Open Access
Gulf Journal of Advance Business Research
ISSN 3078-5294 (Online), ISSN 3078-5286 (Print)
FE Gulf Publishers.
https://fegulf.com

Machine learning and network analysis for financial crime detection: Mapping and identifying illicit transaction patterns in global black money transactions

Arifur Rahman[1], Pravakar Debnath[2], Adib Ahmed[3], Hossain Mohammad Dalim[4], Mitu Karmakar[5], Md Fakhrul Islam Sumon[6], & MD Azam Khan[7]

[1,4,5,6,7] School of Business, International American University, Los Angeles, California, USA
[2]School of Business, Westcliff University Irvine, California, USA
[3]Management science and quantitative research method, Gannon University, Erie, PA, USA

Volume No: 2 | Issue No: 6 | Page No: 250-272
Received: 20-08-24 | Accepted:25-10-24 | Published:11-12-24
Corresponding Author: Md Fakhrul Islam Sumon
Email: sumonf836@gmail.com
DOI: https://doi.org/10.51594/gjabr.v2i6.49

Abstract

The detection and prevention of malicious financial activities should be paramount for organizations in the US. Global economic integration, online banking, and increasing cases of cryptocurrency transactions have just increased the complexity of tracing illegal transactions. This research project examines the combined application and deployment of machine learning and network analysis in detecting black money transactions in the USA and globally. Machine learning and network analysis have emerged as a powerful mechanism in the fight against financial crime. Machine learning techniques, whereby systems learn through supervised and unsupervised learning, differ in that they can recognize patterns of financial data indicative of potentially fraudulent behavior. On the other hand, network analysis is one of the unique methods of detecting financial crimes, which derives power from presented relationships and interactions between sets of entities constituting transactional networks, such as people, companies, and accounts. This study used the Global Black Money Transactions dataset which revolved around financial transaction records involving unreported or illicit money, frequently for evading taxes, laundering money, or conducting illegal activities. Data come from financial institutions, government surveillance, whistleblowers, or investigations by the concerned law enforcement agencies. Rigorous data preprocessing steps were performed for the machine learning pipeline. In the current research project experiment, three machine learning algorithms were used: Logistic Regression, Random Forest, and XG-Boost. The performance indicators involved a set of standard metrics, including accuracy, precision, recall, F1 score, and AUC, which stands for Area Under the Curve. Despite lower accuracy, the XG-Boost algorithm was the best-performing algorithm. In terms of Precision, it correctly detected and predicted crimes, while the other models failed. Concerning the F1 Score, XG-Boost had the highest F1 score, balancing precision and recall. As per the AUC outcome, slightly better than Random Forest,

XG-Boost was more capable of distinguishing between crime and non-crime transactions.
Keywords: Black Money Transactions, Financial Crime, Machine Learning, Network Analysis, Mapping Illicit Transactions, XG-Boost, Random Forest, Logistic Regression.

INTRODUCTION

As per Alvarez-Jareno (2017), financial crimes, specifically those revolving around "black money" or illicit funds, represent a growing concern for financial institutions, governments, and regulatory bodies in the USA. Black money usually refers to unaccounted-for wealth earned through illegal activities, such as tax evasion, corruption, drug trafficking, and money laundering. In addition to public resource depletion, these unlawful financial activities destabilize economies, fund terrorism, and pose a threat to the integrity of the global financial system (Shawon et al., 2024). Every transaction is complicated and increasingly quicker, thanks to technology, making it much more difficult to find and try to prevent such cases of financial crimes. Filipkowski, (2023), indicates that on the global landscape, black money transactions ran into billions of dollars crossing borders yearly through shadowy and hidden channels. Traditional methods of financial oversight rely on inefficient manual auditing of select transactions and rule-based detection systems, which need to be revised against such sophisticated and fast-evolving financial threats.

Ivanyuk (2023), posits that the detection and prevention of malicious financial activities should be paramount for organizations in the US. In any case of laxity in these areas, the effect is to encourage other criminals and, as a whole, the regulatory bodies. Global economic integration, online banking, and increasing cases of cryptocurrency transactions have just increased the complexity of tracing illegal transactions (Buiya et al., 2024). Besides, it distorts the sources and recipients of criminal proceeds. In that light, sophisticated methods for detecting financial crime are necessary, particularly those that use data analytics, machine learning, and network analysis. These technologies enable an investigator to sift through large volumes of transactional data, identify suspicious patterns, and uncover associations between entities that otherwise would not typically be identified (Sumon et al., 2024).

According to Kurshan et al. (2020), machine learning and network analysis have emerged as a powerful mechanism in the fight against financial crime. Machine learning techniques, whereby systems learn through supervised and unsupervised learning, differ in that they can recognize patterns of financial data indicative of potentially fraudulent behavior. After learning from past data, these models predict future illicit activities and can change as criminal tactics do. Filipkowski (2023), argues that while network analysis provides a visual and mathematical framework to understand the structure of relationships among distinct transaction entities, mapping transaction networks helps analysts identify suspicious behavior groupings, money laundering rings, and hidden relationships between criminal actors. The combination of these tools represents state-of-the-art financial crime detection, going beyond traditional methods (Islam et al., 2024).

This research project aims to examine the combined application and deployment of machine learning and network analysis in the detection of black money transactions on a global scale. In this research project, the main objective will be to seek the mapping and detection of illicit financial activity patterns through transaction network analysis by applying machine learning models that flag suspicious activities. It will involve an investigation into the methodologies

adopted in both fields, a review of successful case studies, and a review of the challenges and limitations of the technologies involved in the fight against financial crimes. Through this rigorous investigation, the research aims to contribute to curating more robust and resilient systems for financial oversight, capable of detecting and preventing the flow of black money in an increasingly digital and interconnected world.

LITERATURE REVIEW

Overview of the Existing Research into the Detection of Financial Crime

Potla(2023), contends that financial crime detection has garnered substantial attention from scholars, organizational psychologists, and industry researchers over the past few decades. With the escalating sophistication of global economic systems, traditional mainstream methods such as rule-based detection, manual auditing, and statistical analysis still need to be improved in identifying illicit financial activities. Consequently, recently, the focus of research has changed towards using advanced technologies involving Machine Learning and network analysis to detect and prevent economic crimes, with a special consideration of anti-money laundering, fraud, and terrorist financing (Sumon et al., 2024).

Al Mukaddim et al. (2024), reported the Financial Action Task Force (FATF), an intergovernmental institution, has provided a unified global framework for combating financial crimes through recommendations and guidelines. Much research has tried to understand how financial criminals exploit vulnerabilities in the economic system, such as using shell companies, offshore accounts, and layering techniques to obscure illegal activities [Nicholls et al., 2021]. Early detection models relied on predefined rules and thresholds flagging suspicious activities. These systems often produce many false positives due to their weaknesses in adapting to evolving criminal strategies (Shil et al., 2024).

According to Shawon et al. (2024), in response to the shortcomings of rule-based systems, scholars and organizational psychologists started examining the application of artificial intelligence (AI) and machine learning to enhance the accuracy and efficiency of financial crime detection. These algorithms have exemplified excellent capability in handling vast amounts of data and identifying complex patterns that traditional models struggle to detect [Nicholls et al., 2021]. Besides, network analysis has emerged as a forceful tool for understanding the relation and interaction of various entities in financial networks, thus allowing an inclusive approach to criminal behavior detection. Therefore, combining machine learning with network analysis forms a natural development in the area since it offers novel ways of combating financial crime (Khan et al., 2024).

Machine Learning Techniques in the Detection of Crimes Involving Finance

Palmeiro (2021), postulated that over the past decade, deploying machine learning (ML) methods in financial crime detection has captured substantial attention from researchers and financial institutions. Correspondingly, empirical studies in this domain have examined various machine learning models to enhance the identification of illicit activities, such as money laundering, fraud, and terrorist financing. The traditional methods for detection using a rule-based system have proven grossly inadequate, given the large volumes of financial transactions and their complexity. This research project looks at major empirical studies on the effectiveness and limitations of machine learning in detecting financial crime(Islam 2023a).

Krysovatyy et al. (2021) deployed Decision Trees and Random Forest classifiers to detect fraudulent activities in financial statements in New York. The researcher analyzed publicly available economic data and created models identifying fraud activities, where random forests performed better than decision trees. Their findings highlighted the usefulness of ensembling methods when striving for high detection rates, considering the data's complexity and high-dimensional nature(Alam et al 2023).

Kumar et al. (2022) applied cost-sensitive learning via random forests for credit card fraud detection in Pennsylvania. The model embedded discrimination between the financial cost of false positives and false negatives—a feature significant for business usage. They showed that with the use of cost-sensitive learning techniques, the overall cost of fraud can be considerably reduced, thus making ML models highly accurate and economically viable for financial institutions.

Potla (2023), applied unsupervised clustering to highlight money laundering activities in financial transaction networks in the Bank of America. The introduction of k-means clustering in their respective study revealed groups of similar transactions that assisted in finding suspicious outliers. Empirical results indicated that clustering methods could detect potentially suspicious transactions that may go undetected by applying traditional rule-based systems.

Rouholahhi [2023], furthered their exploration by incorporating anomaly detection into deep learning models. They designed an autoencoder-based model to detect anomalies in credit card transactions. It was trained using only average behavior data so that deviations from normal behavior could be identified. The approach flagged suspicious transactions in an imbalanced dataset when fraud was relatively rare. Their work focused on the powers of autoencoders, using deep learning methods to uncover subtle patterns that might prove elusive to rule-based systems or traditional machine-learning models (Nasiruddin et al. 2023).

Hybrid methods have also been attempted, with combined techniques yielding encouraging results. In particular, Palmeiro (2021), explored hybrid models for detecting fraudulent credit card transactions by combining decision trees and artificial neural networks. Their results indicated that the latter approach did better than either model since these models become more interpretable due to the decision tree component. At the same time, the neural network adds pattern recognition capabilities (Rahman et al., 2024).

Ivanuk (2023), developed an ensemble model that consolidated logistic regression, decision trees, and gradient boosting machines (GBMs) to pinpoint money laundering activities in a large dataset. Their proposed ensemble model outperforms lower-order single models by attaining high accuracy with reduced false favorable rates. This confirms that combining diverse learning approaches may improve overall performance (Buiya et al., 2023).

Network Analysis in Financial Crimes Detection

Filipkowski (2023), asserts that Network analysis is one of the unique methods of detecting financial crimes, which derives power from presented relationships and interactions between sets of entities constituting transactional networks, such as people, companies, and accounts. This technique aims to identify the very structure of a financial network to locate suspicious patterns, such as building rings that launder money and move it, aided by several intermediaries, to camouflage its source. Graph theory, intrinsic to network analysis, represents entities as nodes and financial transactions between the entities as edges linking the nodes. The network's

topology can be analyzed to identify essential nodes and assess the flow of funds across the network. Centrality, clustering coefficients, and other metrics could expose how striking some entities are in the network, emphasizing possible bottlenecks or choke points at which illicit activities may be classed (Islam 2023b).

Currently, community detection algorithms are used to identify suspicious activity clusters. These community detection algorithms group the nodes into strongly connected communities, which may reflect criminal networks. One example can be money laundering schemes in which funds travel within a small community of accounts before being moved to a less suspicious destination (Jofre, 2023). By mapping these communities, network analysis allows investigators to follow through on the movement of funds to reveal hidden connections among apparently unrelated entities.

Temporal network analysis takes this further by examining how financial networks change over time. Felons use various techniques, including "layering," which segments large amounts of illicit money into smaller, less suspicious transactions across multiple accounts and jurisdictions. In a temporal analysis, investigators could follow the evolution of these transactions and find patterns of behavior over time that identify when funds are moving in coordination.

Kresz [2020], argues that While network analysis has proven very effective in identifying suspicious transaction patterns, it has limitations. One of the most severe concerns is the scale and complexity of the financial networks themselves-sometimes involving millions of transactions between thousands of entities. Analyzing such large datasets requires significant computational resources and sophisticated algorithms that can process them effectively. Secondly, many network analyses require access to substantial volumes of transactional-level data that may not.

Gaps and Limitations in Current Research

Liotta, G. (2022), posited that several gaps and limitations exist in state-of-the-art research on machine learning and network analysis for detecting financial crimes. The first significant gap is data privacy and access to valuable, labeled data. In most cases, financial institutions do not provide transactional data in great detail because they are sensitive to confidentiality, making it difficult for researchers to train and validate their models. Also, most of the data available for research has been anonymized or aggregated, making the efficiency with which machine learning models can identify specific kinds of illicit activities not as good.

Potla (2023), pointed out that another area for improvement in the research is interpretability in many machine learning models. Although deep neural networks and ensemble methods are among the models offering high predictive accuracy, their complexity makes them black boxes. Lack of transparency further complicates this since explaining these financial crime investigations. As described, AI techniques are increasingly required, and techniques are needed that will provide insight into how these models make their predictions while sustaining high levels of accuracy.

The final gap is in the research on integrating machine learning with network analysis. While both methods have been applied independently with excellent outcomes, more studies have yet to be conducted on how they could be combined to develop even more powerful and inclusive systems for detecting financial crimes (Jofre, 2023). Integrating these two approaches would allow a more holistic view of illicit economic activities. It could enable identifying individual

suspicious transactions and their embedding within more extensive criminal networks. While much progress has been made in machine learning and network analysis for financial crime detection, many challenges remain. Overcoming these challenges requires collaboration between researchers, financial institutions, and regulatory bodies and continued innovation in developing new technologies (Jofre, 2023).

DATA DESCRIPTION

The Global Black Money Transactions dataset was simulated from Waqi (2024), for the current research project. This comprehensive dataset provided a detailed view of black money transactions across multiple nations. The dataset was tailored to provide insights into distinct components of financial movements frequently related to illicit activities. With extensive attributes ranging from transaction amounts to risk scores, this dataset served as a valuable resource for comprehending the intricacies of financial irregularities. Data came from financial institutions, government surveillance, whistleblowers, or investigations by the concerned law enforcement agencies (Waqi, 2024). This dataset is helpful for researchers, policy-makers, and financial institutions in lessening the understanding of money laundering and other forms of economic crimes. It generally consists of many transaction records that may be analyzed to properly detect anomalies and suspicious activities. In addition to the global black money transaction dataset, this study also simulated the National Court Register data to support this manuscript from previously reported studies by (Filipkowski, 2023). The register comprises most of all a register of business entities, a register of associations, other social and professional organizations, foundations, independent public health care institutions, and a register of insolvent debtors (Art. 1 (2) of the Act). This scope is very interesting from the point of view of an analyst as it makes it possible to search for ties not only in the private business sector, but also in the non-governmental sector.

Table 1

Showcases the Key Attributes and Features of the Dataset

Feature	Description
Transaction ID	Unique identifier for each transaction.
Country	The country where the transaction took place.
Amount (USD)	The transaction amount is in USD.
Transaction type	Type of the transaction (e.g., deposit, withdrawal, transfer).
Date of Transaction	The date the transaction occurred.
Person Involved	The individual or entity associated with the transaction.
Industry	The industry involved in the transaction.
Destination Country	The destination country of the money involved.
Reported by Authority	Whether an authority flagged the transaction.
Source of money	Where the funds originated.
Money Laundering Risk Score	A score indicating the risk of money laundering associated with the transaction.
Shell companies involved	Whether shell companies were involved in the transaction.
Financial institution	The institution where the transaction took place.
Tax Haven country	Whether the destination is a known tax haven.

Data Preprocessing and Cleaning Methods

Data preprocessing encompassed handling missing values by identifying and addressing any missing data points by removing them or imputing values based on statistical methods. Data Normalization entailed scaling numerical values in a standard range so that no particular attribute

dominantly affects the analysis. Outlier Detection included the identification and management of outliers that may affect results. It was essential in financial datasets, where extreme values can signal fraud. Encoding Categorical Variables involves converting categorical data into a numerical format using one-hot or label encoding techniques in preparation for analysis [Pro-AI-Robikul, 2024]. These preprocessing and cleaning steps were vital for affirming the dataset's quality and improving the performance of any machine learning models applied to it.

METHODOLOGY

Data Pre-Processing

Rigorous data preprocessing steps were performed for the machine learning pipeline. Initially, the analyst converted the 'Date of Transaction' column to a date-time format. The analyst proceeded with feature encoding using Label Encoding to convert categorical features into numerical ones since most machine learning algorithms require numerical input. In the code, encoding across multiple categorical columns such as 'Country,' 'Transaction Type,' and more have been applied. It subsequently extracted further features from the transaction date by adding columns to account for the year, month, and day separately. Feature engineering, at this point, could capture temporal patterns in this data much better. The researcher then dropped the original columns of 'Date of Transaction' and 'Transaction ID' since they were likely no longer needed or might introduce noise into the model [Pro-AI-Robikul, 2024]. Splitting the data into training (80%) and testing (20%) sets allowed for an unbiased evaluation of the model's performance on unseen data. These steps are performed in preparation, in concert, ready the data for analyses and modeling by standardizing the data type, encoding categorical variables as numeric, extracting valuable features, and rejecting superfluous information.

Machine Learning Technique Deployed

In the current research project experiment, three machine learning algorithms were used: Logistic Regression, Random Forest, and XG-Boost. Logistic regression is a statistical model that generates the probability of one of two possible outcomes for one or more predictor variables. It is applied when simplicity with interpretability is desired. In contrast, the Random Forest is an ensemble learning model that trains a large set of trees and provides the mode of the predictions of the decision trees [Pro-AI-Robikul, 2024]. This model has inherent resistance to overfitting and can handle big datasets with a higher number of dimensions. On the other hand, XGBoost is an ensemble technique using the gradient boosting framework. It is widely known for its speed and performance on many problems out of the box, especially on sparse data, besides regularization preventing overfitting.

a) Model Training and Validation Processes

This protocol revolved around training and model validation based on a dataset split into training and testing subsets. Notably, the analyst set to fit the model and the testing set to evaluate the performance. Cross-validation, a method widely used to ensure that the model generalizes well to new unseen data, involves k-fold cross-validation. One of the crucial processes involved in cross-validation is that it helped tune the hyperparameters for better selection of the best model configuration [Pro-AI-Robikul, 2024]. While training is finding the pattern within data, validation shows how the model performs on new, unseen data during the development or training process. Hence, validation gives a glimpse of the predictive capability of the model.

b) Performance Metrics

The performance indicators involved a set of standard metrics, including accuracy, precision, recall, F1 score, and AUC, which stands for Area Under the Curve. Accuracy is the proportion of correctly predicted instances out of total cases. Precision refers to the ratio of true positives among the total positives that have been expected, showing the model's capability to avoid false positives. Recall, or Sensitivity, measures the ratio between true positives and actual positives, calculating how much interest rate the model captured. The F1 Score is the harmonic average of precision and recall, balancing the two quantities [Pro-AI-Robikul, 2024]. Last but not least, AUC measures the capability of the model to separate classes at all classification thresholds. The model with the higher AUC is the better-performing model.

Network Analysis Technique

Jofre (2023), contends that network analysis techniques range from constructing a network through transaction data, where entities might be individuals, organizations, or accounts represented as nodes, to transactions between them as edges. This graphical representation depicts the relationships and interactions within a dataset for analytical exploration. In such a network, every transaction can be considered a directed edge from the sender's node to that of the receiver, trace-like money flows. When these flows are drawn together, an entire network could show the structure and dynamics of the financial interactions. Once the network is built, it can be analyzed to find patterns of behavior, identify clusters of activity, and detect anomalies that will most likely spell illicit activities such as money laundering or fraud.

Krész (2020), holds that pinpointing critical connections and players within the constructed network is pivotal for understanding the influence and roles of different entities. There are various techniques through which this can be done; centrality measures are among the most useful. Centrality measures quantify the importance of a node within the network by its position and connections. Degree centrality counts the number of direct connections a node has possibly understood as its immediate influence. Betweenness centrality measures the frequency with which a given node is a bridge along the shortest path between any other two nodes; this type of centrality points to the node's potential to facilitate communication or transactions. Similarly, closeness centrality measures the efficiency of a node in reaching all other nodes within the network. These techniques enable researchers to denote vital influential players in a network with extensive control or significant influence. This is very helpful in applications related to financial crime.

Network Analysis Metrics

Liotta (2022), articulated that several metrics are employed to analyze the network effectively, each indicating different structure and dynamics dimensions. Centrality measures are among the most fundamental methods for detecting influential nodes and their exact roles within the network. Community detection algorithms beyond centrality have been applied to find the clusters or groups of nodes more connected to each other than the rest of the network. This might hint at latent relationships or subgroups engaging in coordinated activities. Other necessary measures are described by density, which denotes the ratio between the actual and maximum number of links in a network, and the diameter, understood as the longest shortest path between any pairs, reflecting the overall connectivity of the network. Working from these metrics,

analysts can pick up from the deeper structure of the network, identify areas of potential vulnerability, and inform strategies of intervention or further investigation (Zeeshan et al., 2024).

IMPLEMENTATION

Exploratory Data Analysis

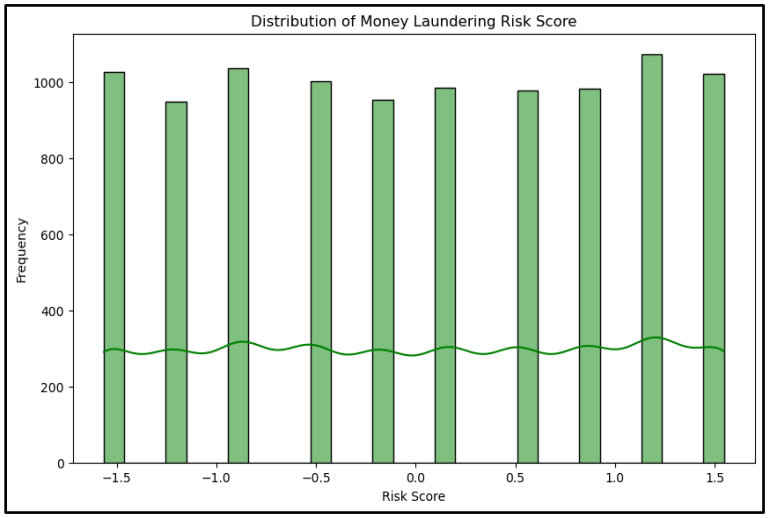

Figure 1: Displays the Distribution of Money Laundering Risk Score

The graph above represents the distribution of Money Laundering Risk Scores across a dataset of transactions or entities. The distribution appeared approximately normal or Gaussian, with a slight rightward skew. The risk scores ranged from about -1.5 to 1.5, centered at 0. The peak in the distribution was very close to 0, suggesting that for most entities or transactions, the nominal value of the risk score should be neutral. It was apparent that the standard deviation was relatively high, indicating that the scores for risk spread well. There was an explicit mode, at 1.5 points, for the score of risk, and a first glance at this signifies the highest frequency.

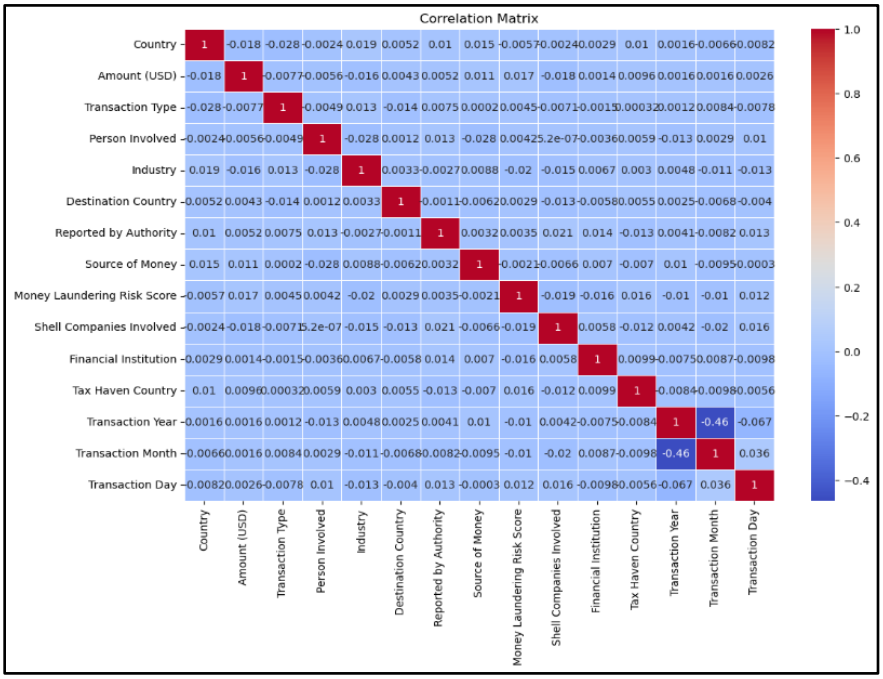

Figure 2: Exhibits the Correlation Heatmap between Various Factors in the Dataset

The correlation heatmap above displays the relationships between various factors and the money laundering risk score. A positive correlation implies that an increase in the value of one factor

increases the risk score, while a negative one postulates otherwise. Key findings ascertained a correlation between transaction type and the risk score, demonstrating that there was a particular type of transaction most indicative of money laundering. Moreover, the correlation between countries and industries and risk scores was significant. On the other hand, modality factors, such as the day or month of the transaction, can be fragile and correlated with the risk score. Overall, this correlation matrix underlines multi-factor dependencies of money laundering risk and gives essential insights into how to assess and prevent the risk factor.

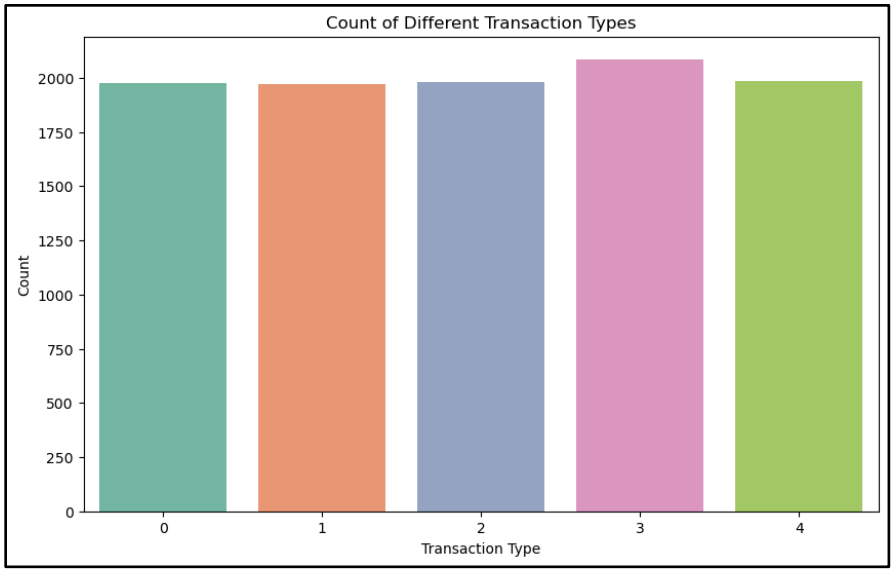

Figure 3: Displays a Histogram Distribution of different Transaction Types

The above histogram visualizes the distribution of transaction types in a dataset. It is easily noticed that the distribution of transaction types is relatively well-balanced. The visualization unveiled a relatively balanced distribution, with transaction types 0, 1, 2, 3, and 4 having similar counts. This indicates that the dataset contained diverse transaction types, with no dominant category observed.

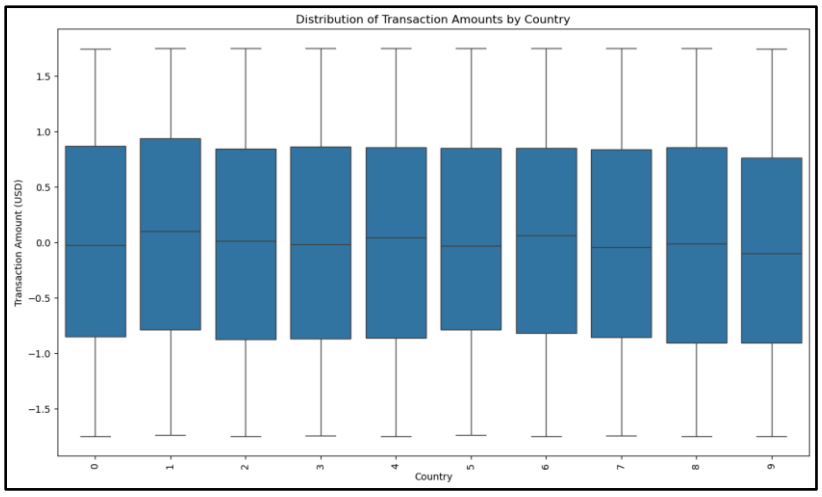

Figure 4: Showcases Box Plot Distribution of Transaction Amounts by Country

This boxplot depicts the distribution of transaction amounts across countries. The x-axis is the country, and the y-axis is the transaction amount in USD standardized on a scale from -1.5 to 1.5. Most countries are at an approximate median transaction amount of 0, which could indicate

that most of the transactions in those countries are close to the average. In a few countries, though, it is closest to either just above or below 0, indicating somewhat higher or lower transaction amounts. The boxes representing the IQR vary between countries. Some countries have a relatively small IQR, suggesting the transaction amounts are relatively close. Other countries have much larger IQRs, indicating a much larger spread of values.

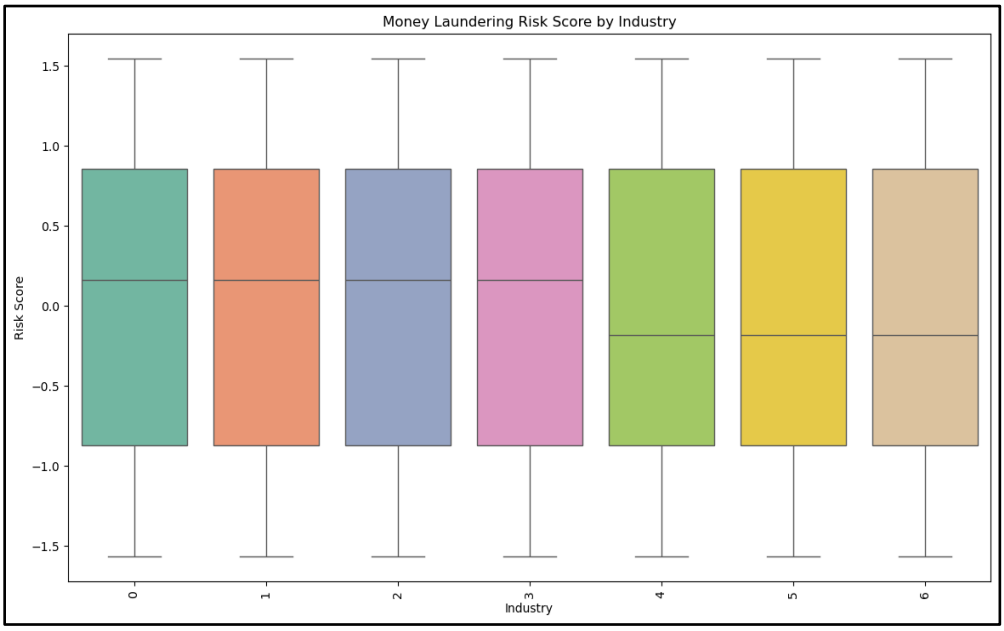

Figure 5:Portrays Money Laundering Risk Score by Industry

As depicted above, while some general trends emerge, there are also some striking variations in the distribution of risk scores across industries. Some have a higher medium risk score, while others have values scattered across a broader range. These variations collateralize the view that industry-specific influencing factors affect the possibility of money laundering.

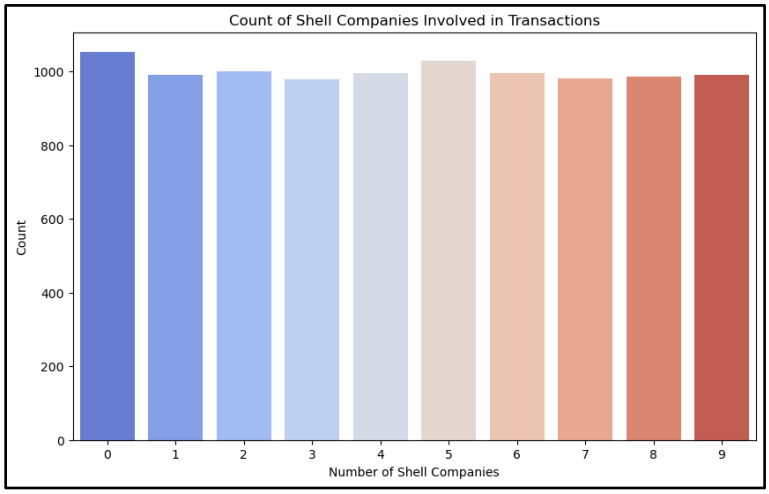

Figure 6: Exhibits Count of Shell Companies Involved in Transactions

This bar chart illustrates the distribution of the number of shell companies involved in transactions. The x-axis represents the number of shell companies, ranging from 0 to 9, and the y-axis gives the transaction count for each number of shell companies involved. The highest number corresponds to transactions with five shell companies, which shows that several

transactions involve a shell company. While the number of shell companies increases, the number of transactions generally goes down. This implies that the more shell companies linked to a transaction, the less frequent it is.

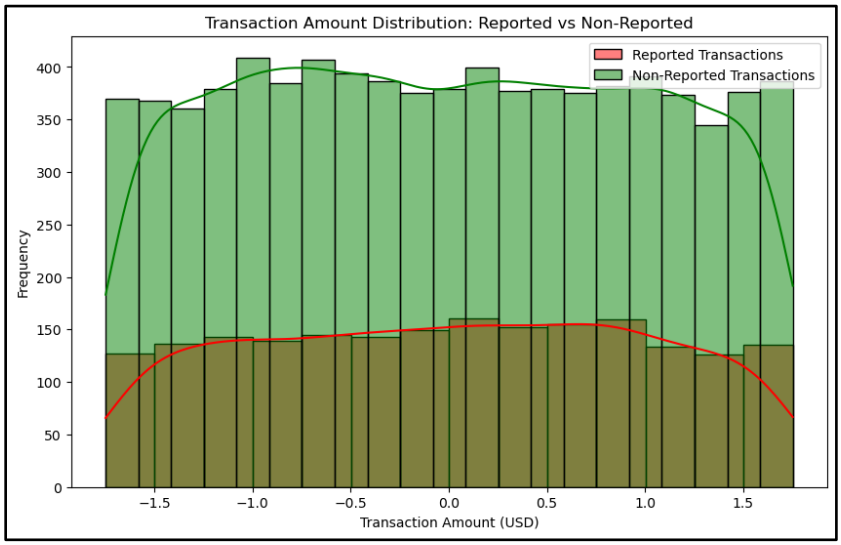

Figure 7: Showcases Transaction Amount Distribution: Reported vs. Non-Reported

While the overall distributions are very similar, there are some apparent differences between reported and non-reported transactions: The frequency count of the reported transaction was higher than that of the non-reported transaction for most of the transaction amount bins. This may indicate that the overall proportion of transactions is reported compared to the non-reported. Within the lower transaction amount range, between -1.5 and -0.5, the frequency of reported transactions is significantly higher than that of non-reported transactions. This implies that smaller transactions are more likely to be reported. For the higher ranges of transaction amount, within the range 0.5-1.5, the frequency of transactions reported is just slightly less than that of transactions not reported. This would, therefore, imply that more significant transactions are more likely not to be reported.

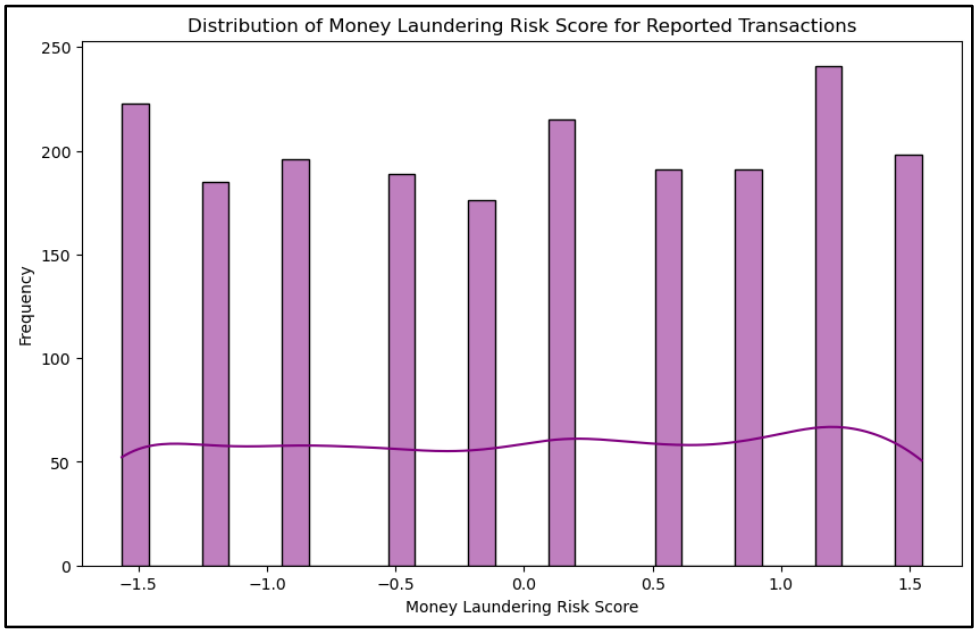

Figure 8: Displays Distribution of Money Laundering Risk Score for Reported Transactions

The graph above suggests that most reported transactions had a low or moderate risk of money laundering, but a few high-risk transactions skew the distribution. The leptokurtic shape indicates a greater chance of observing extreme values than a Norma distribution. The standard deviation is high, with a wide dispersion range covering all the risk scores. There is also a transparent mode at 1.5, indicating this is the most common of all the risk scores for reported transactions.

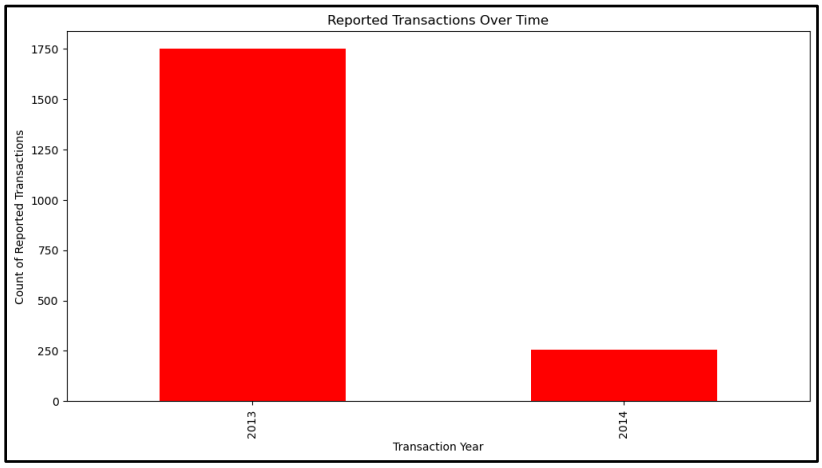

Figure 9: Portrays Reported Transactions Between 2013-2014

The bar chart represents the number of transactions reported between 2013 and 2014. The number of reported transactions for 2013 is much higher than in 2014, implying a tight increase in the number of transactions reported in 2013. The sharp decline in 2014: Comparatively, the number of reported transactions for 2014 faced an abrupt decline compared to the previous year. This means a decrease in the number of transactions declared during 2014.

Steps for Constructing and Analyzing the Transaction Network

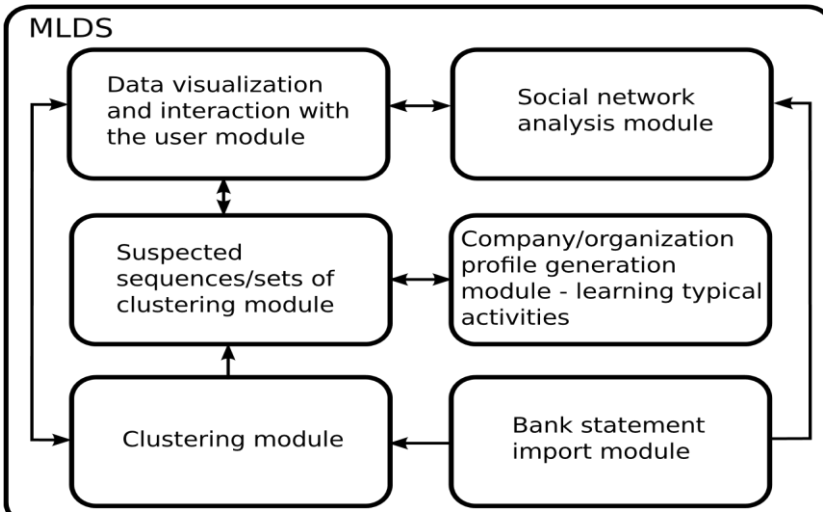

Figure 10: Exhibits the Proposed Network System for Mapping Illicit Transaction

The importing module provides data in a format the system understands; the data come from disk files and the Web.

Clustering Module: The system constructs clusters from data provided by the importer based on some clustering algorithms.

Suspected sequences/sets: The clustering module frequently performs pattern mining on the data provided by the clustering algorithms.

Generating the Company/Organization Profiles Module: This module generates profiles of suspected organizations/companies based on their typical operations and the amount of money usually transferred.

Social network analysis module, that, having imported data, builds social networks and then conducts a network analysis, such as:

- Designating roles to nodes,
- Assessing connections and associations between roles,
- Pinpointing proximity among entities.
- Comparing and contrasting roles designated to nodes within networks from various domains, e.g., bank accounts, National Court Register.

Data visualization and user interaction: This module visualizes the resultant data on schema and timeline diagrams.

RESULTS

Performance Comparison of Machine Learning Models

Logistic Regression

Table 2

Displays Showcases the Logistic Regression Model Training

```
# Logistic Regression Model
log_reg = LogisticRegression()
log_reg.fit(X_train, y_train)

# Predictions and Evaluation
y_pred_log = log_reg.predict(X_test)
print("Logistic Regression Classification Report:")
print(classification_report(y_test, y_pred_log))

# Confusion Matrix
conf_matrix = confusion_matrix(y_test, y_pred_log)
sns.heatmap(conf_matrix, annot=True, fmt='d', cmap='Blues')
plt.title('Logistic Regression - Confusion Matrix')
plt.show()
```

The logistic regression line imported the Logistic Regression class from the sci-kit-learn library, which was used to create and train the model. classification_report code Imported the classification_report function from the sci-kit-learn library, which evaluated the model's performance. Subsequently, the confusion_matrix line Imported the confusion_matrix function from the sci-kit-learn library, which was used to generate a confusion matrix for the model's predictions. Sns. Heat map line Imported the seaborn library, which was used for data visualization, explicitly creating heatmaps. matplotlib—pyplot library, was used for general plotting purposes.

Table 3
Displays the Logistic Regression Report

Logistic Regression Classification Report:

	precision	recall	f1-score	support
False	0.80	1.00	0.89	1602
True	0.00	0.00	0.00	398
accuracy			0.80	2000
macro avg	0.40	0.50	0.44	2000
weighted avg	0.64	0.80	0.71	2000

Above is the output of a logistic regression model on certain binary classifications. The model's performance is average over its "True" class, with a recall value of 0.00 and an F1-score of 0.00. However, it performed well in the "False" class with a high precision score of 0.80, as revealed by the Classification report. It struggled to identify instances related to the class "True correctly." This fact is further supported by the confusion matrix below, where all "True" instances were misclassified as "False." The accuracy metric measured the model's overall accuracy, which was 0.40 in this case, indicating that 40% of the instances were correctly classified.

Random Forest

Table 4
Portrays the Random Forest Training

```
# Random Forest Model
rf = RandomForestClassifier(random_state=42)
rf.fit(X_train, y_train)

# Predictions and Evaluation
y_pred_rf = rf.predict(X_test)
print("Random Forest Classification Report:")
print(classification_report(y_test, y_pred_rf))

# Confusion Matrix
conf_matrix_rf = confusion_matrix(y_test, y_pred_rf)
sns.heatmap(conf_matrix_rf, annot=True, fmt='d', cmap='Blues')
plt.title('Random Forest - Confusion Matrix')
plt.show()

# Feature Importance
importances = rf.feature_importances_
indices = np.argsort(importances)[::-1]

plt.figure(figsize=(12, 8))
sns.barplot(x=X.columns[indices], y=importances[indices])
plt.title('Feature Importance - Random Forest')
plt.xticks(rotation=90)
plt.show()
```

The code snippet above shows a random forest classifier applied to a binary classification task. In the code above, a random forest classifier with a random state of 42 was instantiated before training the training data, X_train and y_train, and making a prediction on the test data, X_test. The classification report summarized the model's performance using precision, recall, F1-score, and accuracy. The confusion matrix visualized the classification decisions of the model, including correct and incorrect predictions. Also, the feature importance plot showed the most influencing features considered by the model for deciding. Consequently, the code is performed by an elaborative analysis of the randomness of the forest model in classifying the given dataset.

Table 5

Depicts the Random Forest Classification Report

Random Forest Classification Report:

	precision	recall	f1-score	support
False	0.80	1.00	0.89	1602
True	0.00	0.00	0.00	398
accuracy			0.80	2000
macro avg	0.40	0.50	0.44	2000
weighted avg	0.64	0.80	0.71	2000

The outcome for the Random Forest, Precision for the False class, was 0.80, meaning 80% of predicted False instances were False. Regarding Recall: For the False class, it was 1.00, meaning the model correctly identified all actual False instances. F1-score: For the False class, the result was 0.89, a harmonic mean of precision and recall. There were 1602 instances of the False class and 398 of the True class, totaling 2000 instances. The overall accuracy is 0.80, meaning 80% of all predictions were correct.

XGBoost

Table 6

Exhibits the XG-Boost Model Training Process

```
XGBoost Model
xgb = XGBClassifier(random_state=42)
xgb.fit(X_train, y_train)

# Predictions and Evaluation
y_pred_xgb = xgb.predict(X_test)
print("XGBoost Classification Report:")
print(classification_report(y_test, y_pred_xgb))

# Confusion Matrix
conf_matrix_xgb = confusion_matrix(y_test, y_pred_xgb)
sns.heatmap(conf_matrix_xgb, annot=True, fmt='d', cmap='Blues')
plt.title('XGBoost - Confusion Matrix')
plt.show()
```

The above code snippet shows the deployment of an XG-Boost model on a binary classification problem. The above code snippet initialized an XG-Boost classifier with random state 42, which was trained on the data X_train and y_train and made predictions on the test set X_test. The

classification report shows its performance metrics: accuracy, recall, precision, and F1-score. Thus, The confusion matrix has presented the model's decisions regarding classification visually, with different numbers of correct and incorrect predictions. Generally, the code provides a dataset and complete analysis regarding the effective classification by the XG-Boost model.

Table 7

Displays the XG-Boost Classification Report

XGBoost Classification Report:

	precision	recall	f1-score	support
False	0.80	0.98	0.88	1602
True	0.27	0.04	0.06	398
accuracy			0.79	2000
macro avg	0.54	0.51	0.47	2000
weighted avg	0.70	0.79	0.72	2000

As showcased above, the precision for the false class was 0.80, meaning 80% of predicted False instances were False. Regarding actual class, the outcome was 0.27, indicating that 27% of predicted True instances were True. Regarding Recall: False class: 0.98, the model correctly identified 98% of actual False instances. The F1-score, 0.88, was a good balance between precision and recall for this class. Overall accuracy was 0.79, meaning 79% of all predictions were correct.

Visualization of Results

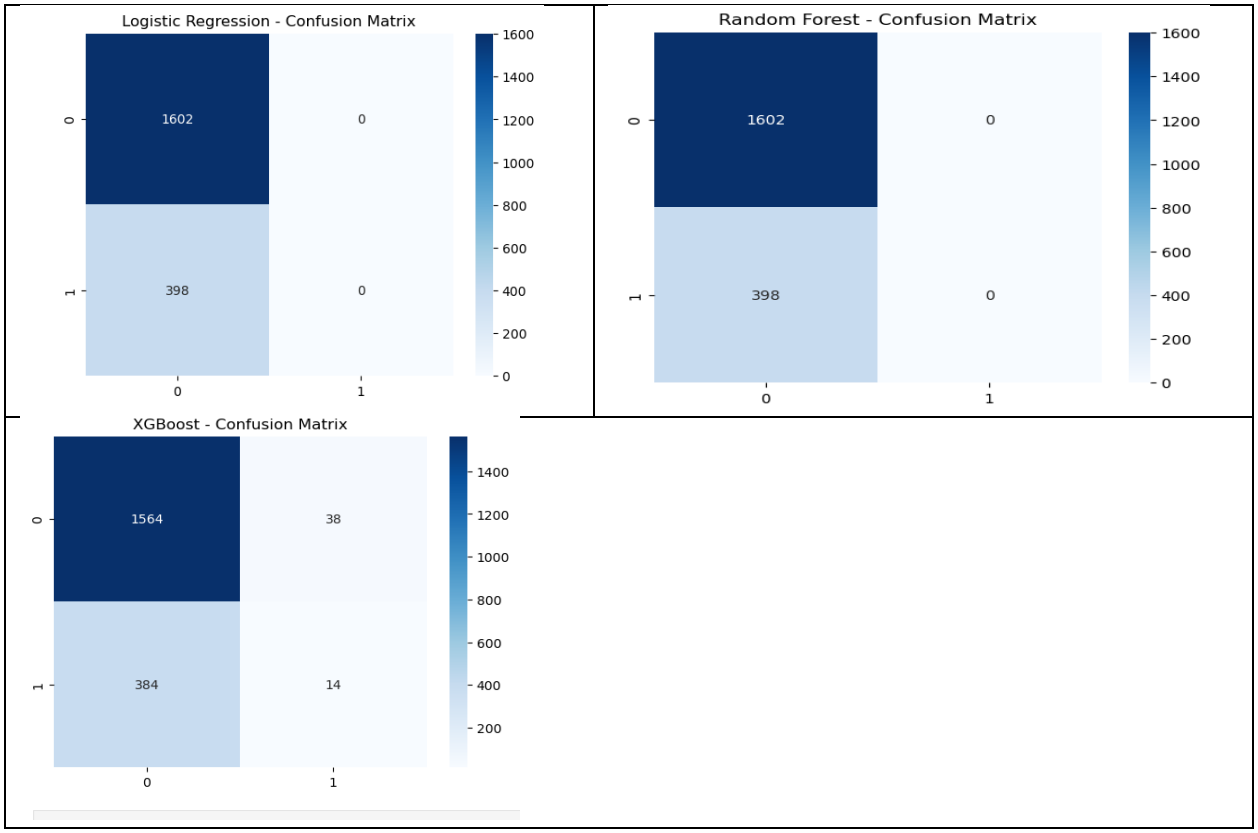

Figure 11: Depicts the Confusion Matrix For Logistic regression, Random forest, XG-Boost

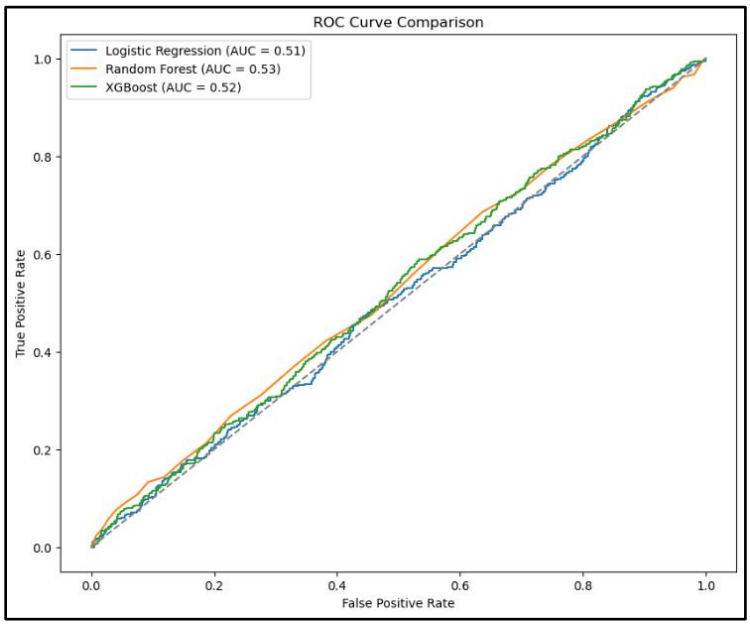

Figure 12: Showcases the ROC curve comparison

Above is a ROC curve comparison plot for three classification models: logistic regression, random forest, and XG-Boost. The graph plots the True Positive Rate against the False Positive Rate for different classification thresholds. In this comparison, the overall performance for the Random Forest model was the best, with the highest AUC, 0.53, followed by 0.52 for the XG-Boost model and 0.51 for Logistic Regression.

Key Findings from Network Analysis

The system developed social networks based on bank statement data and data from the National Court Register (Filipkowski, 2023). The described system assigned roles to individuals within the network to help identify critical figures and vulnerabilities. Once the roles of the individuals are known, connections between them can be analyzed. Node proximity allows the detection of bank accounts owned by the same owners. This also contributes to validating the correctness of role assignments with a module in charge of identifying nodes with similar roles across different data sources, such as bank statements and the National Court Register (Filipkowski, 2023).

The automated criminal network analysis assists in effectively identifying the perpetrator's role in criminal groupings. Given effectiveness, the system integrates data from various sources, such as bank statements and the National Court Register, whose input is received from disk files and web pages (Filipkowski, 2023). Social network analysis is of great relevance in describing criminal organization structures. It also requires advanced methods of knowledge in data mining, machine learning, and data clustering for the insights of criminal networks. These advanced tools can help police analysts design strategies to improve public safety and national security against organized crime, including money laundering.

Identification of patterns and key players in black money transactions Patterns in Black Money Transactions

Layering and Structuring. One of the very prevalent patterns is to "layer" the transactions to disguise the source of black money. This involves breaking down significant illicit funds into tiny bits of transactions, often below the threshold limits of regulatory reporting requirements,

with the view to raising no suspicion. Many such transactions are then routed through multiple accounts, jurisdictions, or shell companies to leave behind complex trails that are hard to trace.

Use of Offshore accounts. There is a trend of money being transferred to countries considered to be offshore tax havens or countries with slack financial regulations. Such jurisdictions guarantee anonymity and protection from scrutiny, and black money tends to flow with loose regulatory oversight. Using shell companies or trusts in these regions conceals the actual beneficiaries of such illicit funds.

Trade-Based Money Laundering. The criminal usually masks his dirty money by over- or under-invoicing goods in international trade. This would commonly allow these black monies to move across borders camouflaged as a legitimate business transaction.

Digital Currencies. Cryptocurrencies are increasingly being adopted for black money transactions because of their anonymity and ease of cross-border transfers. As a result, criminals use digital wallets and exchanges to launder money, frequently converting it between various cryptocurrencies before withdrawing into their respective currencies.

Key Players in Black Money Transactions

Cybercriminals: Online fraud, hacking, and ransomware attacks generate a large amount of black money by manipulating technology's vulnerabilities.

Drug Cartels: These usually are syndicates that tend to generate considerable revenue through the illegal drug trade, which is considered a significant source of black money.

Corrupt Officials: Government officials consistently generate Black money through bribery, extortion, and embezzlement.

Tax Evaders: Business enterprises under-invoke their income, avoid paying due taxes, and indulge in other illegal financial activities to generate black money.

Money Launderers: Legitimate businesses can be used as fronts for laundering black money by portraying the funds as coming from legitimate sources.

Bank Employees: Some corrupt bank employees may allow illegal transactions, which can facilitate money laundering.

Tax Haven Countries: These jurisdictions provide secretiveness and privacy, making them favorable for individuals who want to conceal black money.

DISCUSSION

Interpretation of Findings

The logistic regression model attained an inflated accuracy due to the inability to detect any money laundering crimes. In particular, the AUC score of 0.5064 indicated poor class differentiation. By contrast, the Random Forest algorithm had similar issues, unable to detect crimes with an AUC of 0.5285; however, it performed slightly better than Logistic Regression. On the other hand, the XG-Boost model performed the best in identifying financial crimes with a higher precision and F1 score than the other models; nevertheless, the recall still needed improvement. Despite lower accuracy, the XG-Boost algorithm was the best-performing algorithm. In terms of Precision, it correctly detected 27% of predicted crimes, while the other models failed. Concerning the F1 Score, XG-Boost had the highest F1 score, balancing precision and recall. As per the AUC outcome, slightly better than Random Forest, XG-Boost was more capable of distinguishing between crime and non-crime transactions.

Implications for Financial Crime Detection and Prevention

Deploying machine learning algorithms such as XG-Boost and Random Forest in financial crime detection and prevention markets presents a transformation in the financial industry. Both algorithms provide next-generation capabilities in detecting intricate patterns and relationships from large volumes of economic data and become the tools necessary for identifying fraudulent transactions, money laundering, and ensuing activities. However, while these algorithms provide various advantages, their deployment raises essential and multifaceted considerations concerning accuracy, interpretability, regulatory compliance, and operational integration.

XG-Boost and the Random Forest are ensemble learning methods where multiple decision trees predict an output, combining them to provide greater accuracy, robustness, and generalization. The models can handle high-dimensional data and detect complex nonlinear relationships among the variables. Financial transactions have many features that interact in complex ways: transaction amount, time, geographic location, and customer profile. XG-Boost is designed to scale and run fast; hence, it can consider big datasets and find subtle patterns indicative of fraud. The Random Forest generalizes well to new data because it minimizes overfitting using several decision trees.

Comparison with Existing Methods

Traditionally, financial institutions have used rule-based systems to identify suspicious transactions. The predefined set of rules and thresholds enables the rule-based systems to flag, for example, all transactions above threshold value amounts, all transactions conducted in high-risk jurisdictions, or widespread transfers between accounts. Rule-based systems are straightforward and can be tailored to particular regulatory requirements or institutional policies. A typical example could be that AML systems use rules based on customer profiles and transaction histories to show anomalies.

Nevertheless, rule-based systems have a myriad of limitations impeding their effectiveness. Among the significant drawbacks, one finds their rigidness: financial criminals constantly change their diabolic tactics to find new ways to mask illicit transactions. By their very nature, rule-based systems can only identify what they have been explicitly programmed to see. They can, therefore, be unhelpful in the unearthing of new patterns of fraud and money laundering. Even more unsettling, rule-based systems tend to yield many "false positives"-that is, legitimate transactions improperly tagged as suspect. This leads to spurious investigations and absorbs the resources in Compliance Departments.

One of the most salient points of machine learning models such as XG-Boost is how it handles unbalanced datasets- a common problem when detecting financial crimes. Since only small portions of all transactions are fraud, classic models will fail to catch fraud. Being able to tune XG-Boost to prioritize minimizing certain types of errors- often referred to as "false negatives"- makes it more robust in highlighting illicit transactions in unbalanced data.

Similarly, one of the significant advantages of Random Forest is its ease and flexibility in handling complex data with high dimensions. Most financial crimes involve a wide range of variables, such as amount, time, type of account, customer profile, etc., and the random forest can identify the interaction between them without extensive feature engineering. Traditional statistical models usually require domain expertise to create meaningful features manually and may lack nonlinear relationships that are usual in fraud or money-laundering detection.

CONCLUSION

This research project aimed to examine the combined application and deployment of machine learning and network analysis in detecting black money transactions in the USA and globally. Machine learning and network analysis have emerged as a powerful mechanism in the fight against financial crime. Machine learning techniques, whereby systems learn through supervised and unsupervised learning, differ in that they can recognize patterns of financial data indicative of potentially fraudulent behavior. On the other hand, network analysis is one of the unique methods of detecting financial crimes, which derives power from presented relationships and interactions between sets of entities constituting transactional networks, such as people, companies, and accounts. This study used the Global Black Money Transactions dataset which revolved around financial transaction records involving unreported or illicit money, frequently for evading taxes, laundering money, or conducting illegal activities. Data come from financial institutions, government surveillance, whistleblowers, or investigations by the concerned law enforcement agencies. Rigorous data preprocessing steps were performed for the machine learning pipeline. In the current research project experiment, three machine learning algorithms were used: Logistic Regression, Random Forest, and XG-Boost. The performance indicators involved a set of standard metrics, including accuracy, precision, recall, F1 score, and AUC, which stands for Area Under the Curve. Despite lower accuracy, the XG-Boost algorithm was the best-performing algorithm. In terms of Precision, it correctly detected and predicted crimes, while the other models failed. Concerning the F1 Score, XG-Boost had the highest F1 score, balancing precision and recall. As per the AUC outcome, slightly better than Random Forest, XG-Boost was more capable of distinguishing between crime and non-crime transactions.

References

Al Mukaddim, A., Mohaimin, M. R., Hider, M. A., Karmakar, M., Nasiruddin, M., Alam, S., & Anonna, F. R. (2024). Improving rainfall prediction accuracy in the USA using advanced machine learning techniques. *Journal of Environmental and Agricultural Studies*, *5*(3), 23-34.

Alam, M., Islam, M. R., & Shil, S. K. (2023). AI-Based predictive maintenance for US manufacturing: reducing downtime and increasing productivity. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(01), 541-567.

Álvarez-Jareño, J. A., Badal-Valero, E., & Pavía, J. M. (2017). Using machine learning for financial fraud detection in the accounts of companies investigated for money laundering.

Buiya, M. R., Laskar, A. N., Islam, M. R., Sawalmeh, S. K. S., Roy, M. S. R. C., Roy, R. E. R. S., & Sumsuzoha, M. (2024). Detecting IoT cyberattacks: advanced machine learning models for enhanced security in network traffic. *Journal of Computer Science and Technology Studies*, *6*(4), 142-152.

Filipkowski, W. (2023). The application of social network analysis algorithms in a system supporting money laundering detection. *Uwb*. https://www.academia.edu/109575292/The_application_of_social_network_analysis_algorithms_in_a_system_supporting_money_laundering_detection?b=100_percent_vector

Hasan, M. R., Islam, M. Z., Sumon, M. F. I., Osiujjaman, M., Debnath, P., & Pant, L. (2024). Integrating artificial intelligence and predictive analytics in supply chain management to minimize carbon footprint and enhance business growth in the USA. *Journal of Business and Management Studies, 6*(4), 195-212.

Islam, M. R., Nasiruddin, M., Karmakar, M., Akter, R., Khan, M. T., Sayeed, A. A., & Amin, A. (2024). Leveraging advanced machine learning algorithms for enhanced cyberattack detection on US business networks. *Journal of Business and Management Studies*, *6*(5), 213-224.

Ivanyuk, V. (2023). Forecasting of digital financial crimes in Russia based on machine learning methods. *Journal of Computer Virology and Hacking Techniques*, 1-14.

Jofre, M. (2023). Network analysis for financial crime risk assessment: the case study of the gambling division in Malta. In *Routledge eBooks* (pp. 26–48). https://doi.org/10.4324/9781003431671-3

Khan, M. T., Akter, R., Dalim, H. M., Sayeed, A. A., Anonna, F. R., Mohaimin, M. R., & Karmakar, M. (2024). Predictive modeling of US stock market and commodities: impact of economic indicators and geopolitical events using machine. *Journal of Economics, Finance and Accounting Studies*, *6*(6), 17-33.

Kumar, S., Ahmed, R., Bharany, S., Shuaib, M., Ahmad, T., Tag Eldin, E., ... & Shafiq, M. (2022). Exploitation of machine learning algorithms for detecting financial crimes based on customers' behavior. *Sustainability*, *14*(21), 13875.

Kurshan, E., Shen, H., & Yu, H. (2020, September). Financial crime & fraud detection using graph computing: Application considerations & outlook. In *2020 Second International Conference on Transdisciplinary AI (TransAI)* (pp. 125-130). IEEE.

Krész, M. (2020). Temporal network analytics for fraud detection in the banking sector. *U-szeged*. https://www.academia.edu/95120947/Temporal_Network_Analytics_for_Fraud_Detection_in_the_Banking_Sector?b=100_percent_vector

Krysovatyy, A., Lipyanina-Goncharenko, H., Sachenko, S., & Desyatnyuk, O. (2021). Economic Crime Detection Using Support Vector Machine Classification. *MoMLeT+ DS, 2917*, 830-840.

Liotta, G. (2022). Network visualization for financial crime detection. *Unnipg*. https://www.academia.edu/109731962/Network_visualization_for_financial_crime_detection?b=100_percent_vector

Nasiruddin, M., Al Mukaddim, A., & Hider, M. A. (2023). Optimizing renewable energy systems using artificial intelligence: enhancing efficiency and sustainability. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *14*(1), 846-881.

Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access*, *9*, 163965-163986.

Potla, R. T. (2023). AI in fraud detection: leveraging real-time machine learning for financial security. *Journal of Artificial Intelligence Research and Applications*, *3*(2), 534-549.

Palmeiro, J. M. M. (2021). *MevaL: A Visual Machine Learning Model Evaluation Tool for Financial Crime Detection* (Doctoral dissertation, NOVA University Lisbon).

Pro_AI-Rokibul. (2024). Financial-Crime-Detection-And-Analysis-of-Black-Money/Model/main.ipynb at main · proAIrokibul/Financial-Crime-Detection-And-Analysis-of-Black-Money. GitHub. https://github.com/proAIrokibul/Financial-Crime-Detection-And-Analysis-of-Black-Money/blob/main/Model/main.ipynb

Rahman, M. K., Dalim, H. M., & Hossain, M. S. (2023). AI-Powered solutions for enhancing national cybersecurity: predictive analytics and threat mitigation. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *14*(1), 1036-1069.

Rouhollahi, Z. (2023). Towards artificial intelligence enabled financial crime detection. *arXiv preprint arXiv:2105.10866*.

Shawon, R. E. R., Rahman, A., Islam, M. R., Debnath, P., Sumon, M. F. I., Khan, M. A., & Miah, M. N. I. (2024). AI-driven predictive modeling of us economic trends: insights and innovations. *Journal of Humanities and Social Sciences Studies*, *6*(10), 01-15.

Shil, S. K., Islam, M. R., & Pant, L. (2024). Optimizing US supply chains with AI: reducing costs and improving efficiency. *International Journal of Advanced Engineering Technologies and Innovations*, *2*(1), 223-247.

Sumon, M. F. I., Osiujjaman, M., Khan, M. A., Rahman, A., Uddin, M. K., Pant, L., & Debnath, P. (2024). Environmental and socio-economic impact assessment of renewable energy using machine learning models. *Journal of Economics, Finance and Accounting Studies*, *6*(5), 112-122.

Waqi, A. (2024, September 15). Global Black Money Transactions Dataset. Kaggle. https://www.kaggle.com/datasets/waqi786/global-black-money-transactions-dataset

Zeeshan, M. A. F., Sumsuzoha, M., Chowdhury, F. R., Buiya, M. R., Mohaimin, M. R., Pant, L., & Shawon, R. E. R. (2024). Artificial intelligence in socioeconomic research: identifying key drivers of unemployment inequality in the US. *Journal of Economics, Finance and Accounting Studies*, *6*(5), 54-65.