International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Comparative Analysis of Artificial Neural Networks and Support Vector Machines in Predicting Money Laundering in Zimbabwean Commercial Banks: A Case Study of Banc ABC (Zimbabwe)

Tendayi Nzombe

Harare Institute of Technology, Department of Forensic Accounting & Auditing

Abstract

Money laundering and terrorist financing pose significant threats to the stability and integrity of financial institutions worldwide. Traditional rule-based Anti-Money Laundering (AML) systems are increasingly inadequate to detect complex and evolving financial crimes. This paper presents a comparative study on the application of Artificial Neural Networks (ANN) and Support Vector Machines (SVM) in detecting money laundering activities using transaction data from Banc ABC, a leading Zimbabwean commercial bank. Utilizing a dataset of over 87,000 transactions, the study evaluates the predictive accuracy, precision, recall, F1-score, and Area Under the Curve (AUC) of both models. Results indicate that SVM outperforms ANN with an AUC of 0.9982 compared to 0.753, while both models demonstrate high overall accuracy (~94%). Key risk indicators such as transaction amount, dormant account status, and political exposure are consistently identified as significant factors. The paper concludes with recommendations for integrating machine learning techniques into AML frameworks within Zimbabwe's banking sector to enhance detection efficiency and regulatory compliance.

Keywords: Money Laundering, Artificial Neural Networks, Support Vector Machines, Anti-Money Laundering, Machine Learning, Zimbabwe, Banc ABC, Financial Crime Detection

1. Introduction

Money laundering (ML) and terrorist financing (TF) continue to threaten financial institutions globally, with Zimbabwean banks facing similar challenges. Traditional AML systems based on static rule-based processes struggle to adapt to sophisticated laundering schemes, resulting in high false positive rates and missed detections (Zekos, 2021). This study investigates machine learning (ML) approaches—specifically Artificial Neural Networks (ANN) and Support Vector Machines (SVM)—to enhance the predictive capabilities of AML systems in Zimbabwe, focusing on Banc ABC.

2. Literature Review

2.1 Traditional Rule-Based AML Systems

Rule-based AML systems utilize predefined thresholds and expert-crafted rules to flag suspicious activities

but suffer from rigidity and high false positives (Ngai et al., 2011). They cannot dynamically adjust to evolving laundering methods, limiting their effectiveness (Kamani et al., 2021).

2.2 Machine Learning in AML Detection

Machine learning models can learn complex, non-linear patterns in transactional data, improving detection accuracy. ANN models, inspired by biological neural structures, excel at capturing intricate relationships, while SVMs optimize classification boundaries and handle high-dimensional data effectively (LeCun et al., 2015; Cortes & Vapnik, 1995).

2.3 Comparative Insights

ANNs offer flexibility but are often criticized for their black-box nature, complicating regulatory compliance. SVMs provide more interpretability and robustness but may require careful kernel and parameter tuning (Rudin, 2019). Ensemble approaches combining both models have been proposed to leverage their complementary strengths (Ngai et al., 2011).

3. Methodology

3.1 Data Collection and Preparation

Secondary data comprising 87,295 Banc ABC transactions from 2020 to 2024 were analyzed, including domestic and international transfers, RTGS, ZIPIT, and card payments. Variables included transaction amount, political exposure, account dormancy, and customer profile, with suspicious transaction status flagged via the FIU's GoAML system.

3.2 Data Preprocessing

Data cleaning involved handling missing values, normalization (min-max scaling to [0,1]), and categorical encoding. The dataset exhibited significant class imbalance, reflecting the rarity of confirmed suspicious transactions.

3.3 Model Development

Artificial Neural Network - A single hidden-layer neural network with seven neurons was trained using a logistic sigmoid activation function and backpropagation. Training used a 70:30 train-test split.

Support Vector Machine - A radial basis function (RBF) kernel SVM was optimized via grid search for hyperparameters (gamma and cost). Relevant features were selected using Wilk's Lambda F-test.

3.4 Model Evaluation

Models were evaluated using confusion matrices, accuracy, precision, recall, F1-score, and ROC-AUC metrics, with particular attention to the models' ability to detect the minority suspicious class.

4. Results

4.1 ANN Performance

- Training accuracy: 93.44%; testing accuracy: 93.80%
- Testing precision: 43.65%; recall: 89.23%; F1-score: 58.62%
- ROC-AUC: 0.753, indicating moderate discrimination power.

4.2 SVM Performance

- Training accuracy: 94.38%; testing accuracy: 94.01%
- Testing precision: 71.91%; recall: 72.56%; F1-score: 72.23%
- ROC-AUC: 0.9982, demonstrating excellent classification performance.

4.3 Key Predictors

Both models identified transaction amount, dormant account status, political exposure, KYC quality, and

customer classification as significant variables in detecting suspicious transactions.

5. Discussion

The superior ROC-AUC of the SVM highlights its robustness in handling imbalanced datasets and complex classification boundaries. While ANN provides valuable insights through Neural Interpretation Diagrams, its lower precision suggests the need for further tuning or ensemble approaches. Both models underscore the importance of high-value transactions and account dormancy as indicators of money laundering risk, aligning with FATF recommendations on customer due diligence and monitoring (FATF, 2023).

6. Conclusion and Recommendations

Machine learning models, particularly SVM, offer significant improvements over traditional AML systems in Zimbabwe's banking sector. Banks like Banc ABC should integrate these technologies to enhance real-time monitoring and reduce false positives, thereby optimizing compliance efforts.

Recommendations:

- **For Banks:** - Invest in machine learning infrastructure and data governance to improve AML detection. Combine AI models with human oversight for effective monitoring.
- **For Regulators: -** Encourage adoption of risk-based, technology-driven AML frameworks aligned with FATF standards. Strengthen data quality requirements.
- **For Researchers: -** Explore data augmentation and ensemble learning to address class imbalance and improve model precision.

Acknowledgements

The author acknowledges Banc ABC for providing access to transaction data and the Harare Institute of Technology for academic support.

References

1. Cortes, C., & Vapnik, V. (1995). Support-vector networks. 'Machine Learning', 20(3), 273–297.
2. FATF. (2023). (The FATF Recommendations). Paris: Financial Action Task Force.
3. Kamani, S., Azarnoush, H., & Alipour, A. (2021). Reducing false positives in AML systems using machine learning. (Journal of Financial Crime), 28(2), 423–439.
4. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. (Nature), 521(7553), 436–444.
5. Ngai, E., et al. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. (Decision Support Systems), 50(3), 559–569.
6. Rudin, C. (2019). Stop explaining black box machine learning models for high-stakes decisions and use interpretable models instead. (Nature Machine Intelligence), 1(5), 206–215.
7. Zekos, G. (2021). Anti-money laundering regulations and financial institutions. (Journal of Money Laundering Control), 24(2), 232–252.