Chapter 8
Detecting Bank Financial Fraud in South Africa Using a Logistic Model Tree

Katleho Makatjane
https://orcid.org/0000-0002-3687-4098
Department of Statistics, University of Botswana, Botswana

Ntebogang Dinah Moroke
https://orcid.org/0000-0001-8545-1860
North West University, South Africa

ABSTRACT

Artificial intelligence is gradually becoming the standard mechanism underpinning online banking. Users' profiles can be confirmed using a variety of methods, including passcodes, fingerprints, acoustics, and images through this technology. On the other hand, traditional cybersecurity measures are unable to prevent internet-based fraud after the visualisation process has been infiltrated. In light of this, the aim of this chapter is to examine the efficiency of the logistic model tree (LMT) in detecting financial fraudulent transactions in South African banks and, ultimately, to develop a financial fraud early warning system. Web-scraping credit and debit card fraud data from SA are used to acquire daily data. The LMT is constructed utilizing a training set from the LogitBoost algorithm and obtained 17 financial conditioning elements. Overall, an early warning system model has shown to be a good performer with a prediction rate of 99.9%. This appears to be a promising approach for detecting online fraud vulnerabilities.

DOI: 10.4018/978-1-7998-9430-8.ch008

INTRODUCTION

The identification of financial fraud has grown to become a global topic. Fraud detection systems in financial institutions must be smart and effective. Between 2018 and 2019, online transactions increased credit and debit card theft by 20.5 percent. According to the South African Banking Risk Information Centre Report (2019), the country's failing economy has given hackers the impetus and opportunity to commit financial crimes, with digital banking incidents increasing by 20% in 2019. This number is sure to rise as hackers continue to obtain sensitive and private information from users, allowing them to trade on their accounts without their permission. Unfortunately, cybercrime has led to an increase in total fraudulent transactions on South African-issued cards. This premise is illustrated in Figure 1. Electronic technology, such as PayPal and fraud detectives, are helpful in thwarting ever-changing fraud schemes. According to Abdallah et al (2016), the percentage of fraud loss order channels in online stores is currently at 74 percent, with 49 percent in mobile channels. However, according to Cybersource (2021), the online store has recorded 80 percent of payment fraud and mobile commerce has tracked 68 percent. This suggests that there has been an upsurge in both online and mobile commerce fraud worldwide since 2016. The moral, based on these figures, is to manage discrepancies between different types of fraud deeds that have changed over time. A good fraud detection solution should be able to correctly categorise and detect fraudulent transactions in real-time transactions. According to Seyedhossein and Hashemi (2010), fraud detection is classified into two categories: (1) detecting fraud using AI (Artificial Intelligence) and (2) detecting fraud manually. Data analysts construct algorithms to spot abnormalities and trends using the former. This is accomplished by either creating models and training AI or acquiring "off-the-shelf" fraud detection technologies. A system that involves screening applicants and using training models to discover aspects that humans cannot constructed with the help of experts and AI. The latter, on the other hand, relies on the human eye to detect irregularities in a document's text style, alignment, spacing, and color. Unfortunately, this is not easy to do without a trained eye.

Financial crime has long been a source of concern for businesses and organisations across a wide range of industries. According to Budhram (2012), credit card theft caused financial losses in South Africa to increase by 53% between 2019 and 2021. As a result, the South African Financial Risk Intelligence Centre (SABRIC) has confirmed two events that have occurred in the banking system of South Africa (SA) in recent years. In 2019, the industry generated R403,15 million in revenue. This is an increase of R263,8 million over the previous year (SABRIC Report, 2019). Card fraud is a major concern for businesses that accept credit cards, the financial system, and, most crucially, individual users. The use of debit and credit cards for

MHLM Majority Voting Based Hybrid Learning Model for Multi-Document Summarization

Suneetha S.and Venugopal Reddy A. (2019). *International Journal of Artificial Intelligence and Machine Learning (pp. 67-81).*
www.irma-international.org/article/mhlm-majority-voting-based-hybrid-learning-model-for-multi-document-summarization/233890