraud and cybercrime are evolving rapidly, exploiting technological diversity and human vulnerabilities. Traditional detection systems are reactive and limited against sophisticated threats such as phishing, deepfakes, and insider fraud. This chapter explores AI-driven fraud analytics as a transformative approach to predict, detect, and prevent cyber threats in real time. It highlights how machine learning, deep learning, natural language processing, and graph analytics collectively improve anomaly detection, fraud prediction, and decision speed. Case studies from JPMorgan Chase (2024) and Airtel (2025) demonstrate AI's practical efficiency, achieving

DOI: 10.4018/979-8-3373-5992-2.ch003

up to 96% accuracy and reducing fraud recurrence by 38%. The chapter also addresses ethical and regulatory issues, emphasizing explainability and data privacy. Finally, it proposes a roadmap for AI integration into national and organizational fraud prevention strategies, promoting resilience, accountability, and sustainable digital security.

1. INTRODUCTION

The scale and complexity of cyber-crimes have changed due to massive growth of online transactions, online services and other related systems. The new technologies like Artificial Intelligence (AI), deepfakes, and automation are allowing fraudsters to conduct cross-border attacks in a large scale. Adaptive and data-driven threats can no longer be addressed by rule-based and tradition-based defensive mechanisms. In that regard, the AI-based fraud analytics has proved to be a paradigm shift, as it can be proactive and real time in detecting the anomaly and suspicious events. The chapter concerns how AI technologies, machine learning, deep learning, natural language processing and graph analytics are changing the fraud prevention frameworks (Mızrak, 2024). It has both theory and practical perspectives to demonstrate how AI can be utilised to identify, predict, and even avert cyber threats before they materialise. Besides, it considers the ethical, organizational, and policy consequences of introducing AI into detecting frauds, and the need to promote transparency, accountability, and cross-sector collaboration as one of the options of making the digital economy more resistant to emergent forms of cybercrime.

1.1 Evolution of Cybercrime in the Digital Era

Cybercrime has not merely been an unsuccessful struggle at hacking but currently has evolved into a mass and mature and monetized enterprise to attack the global digital environments. Hackers have the most opportunities to take advantage of vulnerabilities compared to any point in history due to the creation of cloud computing, Internet of Things (IoT), and financial technologies. The current-day types of fraud, including phishing-as-a-service, ransomware, and the recently developed AI-generated deepfakes,