International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 12 ǁ December 2023 ǁ PP. 174-176

Advancement in Machine Learning reinforces Anti-Money Laundering Systems

Ritambhara Jha
jha.ritambhara@gmail.com

Abstract
In the ongoing battle against financial crime, anti-money laundering (AML) is a critical battleground. Conventional rule-based detection systems frequently fall behind the shifting strategies of money launderers. Governments throughout the world have engaged banks and financial institutions to assist with the identification and prevention of money laundering, which is a critical instrument in the battle to decrease crime and generate sustainable economic growth, which corresponds to Goal 16 of the United Nations Sustainable growth Goals. In this work, we look at how the technical and contextual affordances of machine learning algorithms might help these organizations achieve their goals. Machine learning (ML) is a promising alternative that uses complex algorithms to scan large datasets and find suspicious patterns that indicate money laundering activities. This research examines the major components, obstacles, and possible benefits of implementing ML models for AML detection.

Keywords *- Anti-Money Laundering, Fraud Detection, Anomaly Detection, Supervised Machine Learning Models, Graph Neural Network*

Date of Submission: 14-12-2023 Date of acceptance: 28-12-2023

I. Introduction

Anti-Money Laundering (AML) is defined as a system, legislation, laws, and policies that are used to regulate and combat money laundering activities and crimes.

The United Nations' best guess is that between $800 billion and $2 trillion get laundered every single year. This is to comprehend the magnitude and complexity that AML systems and professionals have to deal with on a regular basis. With technology that can sift through mountains of data.[2].

Anti-money laundering (AML) policies impose strict controls and surveillance on financial institutions. This is increasing the use of sophisticated analytics and data science tools for AML.

Machine learning for AML aids firms in identifying suspicious actions and prioritizing responses depending on the amount of perceived risk. As the machine learning model discovers, flags, and prioritizes instances, AML analysts step in to manually examine those alerts to make investigative choices, submit Suspicious Activity Reports (SARs) to stay compliant, and aid law enforcement teams in prosecuting economic offenders.

Related Work

Money launderers typically split illicit money into many portions and legitimate it through a series of modest banking transfers or business transactions. As a result, manually detecting money laundering operations is an extremely tough process[1]. Money launderers typically split illicit money into many portions and legitimate it through a series of modest banking transfers or business transactions. As a result, manually detecting money laundering operations is an extremely tough process.There are few limitations of rule based AML systems. When comparing real-time activity to predefined rules, many false positives are produced. With such a system, an AML analyst may receive hundreds of notifications every day for perfectly legitimate transactions. This is inefficient because analysts cannot get to the real instances, and it also makes genuine situations harder to identify because so many are given for assessment. Money launderers are continually changing the regulations. Analysts are constantly at a disadvantage since the AML system must be adjusted on a regular basis to reflect new criminal activities[2].

Dataset

Due to concerns about privacy, the law, and economic advantage, barely any financial transaction data is widely available. Besides the difficulties of obtaining genuine financial data with regard to laundering transactions, real data contains flaws that synthetic data can assist overcome. For instance, individual banks only observe their own transactions, not those of the numerous other institutions with whom their clients deal[4].

Real-world financial transaction data is highly restricted – for both proprietary and privacy concerns. Even when access is granted, it is difficult to assign the appropriate tag (laundering or genuine) to each transaction, as previously stated. These issues are avoided by IBM's synthetic transaction data for AML which is being used for the research[4].

Implementation

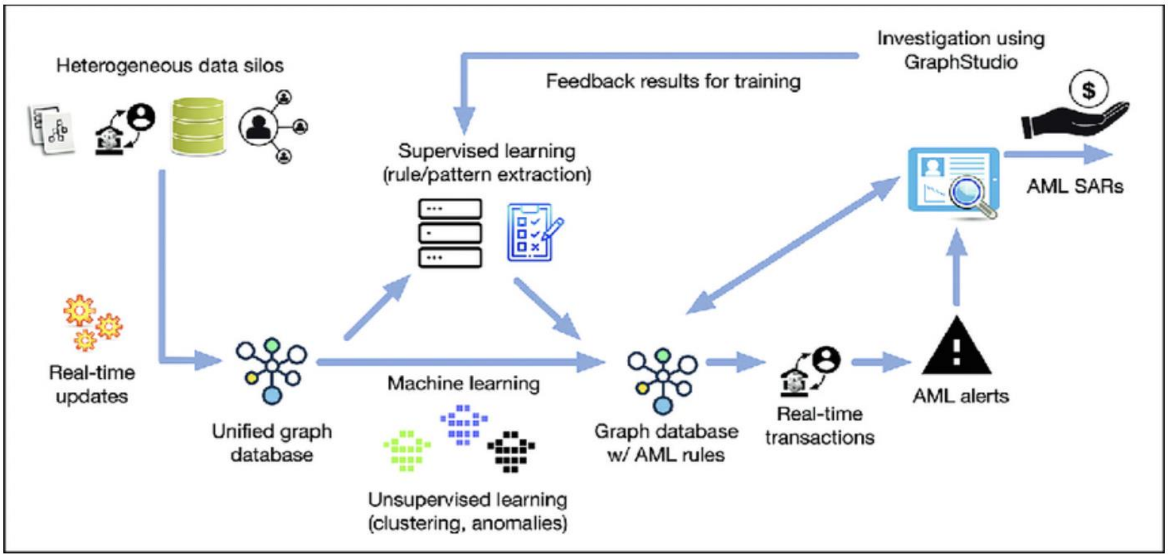

Fig.3 Anti-Money Laundering using Machine Learning[3]

Data Cleaning and Preprocessing

To gain understanding of the dataframe, extracting all accounts from the recipient and payer among all transactions was performed to sort the suspect accounts.In pre-processing step, Timestamp column is transformed by using Min-Max normalization.

Further, a unique ID is assigned to the account by concatenating the bank code and account number.

Similarly, smaller dataset with payment and receiver's information respectively.

LabelEncoder has been used to encode the object columns into classes.

Nodes and Edges features

Each node has aggregate the mean of amount paid and received with types of currency is the new features and node attributes are the bank code and mean of amount paid and received. Columns 'Timestamp', 'Amount Received', 'Receiving Currency', 'Amount Paid', 'Payment Currency' and 'Payment Format' are edge attributes, where each transaction are edges.

Model Creation & Result

Graph Neural Networks (GNNs) are a type of deep learning approach that performs inference on graph-described data. GNNs are neural networks that can be applied directly to graphs, making it simple to perform node-level, edge-level, and graph-level prediction tasks, which is being used in this case.

Once the model was trained and executed for 20 epoches, the average accuracy ranged between 96% - 97.3%

II. Conclusion & Future Work

Vital applications of machine learning models are making the AML systems robust and secure. This includes Risk Scoring, Predictive Analysis, Data Visualization, Network Analysis and Anomaly Detection.

1. Risk scoring is used to identify high-risk accounts and categories based on transaction data, client profiles, and prior behavior. Risk-based monitoring improves investigation allocation.
2. Predictive analytics, which employ hybrid models that combine rules, statistical modeling, and machine learning to estimate the likelihood of suspicious behavior.
3. Data visualizations and dashboards for examining patterns, trends, and outliers in massive transaction datasets. Human intelligence is supplemented by visual analytics.
4. Network analysis to discover relationships between entities and detect organized schemes. Fund transfers may be traced across complicated networks using link analysis, community recognition techniques,

and graph databases. ML models are used to detect anomalies in regular transaction patterns. Unsupervised learning methods like isolation forests and PCA assist in identifying aberrant outliers.

Machine learning has the ability to transform AML detection, allowing financial institutions to tackle money laundering in a more effective and efficient manner. Financial institutions may embrace the potential of ML to defend their systems and contribute to a cleaner financial ecosystem by carefully addressing data difficulties, selecting the correct tools, and adopting strong training and testing processes.

In this research, the core ML model was on GNN which provided great outcomes. In the future, we can focus more on other supervised learning models like Random Forest and Gradient Boost Models.

References

[1]. C. H. Tai and T. J. Kan, "Identifying Money Laundering Accounts", Proc. 2019 Int. Conf. Syst. Sci. Eng. ICSSE 2019, pp. 379-382, 2019

[2]. https://www.featurespace.com/newsroom/machine-learning-in-anti-money-laundering-aml-an-introductory-guide/

[3]. Hobart, Mark. (2020). The 'dark data' conundrum. Computer Fraud & Security. 2020. 13-16. 10.1016/S1361-3723(20)30075-0.

[4]. Realistic Synthetic Financial Transactions for Anti-Money Laundering Models, arXiv:2306.16424v2

[5]. Ana Isabel Canhoto,Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective, Journal of Business Research, Volume 131