A Suspicious Financial Transaction Detection Model Using Auto encoder and Risk-Based Approach

[1] Ms Renuka B N, [2] Ms Priyanka S

[1]Assistant Professor, Department of MCA, BIET, Davanagere, India
[2] Student, Department of MCA, BIET, Davanagere, India

ABSTRACT

This research addresses the identification of suspicious financial transactions within the increasingly complex and opaque landscape shaped by modern electronic financial technologies. It introduces a model designed to dynamically capture trends in diverse fund and transaction flows, with the capability to autonomously learn intricate transaction patterns. Central to this approach is the development of an internal control system based on a risk-focused methodology, which leverages auto encoders to strengthen anti-money laundering (AML) practices. This strategy demonstrates superior performance compared to conventional AML techniques. Furthermore, the model aids in identifying potential indicators of suspicious activity and supports the continuous refinement of alert systems within AML frameworks. This enables more efficient case analysis and reduces the need for exhaustive transaction reviews. Overall, the proposed model significantly enhances both the effectiveness and efficiency of AML operations, offering valuable insights for improving financial institutions' systems for evaluating and managing the risks associated with suspicious transactions.

***Keywords: Suspicious Transaction Detection, Anti-Money Laundering (AML), Auto encoder, Risk-Based Approach, Electronic Financial Transactions, Anomaly Detection, Internal Control System, Financial Fraud Prevention, Transaction Flow Analysis, AML Monitoring Systems*.**

1. INTRODUCTION

The rise of digital finance and electronic transactions has dramatically increased the complexity and volume of financial activities conducted globally. While these advancements have facilitated economic growth and efficiency, they have also introduced significant challenges related to money laundering and illicit fund transfers. Criminal entities often exploit opaque transaction patterns, shell accounts, and rapid digital fund movements to obscure the origins and destinations of illegal proceeds.

Consequently, financial institutions and regulatory bodies are under growing pressure to implement more intelligent and adaptive Anti-Money Laundering (AML) systems.

Traditional AML frameworks typically rely on rule-based or score-based systems, where pre-defined transaction thresholds and heuristic patterns are used to flag suspicious activities. While these systems are interpretable and relatively easy to implement, they are increasingly ineffective in the face of evolving money laundering techniques. They often fail to detect complex or novel suspicious behaviours, especially when those behaviours do not match historical data or pre-set rules. Additionally, these models are prone to high false-positive rates, leading to operational inefficiencies and a burden on compliance teams.

To overcome these limitations, the integration of machine learning and deep learning models into AML systems has become a promising direction. In particular, auto encoders a class of unsupervised deep neural networks—are gaining traction for their ability to model non-linear relationships and detect anomalies in high-dimensional data without requiring labelled inputs. When combined with a risk-based approach (RBA), which focuses on assessing the risk profile of each customer or transaction based on contextual factors, these systems can provide a more robust and dynamic mechanism for identifying potential threats.

This research introduces a novel framework that combines the strengths of auto encoder-based anomaly detection and risk-aware modelling to enhance the detection of mysterious or suspicious money transfers. The system is designed to autonomously learn from transaction data, identify unusual patterns, assess individual risk scores, and dynamically update internal AML alert models. By doing so, it not only reduces dependency on manually defined rules but also adapts more effectively to emerging money laundering schemes.

The proposed methodology addresses critical issues in existing AML systems and contributes toward building a more intelligent, efficient, and scalable fraud detection framework. This study also provides a pathway for integrating such models into real-world financial monitoring systems, ultimately strengthening the financial sector's resilience against illicit financial flows.

2. LITERATURE REVIEW

K. Singh and P. Best, Int. J. Accounting Inf. Syst., vol. 34, Sep. 2019, Art. no. 100418, "Anti-money laundering: Using data visualization to identify suspicious activity". The field of Anti-Money Laundering (AML) has increasingly adopted advanced technological methods to counter the challenges posed by modern financial crimes. Traditional AML systems, typically rule-based, are limited in their capacity to adapt to the evolving nature of money laundering techniques. These systems rely on predefined rules and thresholds, which are relatively easy to interpret and implement but often miss complex or novel patterns of suspicious behaviour.[1]

J. Whisker and M. E. Lokanan, J. Money Laundering Control, vol. 22, no. 1, pp. 158–172, Jan. 2019, "Anti-money laundering and counter-terrorist financing threats posed by mobile money". To address these limitations, researchers have explored the integration of Machine Learning (ML) techniques into AML systems. ML algorithms offer the advantage of learning from historical transaction data to detect patterns and anomalies that may indicate suspicious activities. However, the dynamic and large-scale nature of financial transactions continues to pose a significant challenge in building efficient and adaptive AML systems. Institutions often struggle to maintain the effectiveness of these systems as criminal methods evolve and transaction volumes grow.[2]

Z. Dobrowolski and Ł. Sułkowski, Sustainability, vol. 12, no. 1, p. 244, Dec. 2019, "Implementing a sustainable model for anti-money laundering in the united nations development goals". In recent years, the emergence of Deep Neural Networks (DNNs) has led to further innovation in AML research. Unlike traditional statistical approaches, DNNs are capable of identifying complex relationships within large datasets and improving the detection of non-obvious money laundering behaviours. Although DNN-based models demand extensive computational resources and labelled datasets for training, they significantly enhance the adaptability and performance of AML monitoring processes.[3]

A. S. M. Irwin, K. R. Choo, and L. Liu, J. Money Laundering Control, vol. 15, no. 1, pp. 85–111, Dec. 2011, "An analysis of money laundering and terrorism financing typologies". The Risk-Based Approach (RBA) has also gained prominence in AML frameworks. This method involves evaluating the potential risk associated with each transaction or customer, allowing financial institutions to prioritize cases based on severity and likelihood. RBA facilitates the establishment of a comprehensive risk assessment structure that includes customer verification, monitoring, internal controls, and compliance with legal regulations such as those from the KoFIU.[4]

J. Uthayakumar, T. Vengattaraman, and P. Dhavachelvan, J. King Saud Univ.-Comput. Inf. Sci., vol. 32, no. 6, pp. 647–657, Jul. 2020, “Swarm intelligence based classification rule induction (CRI) framework for qualitative and quantitative approach: An application of bankruptcy prediction and credit risk analysis”. Despite the progress, existing systems still encounter disadvantages, such as the lack of enhanced AML detection capabilities and the inability to autonomously adapt to new laundering techniques. Therefore, recent studies have turned towards unsupervised learning techniques, such as Auto encoders (AEs), which do not require labelled data and can model normal transaction patterns to identify outliers effectively.[5]

C. J. Lee and J. C. Lee, in Proc. Knowl. Sharing Program, KSP Modularization, 2013, pp. 38–42, “Experiences and methodology of Korea's anti-money laundering system deployment and development”. Combining DNNs and RBA with Auto encoder-based models offers a promising direction. These hybrid models can evaluate risk levels, identify suspicious transaction candidates, and update monitoring alerts dynamically. By leveraging these techniques, modern AML systems can achieve greater accuracy, flexibility, and efficiency, surpassing the capabilities of traditional models and better aligning with the needs of financial institutions in a fast-changing digital environment.[6]

3. EXISTING SYSTEM

The integration of a Risk-Based Approach (RBA) into anti-money laundering (AML) systems has enabled a more structured and systematic implementation of AML operations. Such a framework allows financial institutions to establish a comprehensive risk evaluation process that emphasizes prevention, centralized risk management, and department-specific responsibilities. Moreover, it meets the enhanced operational expectations set by regulatory authorities through various AML programs. These programs support key functions such as customer due diligence, suspicious transaction reporting (STR), currency transaction reporting (CTR), risk classification, and reporting compliance to regulatory bodies like the Korea Financial Intelligence Unit (KoFIU).

A critical component in this setup is internal control risk, which refers to the failure in implementing effective measures to mitigate money laundering (ML) and terrorist financing (TF), or to ensure adherence to legal and regulatory guidelines. This type of risk is categorized based on national financial reporting regulations and AML compliance standards, encompassing areas like customer verification, overall control, monitoring, and risk management.

As money laundering techniques evolve and become more complex, identifying illicit financial activities remains a significant challenge. Financial institutions are increasingly exploring machine learning (ML) techniques to enhance AML capabilities. Yet, constructing a reliable AML framework is difficult due to the vast volume of transactions and rapidly changing criminal patterns. Effective implementation of ML models requires alignment with the nature of the dataset being used. Consequently, comparative studies and analyses of various AML methodologies are vital to recognizing suspicious behaviours and detecting organized laundering efforts. Recent research emphasizes the importance of using hybrid or combined machine learning strategies, rather than relying solely on a single type of algorithm.

With the growth of deep neural networks (DNN), AML research has advanced significantly. While traditional models—such as rule-based or score-based systems—offer transparency and good performance with small datasets, DNN-based models provide improved detection accuracy through supervised learning techniques. These deep learning models can capture complex transaction patterns that traditional statistical methods often overlook.

Limitations of the Existing System

Current systems lack advanced AML techniques, particularly those utilizing cutting-edge machine learning or deep learning.

Although RBA frameworks support structured AML operations, they still fall short in handling dynamic transaction patterns and complex behaviours associated with modern money laundering schemes.

4. PROPOSED SYSTEM

This research introduces a novel approach aimed at understanding diverse and complex patterns of financial transactions in real time. The proposed system is designed to overcome the limitations of traditional rule-based AML frameworks by employing an **unsupervised deep learning model** that can autonomously learn intricate transaction behaviours without prior labelling.

The model incorporates two primary objectives. First, it employs an **auto encoder-based deep neural network (DNN)** that enhances the detection of suspicious transactions through internal control mechanisms. This not only improves upon existing rule-based AML systems but also significantly strengthens the RBA-driven risk assessment by incorporating preventive and departmental strategies into a cohesive structure.

Second, the model systematically calculates a **risk score for each customer** based on their transactional data. This score helps in identifying potential suspicious transaction candidates. Through simulation and model updates, the system continuously refines the alert mechanisms in the operational AML monitoring environment, enabling faster processing of flagged transactions and reducing the need for exhaustive manual reviews.

Advantages of the Proposed System

The system merges RBA principles with DNN algorithms, integrating internal control risk factors into a modern AML framework. During model validation using proof-of-concept (POC) data, the auto encoder emerged as the most effective unsupervised learning model.

The predictive framework is designed to generalize well, delivering high accuracy even for unseen data. This enhances the system's ability to adapt to evolving transaction patterns and identify new forms of suspicious activity.

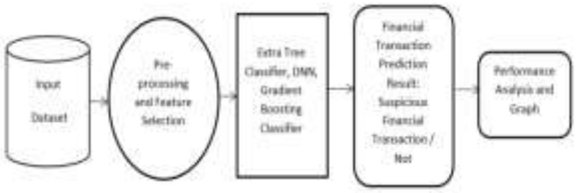
Input
Dataset
Pre-processing and Feature Selection
Extra Tree Classifier, DNN, Gradient Boosting Classifier
Financial Transaction Prediction Result: Suspicious Financial Transaction / Not
Performance Analysis and Graph

Figure 4.1 System Architecture

5. METHODOLOGY

The proposed system is designed with two primary modules: The Remote User module and the Service Provider module, each contributing to a seamless and intelligent anti-money laundering (AML) framework powered by deep learning and risk analysis.

The Remote User module serves as the interface for individuals or financial users who wish to evaluate the legitimacy of their financial transactions. Each user has access to a personalized User Profile, which contains their historical transaction data and behavioural patterns. Through the Prediction Page, users can input new transaction details to receive a prediction on whether the transaction appears suspicious or normal. The system, utilizing a trained Auto encoder model combined with a risk-based approach, evaluates the transaction in real time and provides immediate feedback. This enables users to make informed decisions and increases transparency in financial operations.

The Service Provider module operates as the backend intelligence and management layer of the system. It has administrative access to all users and their prediction results. This module is responsible for handling large-scale data, maintaining the database of transactions, and continuously updating the learning models. Through this module, the service provider can generate and visualize analytics via various graphs that depict trends in suspicious transactions, risk distributions, and detection performance. Additionally, the service provider is empowered to download the entire prediction dataset, which can be used for auditing, compliance checks, or retraining the model for enhanced accuracy. This module ensures that the AML system remains dynamic, interpretable, and aligned with institutional compliance standards.

Together, these modules create a cohesive ecosystem that not only automates the detection of suspicious financial transactions but also provides users and institutions with actionable insights to mitigate financial crimes effectively.

6. TECHNOLOGY USED

The implementation of the system involves the following tools and technologies:

6.1 Programming language

- **Python** – Core language for model development.
- **Django ORM** – Backend framework for managing transactions and risk assessment.
- **HTML, CSS, JavaScript** – Frontend technologies for user interface.

6.2 Machine Learning Libraries

- **TensorFlow & Keras** – Used for deep learning and autoencoder implementation.
- **Scikit-Learn** – Provides essential ML functions like feature scaling and anomaly detection.

6.3 Database Management

- **MySQL** – Relational database for storing transaction data.

6.4 Development Tools

- **Jupyter Notebook** – Used for model development and testing.
- **WAMP Server** – Supports database and backend services.

7. RESULT

The implementation of the proposed model, which combines an Auto encoder based deep neural network with a risk-based approach (RBA), demonstrated superior performance in detecting suspicious financial transactions. Compared to traditional rule-based and statistical methods, the new model was able to more accurately identify abnormal transaction patterns without requiring labelled data. By modelling the normal behaviour of transaction flows, the Auto encoder effectively isolated anomalies that indicate potential money laundering activity. The system also dynamically evaluated customer risk levels and updated alerts in real time, enabling swift and precise responses.

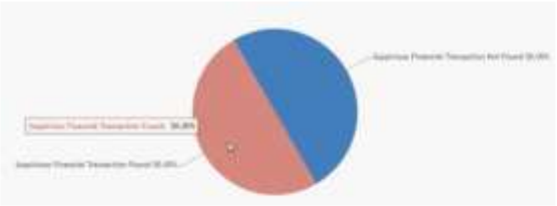

Figure 7.1 Pie Chart

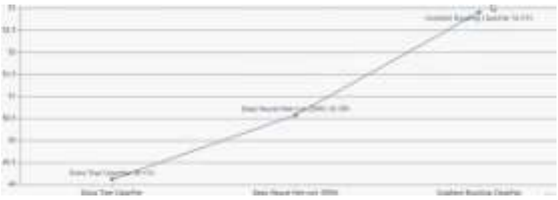

Figure 7.2 Visual Line Graph

Visual graphs and analytics further supported a clear interpretation of the results, providing transparency and actionable insights. Overall, the model significantly enhanced the accuracy, efficiency, and adaptability of AML operations.

8. CONCLUSION

In this study, a novel anti-money laundering (AML) model was developed by integrating an Auto encoder-based deep learning framework with a risk-based approach to enhance the detection of suspicious financial transactions. The proposed system successfully addressed the limitations of traditional rule-based AML methods by autonomously learning complex transaction patterns and evaluating Through unsupervised learning, the model identified anomalous activities with greater precision and adaptability, ensuring improved internal control and regulatory compliance. Additionally, the modular system design facilitated efficient user interaction, dynamic risk evaluation, and seamless prediction monitoring. The results confirm that the model not only improves detection accuracy but also streamlines AML operations, offering a scalable and intelligent solution for the evolving challenges in financial crime prevention.

9. REFERENCES

[1] “Anti-money laundering: Using data visualization to identify suspicious activity,” K. Singh and P. Best, Int. J. Accounting Inf. Syst., vol. 34, Sep. 2019, Art. no. 100418.

[2] “Anti-money laundering and counter-terrorist financing threats posed by mobile money,” J. Whisker and M. E. Lokanan, J. Money Laundering Control, vol. 22, no. 1, pp. 158–172, Jan. 2019.

[3] “Implementing a sustainable model for anti-money laundering in the united nations development goals,” Z. Dobrowolski and Ł. Sułkowski, Sustainability, vol. 12, no. 1, p. 244, Dec. 2019.

[4] “An analysis of money laundering and terrorism financing typologies,” A. S. M. Irwin, K. R. Choo, and L. Liu, J. Money Laundering Control, vol. 15, no. 1, pp. 85–111, Dec. 2011.

[5]“Swarm intelligence based classification rule induction (CRI) framework for qualitative and quantitative approach: An application of bankruptcy prediction and credit risk analysis,” J. Uthayakumar, T. Vengattaraman, and P. Dhavachelvan, J. King Saud Univ.-Comput. Inf. Sci., vol. 32, no. 6, pp. 647–657, Jul. 2020.

[6] “Experiences and methodology of Korea's anti-money laundering system deployment and development,” C. J. Lee and J. C. Lee, in Proc. Knowl. Sharing Program, KSP Modularization, 2013, pp. 38–42.

[7] “The dark side of anti-money laundering: Mitigating the unintended consequences of FATF standards,” G. Pavlidis, J. Econ. Criminol., vol. 2, Dec. 2023, Art. no. 100040.

[8] “Impact of the FATF recommendations and their implementation on financial inclusion: Insights from mutual evaluations and national risk assessments,” K. Celik, World Bank Group, USA, 2021.

[9] “Challenges of implementing an effective risk-based supervision on anti-money laundering and countering the financing of terrorism under the 2013 FATF methodology,” S. D. Jayasekara, J. Money Laundering Control, vol. 21, no. 4, pp. 601–615, Oct. 2018.