EJTAS
ISSN 2786-7447
EUROPEAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES
OPEN ACCESS
PEER REVIEWED

# A Web-Based kNN Money Laundering Detection System

JohnPaul A.C. Hampo
*Department of Computer Science, School of Information and Communication Technology, Federal University of Technology, Owerri, Nigeria*

Euphemia Chioma Nwokorie
*Department of Computer Science, School of Information and Communication Technology, Federal University of Technology, Owerri, Nigeria*

Juliet Nnenna Odii
*Department of Computer Science, School of Information and Communication Technology, Federal University of Technology, Owerri, Nigeria*

**Suggested Citation**
Hampo, J.A.C., Nwokorie, E.C. & Odii, J.N. (2023). A Web-Based kNN Money Laundering Detection System. *European Journal of Theoretical and Applied Sciences, 1*(4), 277-288.
DOI: 10.59324/ejtas.2023.1(4).27

## Abstract:

Money laundering is synonymous to clothes laundering and it is the process of transforming the real nature of the source of an income or money. This transformation of the source is usually from an illegitimate source to a legitimate source. Explicitly programmed system, rule-based system and machine learning system exist as anti-money laundering system, however these systems have one or more setbacks, mostly the explicitly programmed and rule-based systems due to their inability to learn from experiences and to improve their performance as they used. The k nearest Neighbour (kNN) model was developed using open datasets on financial transaction from Kaggle.com, which is an open-source website that holds a lot of data. An accuracy of 98.4% was achieved for the selected model. In this article, we developed a web-based money laundering detection system which is based on the kNN Machine Learning model.

**Keywords:** *machine learning techniques, kNN, prediction, money laundering, classification, kNegbours classifier, detection.*

## Introduction

The world today has drastically changed from the world of last decades. These changes are in areas that are dependent on technology and it is due to the advancement and growth in technology as a result of the birth of state-of-the-art technological ideas, algorithms and systems. These changes are both good but with a resultant bad effect due to the presence of negative minds. The changes are technologically driven (Lokanan, 2022).

Money which is a means of exchange either for goods purchased or for services rendered, is very important in the society and to human. Money is meant to be got legally, but criminals and the notorious minds illegally get money (Doppalapudi et al., 2022). When money is not properly (legally and legitimately) got, it becomes difficult for it to be spent due to the presence of enacted laws, law enforcement agencies/agents and the financial regulatory bodies. Some sources from which dirty money is gotten from are destruction of Critical National

Infrastructure (CNI), trafficking, drugs and kidnapping.

The possessors of illegal money need a way to spend their money without being detected by the law enforcement agents and financial regulatory bodies. Thus, the criminals and notorious minds tend to make the illegal money legal. This is done through some processes and it is termed Money Laundering. A closer look at the businesses that fully encompass the economy these days, appears to be funded through illegitimate sources despite from afar, they appear to be funded through legitimate sources (Ramya et al., 2022).

Money laundering is the process of transforming the real nature of the source of an income or money which is usually an illegitimate source to a legitimate source. In simple terms, it is making illegal money (money from bad sources) to become legal money (money from good sources). Genzman defined money laundering as "an activity that knowingly engage in a financial transaction with the proceeds of some unlawful activity with the intent of promoting or carrying-on that unlawful activity to conceal or disguise the nature, location, source, ownership or control of these proceeds" (Rafay, 2021).

Money laundering which entails processes of making dishonest and prohibited proceeds appear honest and accepted is an international criminal doing, and it is present in different geographical entities. Money laundering is inter-location and intra-location and the advancement of the internet and communication technologies has not helped to reduce the vast nature of money laundering in terms of geographical landscape.

An illustration for better understanding is thinking of money as clothes. The clothes can be clean or dirty. The clean clothes can be used by a sane and responsible person without anyone raising an eye or questioning, so is legal ('clean') money. Conversely, when a sane and responsible person put on a dirty cloth, people will raise an eye and there will be lots of questioning, and so is it with illegal ('dirty') money. For the dirty clothes to be used, they have to be laundered by soaking, washing, drying and ironing. These processes are also in money laundering but with different terminologies, as they turn illegal money to a legal money (Dalpiaz, 2020).

The above illustration suggests that money laundering is indulged in by responsible and highly respected people but they use other people, usually not connected to them in blood; to carry out their activities. This is to cover their identity thereby making the process of discovering them hard.

## Review of Literature

A money is said to be dirty when it is obtained or got from an illegal activity, such as prostitution (in regions where it is not legal), internet crime, destruction of national infrastructure, kidnapping, trafficking, gambling (in regions where it is not legal like India (Kharote & Kshirsagar, 2014)) and hacking. A 'dirty' money can't be spent especially by those that claim to be responsible without laundering it, else it will call for questioning by the society.

The term 'money laundering' has been given different definitions by different authors. Notably, (Alexandre & Balsa, 2016) sees it as a crime that typically turns certain illegal financial gains to legal gains. They went further saying that a set of financial and commercial operations characterize money laundering that is aimed at incorporating into economy illicitly derived goods, resources or values in a transitory or permanent way.

Kharote & Kshirsagar (2014) referred money laundering as washing of illegal (dirty) money through a cycle or iterative transaction to produce what appears to be a legal (clean) money. They stated that illegal money is that money which the bearer is not notified anywhere and that the rightful tax on that money is not paid. Another definition of money laundering is by (Demetis, 2018) which is, "the masking of monetary gains resulting from any type of criminal activity". He stated that predicate offences are those criminal activities that are associated with money laundering, however, money laundering is a crime on its own.

Money laundering is a cycle or an iteration of transaction. The processes in the cycle of money laundering are collection, placement, layering and integration. This process is dynamic and it continuously mask the revenues from illegal activities gradually and over a long time.

1. Collection – after the successful execution of a crime, the criminal is paid. The payment for the crime might be ransom money for a kidnapped, the money from trafficking, drugs sales, bunkering and proceeds from other crimes. The collection is not limited to cash, as resources and goods can be collected but later transformed to cash. This process is usually done once.

2. Placement – the movement of the collected money by the collector to the place of investment, business, or a financial house. This is the first step in covering or disguising the act and the money launderer. Placement might involve more than once from a collection or once in different investments from a collection. This can be done internationally or locally. Smart money launders don't place their collection at once or they divide their collection and place it in different investments.

3. Layering – this is the other steps taken for deeper cover up and disguise (Frumerie, 2021). It becomes a continual of placement from the first placement but this time it is done by the 'house' where the first placement occurred and not by the launderer. This process makes the detection of illegal proceeds difficult for the law enforcement agencies.

4. Integration – over a said time, when the launderer feels that the money has been properly laundered, the 'clean' money is moved back into the economy either through purchase or through the bank from the laundering 'house' to the money launderer, that is the person that did the collection and placement. The integration process can't be detected except with the help of an informant because the laundered money now appears to be profit from normal legal business.

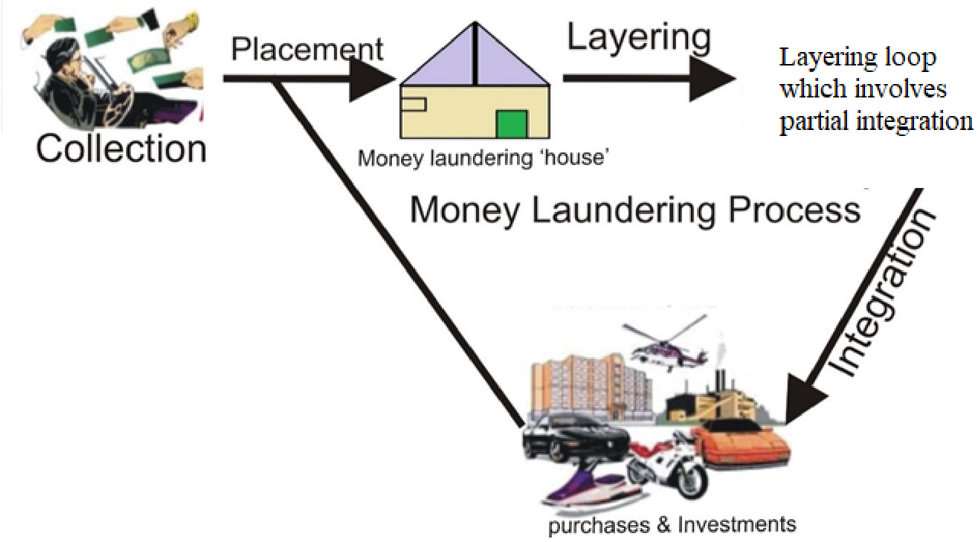

**Figure 1. Money Laundering Processes**
**Source:** Manjunath (2015)

Figure 1 is the process that money laundering can be detected is at the placement process and the layering process. For prevention of money laundering, the process is collection process. The money laundering house can be a legal investment, business or financial structure. The integration process is a loop and after the integration, the laundered money can be recollected by the owner or it can be exchanged as purchases.

Humans have been doing the work of detecting suspiciousness and anomalies in financial accounts of people before the advent of anti-money laundering systems. This they did and recorded little successes despite the small volume of data in those years (Cem, 2023). Businesses are on the increase daily and so are transactions, hence a human anti-money laundering system cannot monitor the transaction of such large companies since their transactions are in hundreds and at times thousands, and from different locations. If human anti-money launderers can't successfully detect anomalies in large businesses, then what about conglomerates and multinational businesses with possibly thousands and tens of thousands transactions daily? This definitely call for anti-money laundering systems that are programmed using data mining techniques since it is an era of big data.

Prior to the era of machine learning, systems were programmed explicitly hence their performance were exclusively on the written program. Machine learning being a branch of Artificial Intelligence (AI) is the practice of enabling a system to learn from data rather than through explicit programming. Machine learning came as a result of big data analytics. Predictive, analytic and descriptive models have to be improved therefore machine learning techniques are required (Ruiz & Angelis, 2022; Sujith et al., 2022).

Machine learning means to enable machines to learn without programming them explicitly. The objectives of machine learning are to enable machines make predictions, perform clustering, extract association rules, or make decisions from a given dataset. According to (I-Hsien Ting et al., 2010; Lokanan, 2022; Lopez-Rojas & Axelsson, 2012; Rafał Drezewski et al., 2015), big data is any kind of data source that has at least one of four shared characteristics, called the four Vs:

- Extremely large ***Volumes*** of data
- The ability to move that data at a high ***Velocity*** of speed
- An ever-expanding ***Variety*** of data sources
- ***Veracity*** so that data sources truly represent truth.

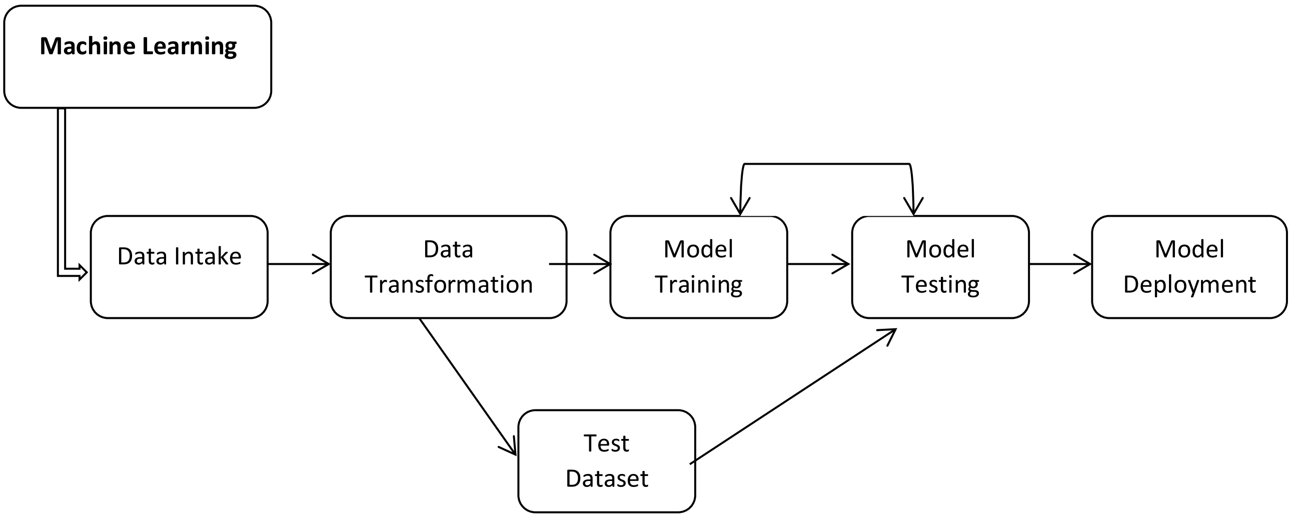

Figure 2. Machine Learning Stages

In a supervised learning, the target is to infer a function or mapping from training data that is labelled. The training data consist of input vector X and output vector Y of labels or tags. A label or tag from vector Y is the *explanation* of its respective input example from input vector X. The X and Y make up the training example. In unsupervised learning, there is no training data and the idea is to find a hidden idea in the unlabeled data. In supervised learning, we have ML as either regression or classification while in unsupervised we have it as clustering (segmentation). Some algorithms used in machine learning are Naïve Bayes (NB), *k* Nearest Neighbour (KNN), Support Vector Machine (SVM), Hidden Markov Model (HMM), J48 Decision Tree, Random Forest and Artificial Neural Network (ANN).

The stages in machine learning are data intake, data transformation, model training, model testing and model development (Ahmed, 2019; Alarab et al., 2020; Llu´ıs et al., 2012) (Figure 2)

- Data Intake – A dataset is loaded and saved into the memory

- Data Transformation – Here the inputted data is transformed, cleaned and regularized. Data conversion to the needed format is done and the data is separate into training and test data. A training data is for building the model and testing data is for validating the built model.

- Model Training – A model is built using a chosen algorithm

- Model Testing – The built model is tested using test data and this is a continuous process because the produced result from the testing is used to build new model. This is the learning in machine learning.

- Model Development – The best model after a desired iteration or one that fits the desired result is selected.

Money laundering being a world epidemic needs to be addressed. There are different models that see to address the issues of money laundering. (Joana, 2015) gave a risk assessment model for anti-money laundering system. The aforesaid model is a client behaviour model based on clusters, also using Prospero software, which with Random Forest and the method of Self Organizing Maps allows to group clients according to their behaviour in terms of transactions. Her model allows each cluster to have an associated risk, and those with higher risk are targets of special attention. Whenever there is a deviation from the expected behaviour, there is a warning of suspected money laundering. The model is shown in Figure 3.

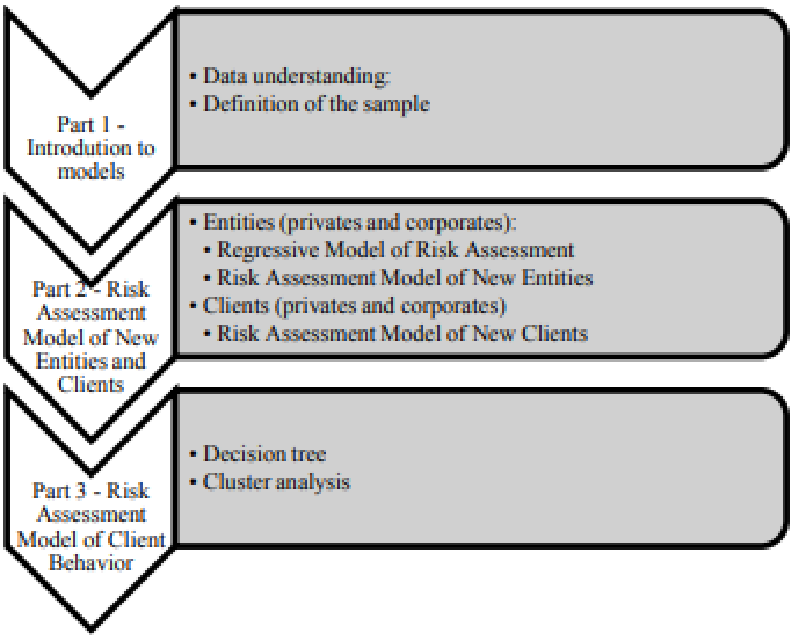
Part 1 - Introdution to models
• Data understanding:
• Definition of the sample
Part 2 - Risk Assessment Model of New Entities and Clients
• Entities (privates and corporates):
• Regressive Model of Risk Assessment
• Risk Assessment Model of New Entities
• Clients (privates and corporates)
• Risk Assessment Model of New Clients
Part 3 - Risk Assessment Model of Client Behavior
• Decision tree
• Cluster analysis

**Figure 3. Risk Assessment Model**
**Source:** Joana (2015)

In a knowledge discovery database (KDD) process, anti-money laundering is a process of four types and these steps corresponds to the four levels of analysis: transaction, account, institution and multi-institution (Le Nhien et al., 2010). The first three levels: transaction, account and institution are the most important where the last one depends more or less on the organisations and their policy. The data mining framework proposed by then also consist of three levels and consist of different components. The three levels are: data pre-processing, data mining and knowledge management.

### Data Pre-Processing

The main role of this component is to extract and clean raw datasets from data sources located in different sites of this international bank. It then integrates them into consolidated databases that are used to build a data warehouse of customer information and customer transactions.

### Data Mining

This component provides classification and clustering techniques for the most basic level of this framework: analysing transaction datasets. At this level, transaction records are extracted for investigations.

### Knowledge Management

Results of mining process, experience of AML experts, running results are collected, stored in relevant repositories and analysed by this component. It also generates significant, interpretable rules and knowledge.

Le Nhien et al. (2010) also gave a diagrammatic representation for their process. They applied a clustering technique for the analysing and investigating process of the anti-money laundering system. This is shown in the Figure 4.

Another model as studied by (Timm et al., 2016) is the Customer Identification Process in Figure 5. The CIP model is like the Know Your Customer (KYC) model. The CIP is triggered every time the institute enters a new business relationship with a customer just like the KYC.

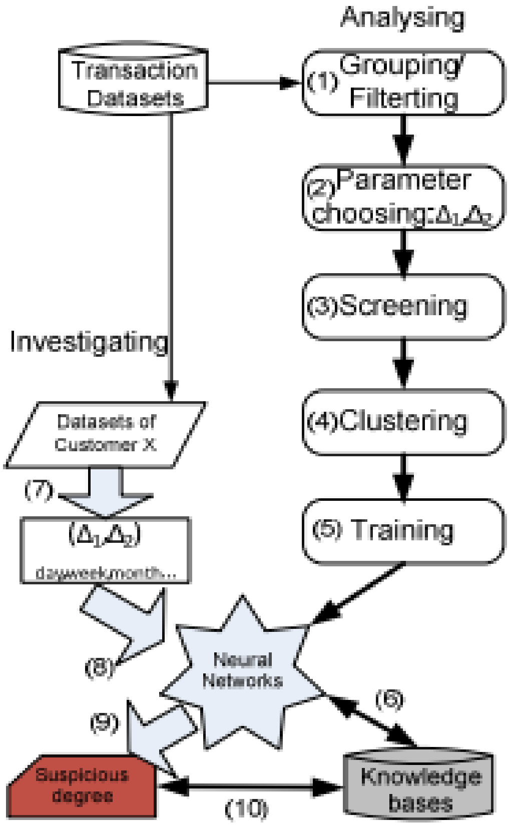

**Figure 4. Analysing and Investigating Process**
**Source:** Le Nhien et al. (2010)

The development of a reference model is an iterative process. This process is characterized by different versions of the considered model. The reference model should be evaluated using a validation method, which may lead to adjustments of the reference mode. Timm et al. (2016) used two iteration loops were traversed. While the first iteration loop concentrated on the process perspective, the second iteration loop focused on the data perspective of the AML program.

Xingqi & Guang (2009) proposed a system based on improved minimum spanning tree clustering to detect money laundering. According to them their system (algorithm) is effective and succinct but their system only detected without preventing. Their system used a financial dataset which have 70 fields, 64941 records and it was coded in Microsoft Visual C++. Their work was an analysis of similarity measure and distance metric.

Intelligent agent-assisted decision support system was modelled and developed by Shijia & Dongming (2009) for anti-money laundering system. They decided to use intelligent agents because they are autonomous, reactive, proactive and they are suitable for dynamic, ill-structured and complex money laundering. They were unable to perform task analysis and knowledge acquisition in their system.

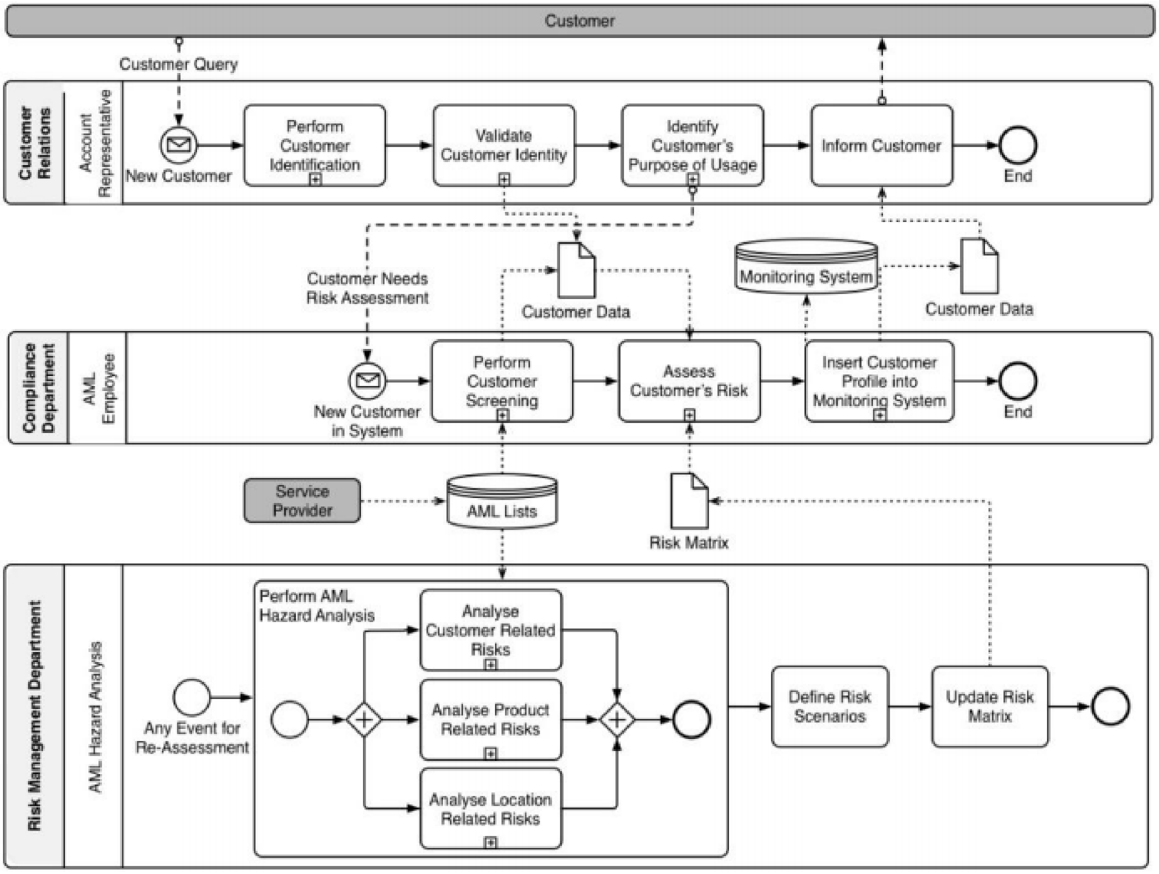
Customer
Customer Query
Customer Relations
Account Representative
New Customer
Perform Customer Identification
Validate Customer Identity
Identify Customer's Purpose of Usage
Inform Customer
End
Customer Needs Risk Assessment
Customer Data
Monitoring System
Customer Data
Compliance Department
AML Employee
New Customer in System
Perform Customer Screening
Assess Customer's Risk
Insert Customer Profile into Monitoring System
End
Service Provider
AML Lists
Risk Matrix
Risk Management Department
AML Hazard Analysis
Any Event for Re-Assessment
Perform AML Hazard Analysis
Analyse Customer Related Risks
Analyse Product Related Risks
Analyse Location Related Risks
Define Risk Scenarios
Update Risk Matrix

**Figure 5. CIP in An AML**
**Source:** Timm et al. (2016)

Le Nhien et al. (2010) in their research applied a data-mining based solution to detect suspicious money laundering cases in an investment bank. They stated that traditional approaches to anti-money laundering followed a labour-intensive manual approach because money laundering is a sophisticated activity with many ways of laundering money. Hence, they proposed an investigating process to money laundering by using the clustering and neural networks algorithm of data mining. In addition to the two proposed algorithms, there was need for they to improve the running time of their system, hence they introduced suspicious screening heuristics.

Synthetic data approach was applied by Lopez-Rojas & Axelsson (2012) for the detection of money laundering. However, there approach was faced by the cons of synthetic data which include; biasness, non-realistic, non-representativeness of the data. Their system was a mobile system.

In the prediction model or technique, Lopez-Rojas & Axelsson (2012), analysed the implications of using machine learning techniques for money laundering detection in a data set consisting of synthetic financial transactions and aimed to detect anomalies inside a data set of mobile money financial transactions by using the classification techniques to group transactions as suspicious or nonsuspicious.

Zhiyuan et al. (2014) explored the benefits and effectiveness of expectation maximization algorithm for suspicious transaction detection in anti-money laundering and they discovered that EM method out phased the traditional clustering method. They showed that EM (Expectation Maximization) is a better algorithm to support clustering operation than k-means. However, their system was based on clustering alone, and it has a high false positive rate. Hence some normal transactions were seen as abnormal.

Clustering, classification and prediction were the data mining techniques identified by Manjunath (2015) that can be used by banks for the purpose of uncovering money laundering trends in their large financial database.

Alexandre & Balsa (2016) in their paper on profiling banks customers profile used data mining techniques. This was done to support the process of detecting money laundering operations in a bank. They employed the WEKA tool (Waikato Environment for Knowledge Analysis) which is a product of the University of Waikato, New Zealand. The WEKA tool uses k-means, J48 and PART algorithms.

Timm et al. (2016) in their research classified the anti-money laundering programme for financial institutions into planning and controlling. The steps in Table 1 should be used in developing an anti-money laundering system.

### Table 1. AML Program for Financial Institution

| Phase | Step | Name |
|---|---|---|
| **Planning** | 1. | Identify regulations |
| | 2. | Derive company guideline |
| | 3. | Conduct risk analysis |
| | 4. | Define process and control activities |
| | 5. | Implement control system |
| | 6. | Define control structure |
| **Controlling** | 7. | Define organization function |
| | 8. | Appoint representative |
| | 9. | Conduct employee training |
| | 10. | Conduct internal and external audits |

A graph based machine learning approached was implemented by Soltani et al (2016) in their money laundering detection framework. Their aim was to mine a cluster or group of transaction that have the features of money laundering with respect to their dataset and their rules. After the execution of their framework, a human investigator has to perform further analysis on the groups obtained by the framework.

Demetis (2018) reported the situation of banks trying to combat money laundering through structural coupling and machine learning profiling. In his work, the critical dynamics between computer profiling and human profiling was presented.

## Methodology

This study explored the performance of a supervised learning algorithm called k nearest neighbour in the classification of illicit financial transactions from licit financial transactions, available in a financial dataset. The algorithm was trained and executed dataset on a specific engineered dataset and the performance metrics such as the accuracy, specificity and precision were documented. To analyse the performance of the kNN algorithm, the datasets engineered on were from Kaggle and the basic data are presented in Table 2.

The datasets are publicly available with well defined features. The engineered dataset has 25 features and 1480 observations. The classes in the engineered dataset are 1 for fraud and 0 for no fraud. All the missing values were dropped in the original datasets especially in cases where the label ‘isFraud’ has a missing value. This is because kNN is a supervised learning algorithm and cannot determine the status of a transaction if the label has missing value.

Table 2. Source Details of Datasets

| Filename | URL | Date Downloaded |
|---|---|---|
| PS_20174392719_1491204439457_log | https://www.kaggle.com/ealaxi/paysim1 | *20-09-2019* |
| MLtag | https://www.kaggle.com/maryam1212/money-laundering-data | 16-04-2020 |
| ML | https://www.kaggle.com/maryam1212/money-laundering-data | 25-08-2021 |

The engineered dataset having 25 features consists of 11 numeric variables and 14 categorical variables. None of the variables has missing value; the missing values were removed before the dataset was engineered.

The cleaned and engineered dataset was split into train and test set in the percentage of 75 and 25 respectively. A standardizer was used to scale the variables (features) into a unit variance whereby the mean is removed. It was the standard scaler that was implemented and the scaled dataset was trained using the kNeighbour classifier.

Four experiments were done using the kNeighbour classifier algorithm, as detailed in the table below.

Table 3. Experiments Details

| Name | Standardized | Hypertuned |
|---|---|---|
| Model 1 | No | No |
| Model 2 | No | Yes |
| Model 3 | Yes | No |
| Model 4 | Yes | Yes |

The metrics used to calculate the performance of each of the experiments are accuracy, recall, precision and f1 score. Table 3 depicts two out of four experiments has scaled data while two had unscaled data. Parameter hyper tunning was done to a model that had scaled data and to another model that has unscaled data. Also, a model that had unscaled data and a model that had scaled data used the default parameters of the kNeighbours classifiers.

The equations for the performance metrics used are:

$$accuracy = \frac{TP+TN}{TP+TN+FP+FN} * 100 \qquad (1)$$

$$Precision = \frac{TP}{TP+FP} * 100 \qquad (2)$$

$$Recall = \frac{TP}{TP+FN} * 100 \qquad (3)$$

$$F1\ Score = 2 * \frac{Precision*Recall}{Precision+Recall} * 100 \qquad (4)$$

Flask which is a python web framework for development of light weight applications was used for the development of the web-based system. In a combination to flask, HTML5 and CSS3 were used for the frontend. In this study and experiment, python programming language has been used as the bedrock to both the model development and nthe web development phases.

## Result and Analysis

This study sightsaw the use of kNN to train a model that will be used to combat money laundering in the financial space. The different models built in this study are all kNN classifier (a supervised learning algorithm). Four metrics namely accuracy, precision, recall and f1 score; were used for performance analysis. The performance metrics per model is presented in Table 4.

Table 4. Performance Metrics

| Name | SC | H | Accuracy (%) | Precision (%) | Recall (%) | F1 score (%) |
|---|---|---|---|---|---|---|
| Model 1 | No | No | 96.2 | 96.4 | 99.7 | 98 |
| Model 2 | No | Yes | 98.4 | 98.3 | 100 | 99.2 |
| Model 3 | Yes | No | 96.2 | 96.4 | 99.7 | 98 |
| Model 4 | Yes | Yes | 98.4 | 98.3 | 100 | 99.2 |

Table 4 indicates that model 1 (unscaled and not tuned) and model 3 (scaled and not tuned) has same metrics, while model 2 (unscaled and tuned) and model 4 (scaled and tuned) have same metrics. This shows that the parameters that were hyper tuned positively affected the performance of the model. The hyper tuned parameter is number of neighbours, hence, n_neighbors = 5, metric = 'minkowski', p = 2. Only n_neighbors which represents the number of k was hyper tuned as metrics and p maintain their default values.

The confusion matrix was plotted using seaborn on the accuracy as produced by model 4 (the selected model). The confusion matrix shows the classification of the model with respect to the true positive, true negative, false positive and false negative.

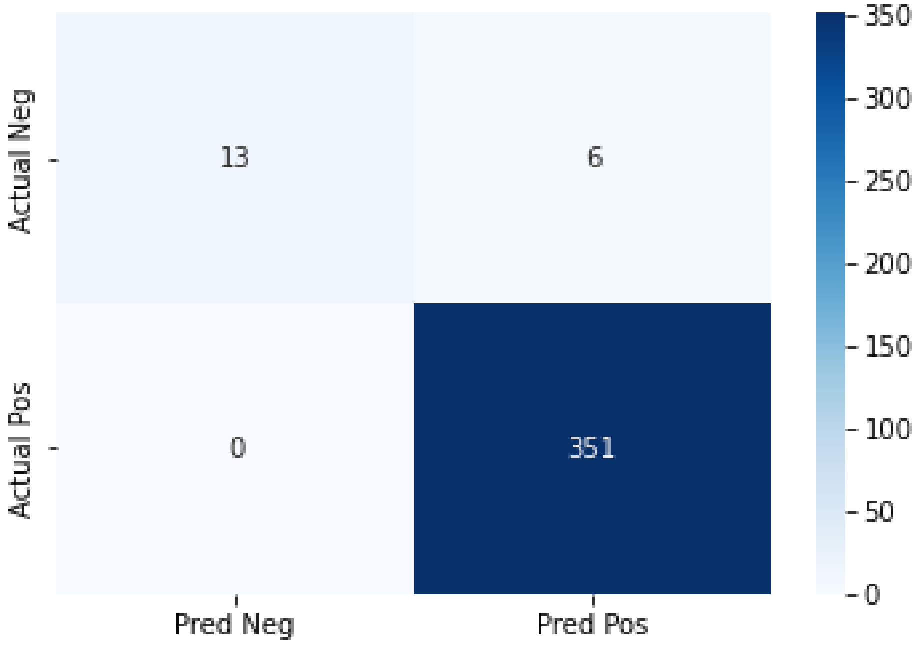

Figure 6 Confusion Matrix of Model

Figure 6 depicts that the values for variables used for the calculation of the various performance metrics. These values are:

True Negative – 13

False Positive – 6

True Positive – 351

False Negative – 0

This shows that the model predicts from the test set that 13 are not money laundering transaction and truly they are not. Also, it predicts from the test set that 351 are money laundering transactions and truly they are money laundering transactions. However, 6 transactions are classified as money laundering by our model of which that are not money laundering transactions. Finally, our model did not any transaction as not money laundering transaction which meanwhile is a money laundering transaction.

## Conclusion

This study built four models based on kNeighbour classifier, for money laundering detection in financial transaction using datasets from Kaggle.com. standard scaler was applied to the dataset for two models and it shows that the application of standard scaler was not seen in the performance metrics as the performance was same with the model that used unscaled data. That is, the performance metrics of the model that was trained with unscaled data and that was not hyper tuned is the same with the model that was trained with scaled data and that was not hyper tuned.

Parameter hyper tunning had a positive effect on the performance metrics of the models that were hyper tuned. The hyper tuned models had an accuracy of 98.4%, a precision of 98.3%, a recall of 100% and a f1 score of 99.2%, against the untuned models, which had an accuracy of 96.2%, a precision of 96.4%, a recall of 99.7% and a f1 score of 98%.

In this study, scaling of data has no effect on the performance metrics, however, in a future study, we suggest the discussion of data scaling and also application of other supervised learning algorithms for money laundering detection.

## References

Ahmed, T.I. (2019). Money Laundering and Financial Crimes in Nigeria. *IOSR Journal of Economics and Finance*, *7*(3), 45-53.

Alarab, I., Prakoonwit, S. & Nacer, M.I. (2020). *Comparative Analysis Using Supervised Learning Methods for Anti-Money Laundering in Bitcoin.* In Proceedings of the 2020 5th International Conference on Machine Learning Technologies (ICMLT '20). Association for Computing Machinery. New York, NY, USA. https://doi.org/10.1145/3409073.3409078

Alexandre, C., & Balsa, J. (2016). Client Profiling for an Anti-Money Laundering System. *ArXiv, abs/1510.00878.*

Cem, D. (2023). Anti Money Laundering Algorithms in 2023: Tackling AML with AI. AI Multiple. Retrieved from https://research.aimultiple.com/aml-software/

Demetis, D.S. (2018). Fighting money laundering with technology: a case study of Bank X in the UK. *Decision Support Systems, 105,* 96-107. https://doi.org/10.1016/j.dss.2017.11.005

Frumerie, R. (2021). Money Laundering Detection using Tree Boosting and Graph Learning Algorithms. Degree Project In Mathematics, Second Cycle, 30 Credits Stockholm, Sweden. Retrieved from https://www.diva-portal.org/smash/get/diva2:1663255/FULLTEXT01.pdf

I-Hsien Ting, Hui-Ju Wu, & Tien-Hwa Ho (2010). *Mining and Analyzing Social Networks. Studies in Computational Intelligence.* Springer-Verlag Berlin Heidelberg. https://doi.org/10.1007/978-3-642-13422-7

Joana, F.O.M. (2015). *Risk Analysis in Money Laundering: A Case Study.* Instituto Superior Técnico Lisbon, Portugal. Retrieved from https://fenix.tecnico.ulisboa.pt/downloadFile/563345090414324/resumo.pdf

Kharote, M., & Kshirsagar, V.P. (2014). Data Mining Model for Money Laundering Detection in Financial Domain. *International Journal of Computer Applications*, *85*(16), 61-64. https://doi.org/10.5120/14929-3337

Le Nhien, A.K., Sammer. Markos, & M-Tahar, K. (2010). *A Data Mining-Based Solution for Detecting Suspicious Money Laundering Cases in an Investment Bank.* In 2010 Second International Conference on Advances in Databases, Knowledge, and Data Applications, Menuires, France. https://doi.org/10.1109/DBKDA.2010.27

Llu´ıs, A., Awasthi, A., & Jorg, L. (2012). *Genetic Clustering Algorithms for Detecting Money-Laundering.* MathMods Master Thesis. Universitat Aut`onoma de Barcelona. Retrieved from https://mat.uab.cat/~alseda/MasterOpt/GenClustering-AlsAwaLass.pdf

Lokanan, M. (2022). Predicting Money Laundering Using Machine Learning and Artificial Neural Networks Algorithms in Banks. *Journal of Applied Security Research*, 1-25. https://doi.org/10.1080/19361610.2022.2114744

Lopez-Rojas, E. A., & Axelsson, S. (2012). *Money Laundering Detection using Synthetic Data.* Annual workshop of the Swedish Artificial Intelligence Society (SAIS). Örebro, Sweden. Retrieved from https://www.diva-portal.org/smash/get/diva2:834701/FULLTEXT01.pdf

Manjunath, K.V. (2015). Data Mining Techniques for Anti Money Laundering. *International Journal of Advanced Research in Science, 12*(20), 10084-10094.

Rafał Drezewski, Grzegorz Dziuban, Łukasz Hernik, & Michał Paczek (2015). *Comparison of Data Mining Techniques for Money Laundering Detection System.* In 2015 International Conference on Science in Information Technology (ICSITech). Yogyakarta, Indonesia. https://doi.org/10.1109/ICSITech.2015.7407767

Ruiz, E. P., & Angelis, J. (2022). Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchanges. *Journal of Money Laundering*, *25*(4), 766--778. https://doi.org/10.1108/JMLC-09-2021-0106

Shijia, G., & Dongming, X. (2009). Conceptual modeling and development of an intelligent agent-assisted decision support system for anti-money laundering. *Expert Systems with Applications*, *36*(2), 1493-1504. https://doi.org/10.1016/j.eswa.2007.11.059

Soltani, R., Nguyen, U. T., Yang, Y., Faghani, M., Yagoub, A., & An, A. (2016). A *New Algorithm for Money Laundering Detection Based on Structural Similarity. Advance online publication.* In 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). https://doi.org/10.1109/UEMCON.2016.7777919

Sujith, A.L.N.V., Qureshi, N. I., Harshavardhan, V., Dornadula, R., Rath, A., Prakash, K. B., & Singh, S. K. (2022). A Comparative Analysis of Business Machine Learning in Making Effective Financial Decisions Using Structural Equation Model (SEM). *Journal of Food Quality, 2022,* 6382839. https://doi.org/10.1155/2022/6382839