Chapter 17
Study on Application of Artificial Intelligence and Machine Learning in the Banking Sector for Fraud Detection and Prevention

Retheesh P. Pillai

https://orcid.org/0009-0000-4203-8371
Karunya Institute of Technology and Sciences (Deemed), India

D. Ponmary Pushpa Latha
Karunya Institute of Technology and Sciences (Deemed), India

ABSTRACT

Cyberbanking fraud is a growing concern in the digital age, posing risks to financial institutions and consumers. Malicious actors exploit advanced technologies to steal money from banks and users. Traditional methods like rule-based analysis have limitations, especially against digital fraud schemes. This paper highlights the need for constant improvement in fraud prevention strategies. Financial institutions can use AI and ML, particularly deep learning, to enhance their defenses. These technologies enable real-time analysis of large data, detecting unusual patterns and improving fraud identification accuracy. Proactively adopting technological advancements is crucial to combat the ever-changing threat of cyberbanking fraud.

DOI: 10.4018/979-8-3693-3940-4.ch017

INTRODUCTION

The banking and finance industry is experiencing unprecedented growth on a global scale, fueled by technological advancements and the digitization of financial services. However, this rapid expansion has also led to a surge in fraudulent activities, as fraudsters continually devise innovative methods to exploit vulnerabilities in banking systems. In this modern era, there is no singular solution that can guarantee complete protection against fraud; rather, the landscape is characterized by a "double-edged sword" of technology, which evolves continuously, presenting both opportunities and challenges for fraud prevention. Fraudulent transactions not only outcome in losses of the financial for banks but also fuel criminal activities such as identity theft, money laundering, and terrorist financing, posing significant threats to national security. Despite the proliferation of studies aimed at exploring methods for online transaction fraud detection, existing approaches often fall short of achieving high precision and accuracy. In response to these challenges, there is a pressing need for banks to leverage advances in technology and analytics to enhance fraud prevention capabilities. The digital age has ushered in a golden era of convenience in banking. Gone are the days of long lines and limited access; online banking, mobile apps, and contactless payments have transformed how we manage our finances (Mead et al., 2018a). However, this ease of access comes with a lurking shadow – the ever-present threat of fraud. The convenience of modern banking, with its 24/7 access and digital transactions, comes with a hidden adversary: fraud. As financial institutions (FIs) strive to deliver a seamless user experience, safeguarding customer assets and preventing financial losses remains paramount. This fight for financial security necessitates robust fraud detection and prevention strategies.

Banks can create more reliable and flexible fraud detection systems by utilizing the power of cutting-edge technologies like AI, ML, and big data analytics. These systems are capable of analyzing vast volumes of transactional data in real-time, identifying anomalous patterns indicative of fraudulent behavior, and taking proactive measures to mitigate risks. Technology is a pivotal component in the fraud detection framework of the banking sector in India and various other countries worldwide. According to numerous survey reports, proactive forensic data analysis stands out as an automated solution aiding governments, regulatory bodies, and corporations in identifying the escalating incidence of fraud across various sectors, particularly in financial institutions like banks and insurance companies. One of the key ways in which technology is transforming the detection of fraud in the banking sector is through the utilization of advanced analytics and machine learning algorithms. These technologies have the ability to instantly detect patterns and anomalies that could point to fraudulent activity by analyzing enormous volumes of data in real-time (Biswas et al., 2022b). Additionally, advancements in artificial intelligence have