IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11702

Detecting Money Laundering Transaction in Real Estate Using Machine Learning

H. Suraj[1], Aniruddha SP[2], Md.Rehan[3], Keshava Gowda[4], Jayakrishna Datta[5]

Department of AIML, Dayananda Sagar Academy of Technology and Management, Bangalore, India [1-5]

Abstract: Leveraging a comprehensive dataset from DNB, Norway's largest bank, this study aims to design, detail, and assess a machine learning system tailored to prioritize financial transactions for manual review in the context of potential money laundering. The model employs supervised machine learning techniques and draws on three categories of historical data: transactions flagged as suspicious by the bank's internal alert system, routine legal transactions, and potential money laundering cases reported to authorities. By analyzing sender and recipient background information, historical behavior, and transaction history, the model is trained to predict the likelihood that a new transaction should be reported. The findings indicate that excluding unreported alarms and uninvestigated transactions from the training process can lead to suboptimal model performance.

Keywords: Supervised Learning, Machine Learning, Beneish Score, Hybrid Model, Suspicious Transactions, Financial Statement Fraud, Hidden Markov Model.

INTRODUCTION

Financial statement fraud is a well-known issue in the business world, resulting in financial statements that are misleading and inaccurate. Numerous high-profile cases have brought attention to this problem, including those involving Enron Corporation, WorldCom, Tyco International, PT. Kimia Farma Tbk., PT. Hanson International Tbk., and PT. Garuda Indonesia (Persero) Tbk. Despite these examples, fraud continues to be a significant concern if not actively prevented and detected (Yesiariani & Rahayu, 2017).

One of the primary reasons for the persistence of financial statement fraud is weak internal control (Hamdani & Albar, 2016). To combat this, companies need internal auditors who possess comprehensive knowledge of internal control systems and their various aspects.

These auditors can then provide valuable insights and recommendations to stakeholders on establishing effective control mechanisms (Indonesian Bankers Association, 2019).

The rise in fraudulent financial reporting among public companies has heightened concern among various stakeholders, including investors, auditors, creditors, and others (Razali & Arshad, 2014). This increasing awareness underscores the critical need for robust detection and prevention measures to safeguard the integrity of financial statements and maintain stakeholder trust.

RELATED WORK

[1] Card Fraud

Credits are usually referred to as electronic financial transactions executed without physical currency. A credit card, widely utilized for online purchases, is a slim piece composed of thin plastic material containing credit services and customer information. Criminals employ credit cards for unauthorized transactions, causing significant losses to both banks and cardholders. The rise of counterfeit cards has further facilitated illicit transactions for fraudsters. Unauthorized use of a credit card without the owner's consent is deemed illegitimate. Any transaction conducted through unauthorized access to an account is considered fraudulent. Credit card fraud activities encompass offline and online fraud.Offline fraud involves criminals using stolen credit cards like legitimate cardholders, while online fraud scenarios occur on the internet.

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11702

[2] Financial Fraud in Statements

Financial statement fraud involves the manipulation of financial documents to portray a company as more profitable than usual. This can help in avoiding taxes, boosting stock prices, or securing bank loans. Financial statements hold critical records showcasing a company's financial status, including expenses, profits, and income. These reports also include management notes discussing business performance and future projections. These financial records shed light on a company's true financial health, determining its credibility and bankability. However, fraudulent statements can mislead stakeholders by altering data to make the company seem more prosperous. Manipulation of financial documents to portray a company as more profitable than usual.

Financial statements hold critical records showcasing a company's financial status, including expenses, profits, and income. However, fraudulent statements can mislead stakeholders by altering data to make the company seem more prosperous.

[3] Fraud in Insurance

The fraudulent use of insurance plans to get benefits from insurance companies is known as insurance fraud. Generally speaking, insurance protects people or organizations against monetary hazards. Fraudulent claims often target healthcare and vehicle insurance firms, while there are also cases of house and crop insurance fraud, albeit little research on these cases has been done. According to recent estimates, insurance fraud costs the US economy more than $1 billion USD a year, which ultimately drives up insurance costs for consumers.

The insurance company and the insured party usually have an agreement in place to pay expenses related to theft or unintentional damage in motor insurance claims. Even though lone thieves can commit insurance fraud by giving misleading information to the claims department, organized groups can also commit fraud.

[4] Financial Cyber-Fraud

The term "financial cyber fraud," which refers to illegal activity carried out in cyberspace with the intention of obtaining illegal financial advantages, is relatively new. Finding the criminals responsible for these kinds of crimes is a difficult task. These people deliberately conceal their activities to give the impression that they are regular users of financial services and online platforms. But when their activities are collectively examined, their aberrant behaviors become more apparent. The more sophisticated technologies and superior technical abilities that criminals get, the more difficult it is to stop them from committing illicit crimes. Financial institutions are under pressure to develop internal measures like real-time analytics and interception to reduce financial losses due to the convergence of financial crime and cybersecurity.

[5] Fraudulent Reporting

When data in financial statements are purposefully understated or falsified for illegal reasons, it is considered fraudulent financial reporting (ICAEW, 2020). Even while identifying fraudulent credit card transactions by fusing Genetic Algorithms (GA) and . This approach showed better efficacy in detecting fraud since it uses GA to calculate clustering threshold values and HMM to store historical transaction logs.this kind of fraud is uncommon, when it does happen, businesses may suffer large financial damages. In order to deceive users, financial statements may contain statistics that have been omitted or misrepresented (Hery, 2016). Attempts to conceal unearned income (liabilities) and replace it with revenue, or to inflate assets and revenues in order to minimize reported income, are common instances of fraudulent financial reporting. To cut costs and income taxes, some businesses purposefully lower revenue. According to Hery (2016), intentional misstatements in disclosure, purposeful misapplication of accounting principles in financial statements, and manipulation, falsification, or alteration of accounting data are the usual methods used in fraudulent financial reporting.

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11702

METHODOLOGIES USED

The monitoring of suspicious transactions linked to illicit money operations in a typical Norwegian bank consists of three main stages: alert, case, and reporting. Our data originates from DNB, the biggest financial corporation in Norway, and these steps apply to them as well. Every transaction that is done with a bank customer first goes through an alert phase, where a proprietary technology assesses the transaction according to a predetermined set of rules. Alert-setting transactions that pass through a streamlined manual review process but are found to be legal are classified as non-reported alerts or no cases (B) and are not subject to additional scrutiny. The remaining warnings are combined into cases that revolve on the main suspect and possibly connected parties.

1. BENEISH M-SCORE

The Beneish M-Score model, developed by Messod D. Beneish, gained significant attention with his influential 1999 paper "The Detection of Earnings Manipulation" and his 2012 follow-up study "Fraud Detection and Expected Returns." This model has become a crucial tool for identifying companies that might be manipulating their earnings as reported in financial statements.

The Beneish M-Score relies on various metrics, collectively known as the Beneish Ratio Index, to analyze financial statements for indications of potential fraudulent activity. By examining these ratios, the model helps detect discrepancies and anomalies that suggest income falsification. This methodology is an essential part of the broader effort to ensure the accuracy and reliability of financial reporting, providing a systematic approach to identifying and addressing financial statement fraud.

2. Markov Model

Compared to conventional Markov models, the Markov Model is widely used as a dual-embedded stochastic approach to handle more complicated stochastic processes. The HMM concept has been used in a variety of ways to improve efforts to identify financial fraud. employed an HMM-based technique to look at incoming transactions and assess card owners' activity. They used a clustering method based on aggregating factors within particular regions to differentiate between fraudulent and non-fraudulent patterns. Furthermore, . developed a novel hybrid method for

3. Neural Network

Neural networks, inspired by the structure and function of biological neural networks, are highly effective when applied to large datasets. This makes them particularly suitable for detecting fraud in the financial sector. Various approaches based on artificial neural networks (ANN) have been proposed to tackle financial fraud.

Srivastava et al. investigated credit card fraud detection from the trader’s perspective, utilizing a method that connects merchants with payment gateways, which act as intermediaries between the merchant and the fraud detection model. This approach helps in identifying fraudulent transactions more efficiently.

Ghobadi and Rohani developed a hybrid model using a Cost- Sensitive Neural Network to detect credit card fraud. Their model not only improves detection rates but also reduces the costs associated with false negatives, thereby enhancing overall fraud detection effectiveness.

Randhawa et al. have also contributed to this field, though further details of their work are necessary to provide a complete picture. Overall, the application of neural networks in fraud detection is a promising area of research, leveraging advanced computational techniques to protect financial systems from fraudulent activities.

4. Logistic Regression

Logistic regression is primarily used for binary and multiclass classification problems, analyzing a set of variables through regression. Frequently applied for recognizing patterns and relationships among numerous

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11702

dependent binary variables, it serves as a crucial tool in the financial realm. Many studies employ logistic regression (LR) techniques for financial fraud detection, with Peng and You suggesting a suitable technique for identifying fraudulent transaction characteristics using LR. Logistic regression works by estimating the probability that a given transaction is fraudulent based on various factors, such as transaction amount, frequency, and the background of the involved parties. By leveraging historical data, LR models can learn from past instances of fraud to predict and identify suspicious transactions in real-time. This predictive capability makes logistic regression an essential component in the toolkit for financial fraud detection, helping to safeguard the integrity of financial systems and protect stakeholders from the adverse effects of fraudulent activities.

CONCLUSION

Financial fraud manifests in various financial sectors, posing challenges to companies. Despite ongoing efforts to combat financial fraud, it persists, negatively impacting the economy and society. Leveraging artificial intelligence and machine learning, fraud detection can be streamlined by examining vast financial data. This paper reviews and synthesizes existing literature on ML-based fraud detection, highlighting its superiority over rule- based approaches. By adapting and learning from new data continuously, ML-based detection methods outperform traditional rule-based models.

REFERENCES

1. Alexandre, C. and Balsa, J. (2015), "Client profiling for an anti-money laundering system", arXiv preprint arXiv:1510.00878.
2. Bergstra, J.S., Bardenet, R., Bengio, Y. and Kégl, B. (2011), "Algorithms for hyper-parameter optimization", Proceedings of the 24th International Conference on Neural Information Processing Systems, pp. 2546-2554.
3. Beneish, M. D., Lee, C. M. C., & Nichols ,D. C. (2012). Fraud Detection and Expected Returns. *SSRN Electronic Journal*.
4. Bhavani, G., & Amponsah, C. T. (2017). MScore and ZScore for Detection of Accounting Fraud. *Accountancy Business and the Public Interest*, 68–86.
5. Christy, Y. E., & Stephanus, D. S. (2018). Pendeteksian Kecurangan Laporan Keuangan dengan Beneish M-Score pada Perusahaan Perbankan Terbuka. *Jurnal Akuntansi Bisnis*, *16*(1), 19–41.
6. Chen, T. and Guestrin, C. (2016), "Xgboost: a scalable tree boosting system", Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM, pp. 785-794.
7. Parvin, R. (2020). Earnings Management Practice in Bangladesh. International Journal of Business and Management Future, 4(1), 27–32.
8. van Capelleveen, G.; Poel, M.; Mueller, R.M.; Thornton, D.; van Hillegersberg, J. Outlier detection in healthcare fraud: A case study in the Medicaid dental domain. Int. J. Account. Inf. Syst. 2016, 21, 18–31.
9. Bhavitha, B.K.; Rodrigues, A.P.; Chiplunkar, N.N. Comparative study of machine learning techniques in sentimental analysis. In Proceedings of the 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 10– 11 March 2017; pp. 216–221.
10. Pejic-bach,M. Invited Paper:Profiling Intelligent Systems Applications in Fraud Detection and Prevention: Survey of Research Articles Profiling intelligent systems applications in fraud detection and prevention: Survey of research articles. In Proceedings of the 2010 International Conference on Intelligent Systems, Modelling and Simulation, Liverpool, UK, 27–29 January 2010.
11. D'Addio,R.M.; Manzato,M.G. A Collaborative Filtering Approach Based on User's Reviews. In Proceedings of the 2014 Brazilian Conference on Intelligent Systems, Washington, DC, USA, 18–22 October 2014; pp. 204–209.

