

Chapter 9

Protecting Investor Sentiment by Detecting Financial Fraud With the Help of ML and AI Applications

Anumita Chaudhury
Garden City University, India

ABSTRACT

Investors, in spite of their vigilant moves, often are observed to fall victim to financial fraud. There are several machine learning algorithms both supervised and unsupervised which exist and continue to serve the objective of detecting financial fraud like under supervised machine learning random forest, k-nearest neighbours (KNN), logistic regression and support vector machine (SVM) and unsupervised machine learning includes K-means and SOM (self-organizing map). AI will help in mitigating the impact of volatility in the financial market. There is a necessity to adopt new-age machine learning and Artificial Intelligence which will promptly process millions of data and also identify dubious patterns has become very crucial to evade the losses caused by fraudulent activities.

INTRODUCTION

We have seen a sharp rise in fraud in the previous several years in the globalized and liberalized corporate climate, particularly in India's financial sectors. Over the past ten years, the Indian financial industry has experienced exponential expansion.

DOI: 10.4018/979-8-3693-3633-5.ch009

Detecting Financial Fraud With the Help of ML and AI Applications

However, this progress has not been without its challenges, since there has been a spike in fraud instances. Fraud causes the public coffers to suffer large losses, which has a negative impact on industry. To mitigate the threat of financial fraud, a protocol needs to be framed for early financial detection which is commonly witnessed within various service providers. The easy target of financial fraud in particular are the financial institutions in particular such as banks, fintech etc. The tactics adopted by the fraudsters are very dynamic in nature and hence continuous monitoring is required. Also, with the growth of the population of investment avenues, protecting investors' sentiments has progressively become a vital importance linked to global economic growth and people's lives. Financial fraud is a huge industry, causing direct losses of over USD 20 billion a year. Experts in the field believe that this number is actually considerably higher because businesses and investors find it difficult to properly detect and quantify damages resulting from fraud. Financial frauds mostly affect foreign direct investment (FDI) into India (ASSOCHAM, 2024). It is now necessary for the regulators to develop an internal fraud management strategy that is more strategic and technical in nature. They require disciplined and targeted action to overcome this obstacle.

This paper addresses a practical problem and makes several contributions to the body of knowledge on financial fraud detection. First of all, it discusses the most advanced method of financial fraud detection available in artificial intelligence and machine learning, which has excellent performance accuracy. Since traditional systems mostly depended on human interaction, they are unable to adjust to potential changes or circumstances. Adjuster inspections, agent inquiries, and internal auditor examinations were formerly used to combat fraud. However, traditional approaches have grown cumbersome and slow as the industry generates and processes more records, papers, and data on a Terabyte and Petabyte scale. As a result, practitioners and academics can better grasp this topic by using machine learning and artificial approaches as a road map.

The findings of this study are helpful for the finance industry, investors, and policy makers to obtain a better understanding of fraudulent activities and for detecting it using a predictive model. The remainder of the paper is as follows: section 2 discusses the past relevant studies; section 3 includes the materials and methods that are being used to build the solution for fraud detection. Moreover, data preprocessing, feature computation, and predictive models are being described here. Section 4 covers the overall discussion and concludes the paper where it also includes the theoretical implications, practical implications, discussion, and conclusion of the study.

22 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/protecting-investor-sentiment-by-detecting-financial-fraud-with-the-help-of-ml-and-ai-applications/351515

Related Content

Distributed WSN Vulnerability Remediation System Based on Mobile-N Policy

Zihan Zhou (2025). *International Journal of Information Security and Privacy* (pp. 1-25).

www.irma-international.org/article/distributed-wsn-vulnerability-remediation-system-based-on-mobile-n-policy/372903

Formal Verification of Secrecy, Coercion Resistance and Verifiability Properties for a Remote Electronic Voting Protocol

Khaoula Marzouki, Amira Radhouani and Narjes Ben Rajeb (2013). *International Journal of Information Security and Privacy* (pp. 57-85).

www.irma-international.org/article/formal-verification-of-secrecy-coercion-resistance-and-verifiability-properties-for-a-remote-electronic-voting-protocol/87425

Social/Ethical Issues in Predictive Insider Threat Monitoring

Frank L. Greitzer, Deborah Frincke and Mariah Zabriskie (2011). *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives* (pp. 132-161).

www.irma-international.org/chapter/social-ethical-issues-predictive-insider/46344

Building a Maturity Framework for Information Security Governance Through an Empirical Study in Organizations

Yassine Maleh, Mounia Zaydi, Abdelkbir Sahid and Abdellah Ezzati (2018). *Security and Privacy Management, Techniques, and Protocols* (pp. 96-127).

www.irma-international.org/chapter/building-a-maturity-framework-for-information-security-governance-through-an-empirical-study-in-organizations/202040

Detection of Drive-by Download Attacks Using Machine Learning Approach

Monther Aldwairi, Musaab Hasanand Zayed Balbahaith (2017). *International Journal of Information Security and Privacy* (pp. 16-28).

www.irma-international.org/article/detection-of-drive-by-download-attacks-using-machine-learning-approach/187074