IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Income Tax Fraud Detection Using Machine Learning

Mohammed Kaif [1], Darshan S[2], Anurag Kumar[3], Vaibhav V[4], and Amrutkumar Bandihal[5]
Students, Presidency University, Bangalore, India

Abstract— detecting tax fraud is the highest priority of almost all of the tax administrations aiming at the maximization of revenues and most importantly, the high level of compliance. These methods, including data mining, machine learning and the other methods, such as traditional random auditing, have already been applied to a large proportion of studies to address tax fraud. Work of this study is to apply Artificial Neural Networks in order to detect tax fraud factors in income tax data. The findings indicate that the Artificial Neural Networks show strong behaviors in the tax fraud detection with an accuracy at 92%, a precision at 85%, a recall score at 99% and an AUCROC value at 95%. All businesses, cross-border or domestic, the size of the business, small businesses or corporate businesses, are to be found among the factors considered by the model to be of greater saliency for income tax fraud detection. In this work, the paper is in agreement with the previous closely related to the previous tax fraud feature that covered all tax types jointly using various machine learning models. To our knowledge, this paper is the first to apply Artificial Neural Networks in the detection of income tax fraud in Rwanda, by different parameters such as layers, batch size, and epochs tuning, to select the most appropriate parameters which perform better than other parameters, in terms of accuracy. In this work, for this subject, it is found that with a simple model, no hidden layer, softsign activation function, performs more excellent. The findings of this work will assist auditors to get a grasp of the factors contributing to income tax fraud in order to decrease audit work generated, to decrease audit costs, and to recover the money lost due to an income tax fraud.

1. Introduction

Tax fraud, which involves intentionally misreporting tax data to reduce liabilities, causes governments to lose billions of dollars annually. This deprivation has put pressure on tax officials to implement effective fraud detection mechanisms. Nevertheless, conventional approach-based on auditors' intrapersonal experience or rule-based systems-is constrained by several aspects, including high rate of false alarms or lack of adaptation to the emerging fraud behavior. As a remedy, Machine Learning models can identify new fraud patterns from big data sets without involving much human labor and resource consumption.

Despite the potential of ML, supervised models rely on the audited data from before, accounting for a minor proportion of the total tax returns. The unsupervised models (i.e., that analyze all data in use) appear to be inefficient in detecting fraud alone. In this manuscript, the authors are showing a hybrid system that has the two paradigms and a supervised and an unsupervised approach with the possibility to decrease false positives and to enhance the fraud detection efficiency.

1.1 Background

Income tax fraud is a significant issue for governments, eroding tax revenue and tax system credibility. Fraud detection by computer is becoming increasingly more challenging in the digital age, with financial transactions multiplying in both number and complexity. Traditional approaches, including manual examinations and strict rule-based schemes, are frequently

insufficient to keep up with innovative fraud schemes, leading to a significant false positive rate, in which valid taxpayers are incorrectly identified for examination.

Recent developments in AI and ML open new avenues for fraud detection. Analyzing vast amounts of data, AI and ML can expose hidden patterns and trends that enable tax authorities to detect fraud better.

1.2 Problem Statement

Tax fraud, even though it is continuously emerging from new technology, still exists. The existing detection methods are not suitable for the new trickology of frauds and, in all cases, also does not stop the fraudulent activity leading to great financial loss. Industrial-scale real-time data analysis as it's used in traditional methods is wasteful and increases operating cost. In this paper, an AI model is proposed in order to better detect fraud combining both supervised and unsupervised learning techniques.

1.3 Importance of the Research

In this study, the discovery of income tax fraud with the help of AI and ML algorithms is of great relevance. The current proposed framework performs a diagnosis of historical tax data, in such a way it can significantly improve the detection accuracy as well as reduce the false positives. This research contributes to the body of knowledge on the application of AI in financial security, offering insights into how technology can transform traditional tax administration practices. The results have a number of practical consequences for tax administrators and policy makers, who are searching for new ways to prevent fraud.

2. Literature Review

2.1 Fraud Detection Technique Overview

Fraud detection in the past decade has experienced a fast evolution, both driven by a technological development and the evolution together of fraudulent strategies. Early methods adopted rule-based systems that identified suspicious activities based on predefined criteria. However, systems operated reactively, detecting fraud after its occurrence. Although these systems could be effective at times, there were several limitations such as relatively high false-positive rates that were not adaptive to evolving patterns of fraud.

Due to the rising volume and complexity of financial transactions, fraud detection has moved toward dynamic and data-driven methods. The contemporary methods employ statistical analysis, data mining and machine learning algorithms to detect outliers in large datasets, enabling real-time monitoring and upfront fraud detection.

2.1.1 Proposed architecture

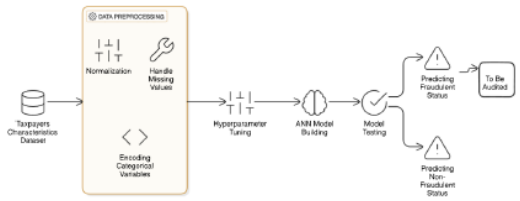


Fig1: Architecture Diagram for Proposed System

The system architecture for the income tax fraud detection platform is constructed to enable effective data mining, model building, and user experience. The architecture consists of several main components, each of these contributing to the overall performance of the system.

2.2 Machine Learning in Fraud Detection

Supervised classification is based on annotated data, whereas unsupervised classification is based on the clustering of patterns and labels in unlabelled data.

Performance measures for classification include the following:

True Positives (TP): Correctly identified fraudulent cases.

False Positives (FP): Actual valid transactions incorrectly labeled as fraudulent

False Negatives (FN): Frauds that are missed by the system.

True Negatives (TN): Actual valid transactions correctly identified.

Among the most frequent performance measures are accuracy (ACC), recall (R), precision (P), F-measure (F) and specificity (S) described in the following.

$ACC = (TP + TN) / N$

$R = TP / (TP + FN)$

P = TP / (TP + FP)

F 2 R P (R P) .

S = TN / (TN + FP)

In our work, supervised classification was performed by means of algorithms including Neural Network, Naive Bayes, Decision Tree, Ensemble Learning, Random Forest and Logistic Regression.

2.2.1 Neural Networks

Neural Networks are models composed of interconnected nodes that simulate the functioning of the human brain. These networks address classification tasks by iteratively modifying weights associated with data features, imutising the difference between the predicted and the true classification.

2.2.2 Naive Bayes

Naive Bayes is a probabilistic classifier which under the assumption of feature independence. It employs conditional probabilities to estimate the probability event and it is effective on large data.

P(A,B) = P(A)P(B)

P(y|x1,…,xn)=P(x1|y)P(x2|y)…P(xn|y)P(y)/

P(x1)P(x2)…P(xn)

2.2.3 Decision Trees

They are hierarchical models where nodes are correlated features, and branches are feature values. For construction of the tree, the data has to be segmented at each node in a way that entropy is minimized up to homogeneous clusters. The process is continued until a complete classification of the data is obtained.

2.2.4 Ensemble Learning

Ensemble Learning combines multiple algorithms to improve overall performance. The following common techniques are used that consist of the combination of classifiers' results, either by averaging the probabilities or by majority voting. Heterogeneous classifier ensembles frequently yield more accurate results by virtue of model heterogeneity.

2.2.5 Random Forests

They use it to extend the decision trees by the ensemble of trees called Random Forests. Here, in the training of single trees, the training data is a random draw out of all the data, and the prediction of the forest is the output of plurality reached by voting of the individual trees. This reduces overfitting and improves the classification accuracy.

2.2.6 Logistic Regression

Logistic Regression is a statistical model that is used for classification of data into two categories, or binary classification, by a logistic function. It computes the probability of an event and refines weights to reduce the prediction error.

2.3 Limitations of Existing Approaches

Despite all that has been accomplished, some of the shortcoming of machine learning based fraud detection is as follows:.

High False Positive Rates: The big issue is that the ML models also flag real transactions as fraud which results in frustration for the customer, waste of resources, and bad PR. This is a need for more advanced models with higher sensitivity and specificity.

Data Quality Issues. The performance of the ML model relies significantly on data quality. Incomplete, outdate or skewed data can significantly imbalanced predictions. In particular, imbalanced datasets (where fraudulent transactions occur with far lower probability than legitimate transactions) pose a challenge to classification-based models.

Lack of Interpretability: Many of the advanced ML models, including deep learning networks, are black boxes. As a result, the user may not be able to discern the purpose of the predictions, by, which will lead to lowered trust in the system as well as increased debugging difficulty.

Adaptation to Emerging Fraud Patterns: Fraudsters continually adapt their techniques, which results in model drift, where the performance of the model deteriorates over time. Continuous learning approaches are required for the continuous efficiency of fraud detection systems.

Integration Challenges: Adopting AI-based fraud detection into existing systems presents the technological and the organizational challenges. Resistance to change, lack of infrastructure, and the need for extensive training can all cause delay in the successful transition.

2.4 Emerging Trends in AI for Fraud Detection

The latest developments in AI are leading new trends towards the improvement of fraud detection functionalities:.

Real-Time Analytics: The capability of real-time analytics facilitates upon-the-fly monitoring of transactions, thereby potentially speeding detection of suspicious behaviour. This preventive strategy prevents fraud at its early stage which saves financial harm.

Natural Language Processing: NLP allows the mining of unstructured data, e.g., email and social media, for fraud detection. NLP can identify communication involving sentiment and context related to potential fraud.

Federated Learning: Federated learning allows different organisations to collaboratively train machine learning models without disclosing any private information to the others, thus maintaining the privacy of the information and enhancing the generalization of ML models onto a variety of datasets.

Explainable AI (XAI): XAI tackles the problem of the interpretability of AI models; the force behind interpretability is trust in the user. In the domain of fraud detection XAI alerts stakeholders as to why decisions on these automated implementations are made; consequently compliance with law and regulatory needs is increased, along with the interpretability of decisions.

2.5 Conclusion

Machine learning and artificial intelligence have greatly advanced fraud detection by providing tools for improving both tax compliance and revenue enforcement. Challenges such as high false positive rates, data quality issues, lack of interpretability, and integration with existing systems are still open issues. The potential applications are outlined within the promising solutions, which are developing trends such as real-time analytics, NLP, federated learning, and explainable AI. Research needs to be carried out to advance these approaches for the creation of increasingly adaptive, efficient, and explainable fraud detection systems, and thus the efficiency of income tax fraud prevention.

3. Research Gaps

High False Positive Rates: Misclassified instances result in wasted resources and diminished taxpayer confidence.

Limited Adaptability: Static models do not take into account the development of the fraud tactics.

Lack of Real-Time Analytics: Most systems are at present batch based which results in delaying detection and intervention of fraud.

4. Proposed Methodology

4.1 Data Collection

The study uses primary data sources, such as anonymous government tax records and synthetic datasets, to ensure a balanced representation of fraudulent and legitimate cases. Data preprocessing deals with seven problems including missing values, outlier identification, normalization and encoding of categorical features for analysis.

4.2 Model Selection

Several machine learning algorithms were evaluated for their applicability:

Artificial Neural Networks (ANN): Demonstrates superior performance in detecting intricate fraud patterns.

Random Forests: It is also robust to overfitting and offers interpretable feature importance metrics.

Logistic Regression: A good baseline for binary classification tasks.

4.3 Implementation Steps

Feature Selection: Detection of key fraud indicators such as inconsistency of declared income and expenses.

Data Partitioning: Splitting datasets into training (70%, testing (20%, and validation (10% subsets.

Model Training and Evaluation: Applying cross-validation and optimizing hyperparameters to enhance performance.

Performance Metrics: Accuracy, precision, recall, F1-score and ROC-AUC guarantee robustness, and effectiveness.

5. Results and Discussion

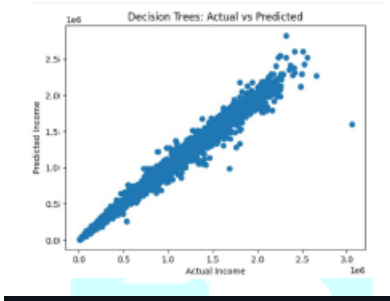
The ANN-based model outperformed to the extent of:

Accuracy: 92% Score, which means reliability in overall predictions

Precision: 85%, error reduction on false positives

Recall: 99%, the highest possible detection ratio with fraudulent cases

AUC-ROC Score: 95%, robust classification capability



Key Findings

The ones with higher weights are business size and years of business operation, which are used to predict the fraudulent activity.

In this way, optimized thresholds have led to a reduction in false negatives while maintaining the recall ratio.

Comparison showed that the ANN model outperformed the established rule-based systems in terms of adaptability and scalability. Still, data acquisition and model interpretability remain the top concerns to overcome in future research.

6. Conclusion

This paper illustrates the extremely powerful potential of machine learning, particularly, ANN, for combating income tax fraud. The proposed framework addresses the existing gaps in methods that are available to it, and leverages the capabilities of advanced analytics, so as to be scalable, efficient and versatile. Subsequent directions would include adding real-time analytics to these models, increasing their explainability via Explainable AI, and extending their use so that they can be used to a variety of taxation contexts. This certainly will help make more resilient compliance frameworks and fairly collect taxes.

References

[1] Poole, D., & Mackworth, A. (2017). Artificial Intelligence: Foundations of Computational Agents.

[2] Breiman, L. (2001). Random Forests. Machine Learning, 45(1), 5-32.

[3] Russell, S., & Norvig, P. (2010). Artificial Intelligence: A Modern Approach.

[4] SAS Insights. "Fraud Detection with Machine Learning." Accessed from sas.com.

[5] Microsoft. "Real-Time Fraud Prevention in Taxation." Accessed from microsoft.com.

[6] McCulloch, W.S.; Pitts, W. A Logical Calculus of the Ideas Immanent in Nervous Activity; Springer: Berlin/Heidelberg, Germany, 1943. [**Google Scholar**]

[7] Kaur, P.; Gosain, A. Comparing the behavior of oversampling and undersampling approach of class imbalance learning by combining class imbalance problem with noise. In ICT Based Innovations; Springer: Berlin/Heidelberg, Germany, 2018; pp. 23–30. [**Google Scholar**]

[8] González, P.C.; Velásquez, J.D. Characterization and detection of taxpayers with false invoices using data mining techniques. Expert Syst. Appl. **2013**, 40, 1427–1436. [**Google Scholar**] [**CrossRef**]

[9] Dias, A.; Pinto, C.; Batista, J.; Neves, E. Signaling tax evasion, financial ratios and cluster analysis. BIS Q. Rev. **2016**. [**Google Scholar**]

[10] Asha, R.B.; Suresh Kumar, K.R. Credit card fraud detection using Artificial Neural Networks. Glob. Transitions Proc. **2021**, 2, 35–41. [**Google Scholar**]

[11] Dangeti, P. Statistics for Machine Learning; Packt Publishing Ltd.: Birmingham, UK, 2017. [**Google Scholar**]

[12] Customer Interactions," Journal of Artificial Intelligence in Financial Services, vol. 18, no. 2, pp. 100-112, 2021.

[13] Neagoe, V.-E.; Ciotec, A.-D.; Cucu, G.-S. Deep convolutional neural networks versus multilayer perceptron for financial prediction. In Proceedings of the [12] 2018 International Conference on Communications (COMM), Bucharest, Romania, 14–16 June 2018; IEEE: Piscataway, NJ, USA, 2018. [**Google Scholar**]

[13] Tax Evasion Most Prevalent Financial Crime in Rwanda. Available online: **https://www.newtimes.co.rw/news/tax-evasion-most-prevalent-financial-crime-rwanda** (accessed on 25 August 2021).

[14] Zhou, Z.; Zheng, W.-S.; Hu, J.-F.; Xu, Y.; You, J. One-Pass Online Learning: A Local Approach; Elsevier: Amsterdam, The Netherlands, 2016. [**Google Scholar**]

[15] Heaton, J.; McElwee, S.; Fraley, J.; Cannady, J. Early Stabilizing Feature Importance for TensorFlow Deep Neural Networks; IEEE: Piscataway, NJ, USA, 2017. [**Google Scholar**]