IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 2)
Available online at: www.ijariit.com

Combating money laundering using artificial intelligence

Nikita M. Patil
nikita.patil@viit.ac.in
Vishwakarma Institute of Information Technology, Pune, Maharashtra

Shraddha M. Dondekar
shraddha.dondekar@viit.ac.in
Vishwakarma Institute of Information Technology, Pune, Maharashtra

Chetan V. Rawale
chetan.rawale@viit.ac.in
Vishwakarma Institute of Information Technology, Pune, Maharashtra

Kiran V. Memane
kiran.memane@viit.ac.in
Vishwakarma Institute of Information Technology, Pune, Maharashtra

Lahu Kamble
lahu.kamble@viit.ac.in
Vishwakarma Institute of Information Technology, Pune, Maharashtra

ABSTRACT

In today's world the money laundering is the major issue, so there is need to fight against the money laundering. "Cleaning stolen money, making the source of money no longer exist, called Money Laundering" Financial transactions are huge so it is challenging task to detect money laundering. As earlier AMLS (Anti-Money Laundering Suite) was introduced to detect the suspicious activities but it is applicable only on individual transaction not for credit card transaction and another bank transaction. To Overcome this issue of AMLS we propose Machine Learning method to identify common attributes and behavior with other bank account transaction and also identify suspicious transaction through credit card. Detection of Money Laundering transaction from large volume dataset is difficult, so we reduce the input dataset and then calculating annual turnover of their credit card transfer set a max value which is to be transfer. Also find pair of transaction with other bank account with common attributes and behavior.

Keywords— *Money, Money Laundering, Criminal Activities, Combating Money Laundering*

1. INTRODUCTION

Money laundering scrub as much as 5% of the world's GDP (Gross Domestic Product.) every year. Combating money laundering using AI is to detect the suspicious activities. Combating money laundering typically requires most entities that complete financial transactions to keep thorough records of their clients' accounts and activities. If they come across any information that appears to be suspicious, they are required to report it to the government for further investigation. In this Transaction records is check to detect money laundering activity if the suspicious data is detected. Here we use Artificial Intelligence and Machine Learning Algorithm to detect the suspicious activities and solve it by training the data of that activity. We are going to use supervised and unsupervised algorithm techniques.

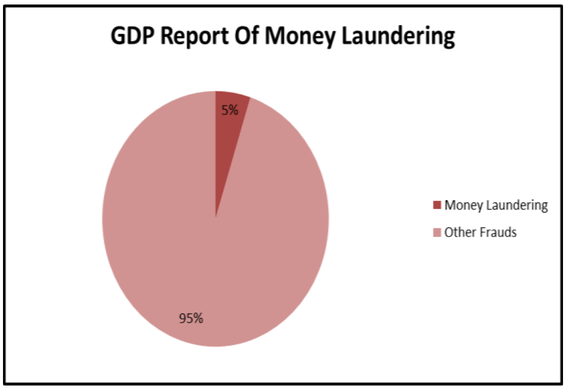

Fig. 1: GDP Report of Money Laundering

2. LITERATURE SURVEY

We did some survey to find out whether such system is already present, which may detect suspicious transaction activities. And we have found that existing technology which is done by UOB. United overseas bank is leading bank in Asia. To avoid the fraud in banks, the bank made a strategic decision to priorities co-creation by working with Tookitaki to develop a fit-for purpose Ai-driven

AML technologies, tools and system in a single integrated platform. UOB chase to implement customized model as it was more fitting for its compliance requirements. Anti-money laundering suite (AMLS), the integrated solution is designed around the banks AML framework that features know your computer, transaction monitoring, name screening and payment screening processes.

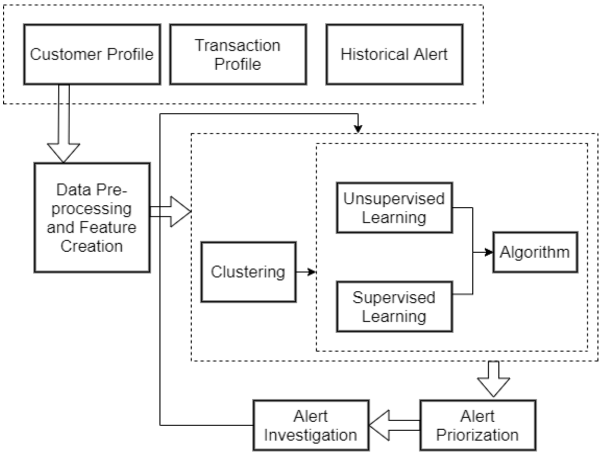

Fig. 2: Machine Learning alert priotization

3. PROPOSED WORK

The aim of this project is to detect the suspicious activities of bank transaction to identifying the money laundering. Also, to reduce the amount of criminal activities. There are some major effects of money laundering, which disturb world's economy system.

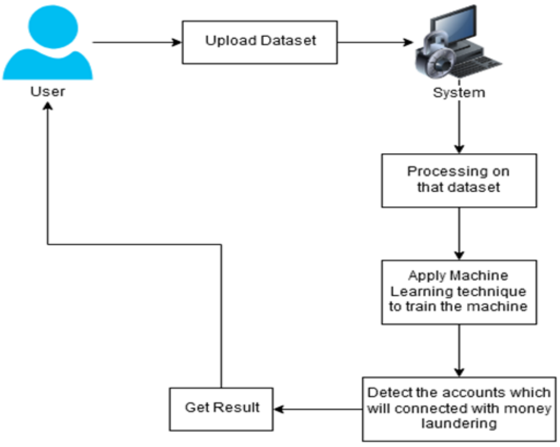
User
Upload Dataset
System
Processing on that dataset
Apply Machine Learning technique to train the machine
Detect the accounts which will connected with money laundering
Get Result

Fig. 3: Architecture of Proposed Framework

We calculate the turnover of particular account from their previous higher transfer amount. System predict suspicious if the transaction is beyond the already set value. This is available for credit card transaction, one bank to other bank transaction. The probabilities of fraud are not on parameters of individual bank transfer but also on relations with other account transaction and the amount that send between them.

4. STAGES OF MONEY LAUNDERING

(a) Placement: This is the first stage of this process, invest the black money into the market. The launderer deposits the illegal money through the different agents and bank in the form of cash or online transaction and having formal and informal agreement.

(b) Layering: In this stage hiding the real income source. The launderer invests the money, in the form of bond, stocks and bank account abroad. So, this process hides the owner and source of money.

(c) Integration: This is the final stage in which the money which is laundered returning into the legal Money

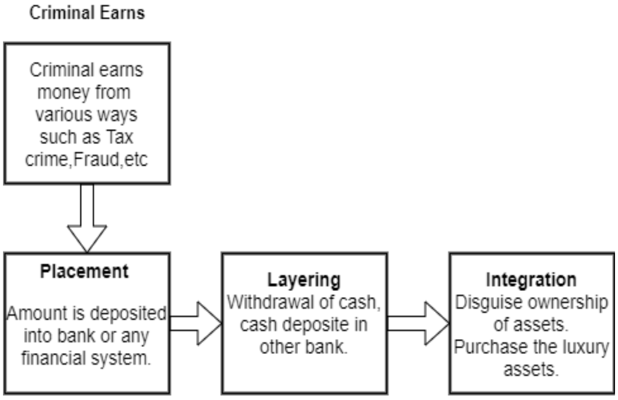
Criminal Earns
Criminal earns money from various ways such as Tax crime,Fraud,etc
Placement
Amount is deposited into bank or any financial system.
Layering
Withdrawal of cash, cash deposite in other bank.
Integration
Disguise ownership of assets. Purchase the luxury assets.

Fig. 4: Stages of Money Laundering

5. ALGORITHM USED

5.1 Support Vector Machine

Support vector machine (SVM) is used in the system because it produces accuracy with less computation power. The purpose of the support vector machine algorithm is to find hyper-plane in an n-dimensional space that distinctly classifies the data point.

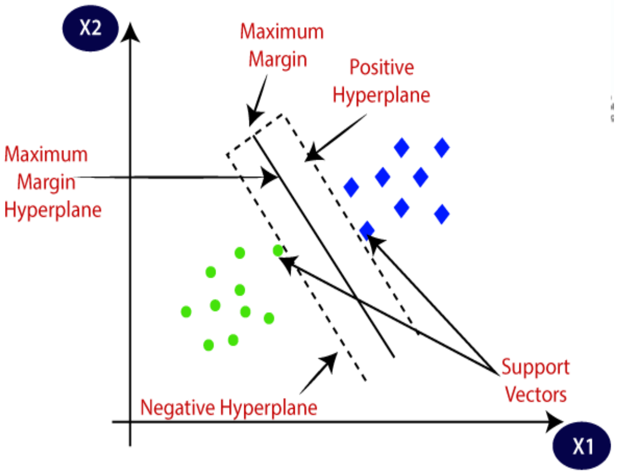

Fig. 5: Support Vector Machine

Our aim is to find the maximum distance between data points of both classes. Maximizing the margin distance provides reinforcement so that future data point can be classified with more confidence. The vectors are data points that are closer to hyperplane and influence the position, orientation of the hyperplane. Using this support vector, we maximize the margin classifier. Deleting the support will change the position of the hyper-plane. These are the points that help to build SVM accurately.

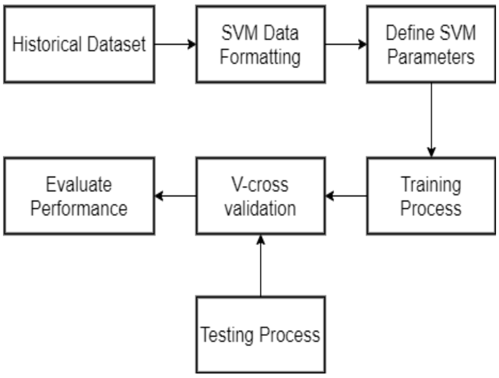

Fig. 6: Operation of SVM Model

5.2 Decision Tree

In this method, decision tree is applied to combating money laundering filed after finding money laundering feature. We select an approximate identifying strategy to discover typical money laundering patterns and money laundering rules. So with core decision tree algorithm, we can identify transaction data which is abnormal more effectively. Using decision tree algorithm more accuracy of the system is checked.

5.3 Naive Bayes

Naive Bayes algorithm is a supervised learning algorithm, specially used for solving classification problems. Naive is the occurrence of a certain feature is not dependent of the occurrence of other features and bayes is depends on the principle of the bayes theorem. In this algorithm we used threshold values to classify money laundering data. If the values is less than the threshold values then it comes in class A otherwise it comes in class B. then according to classification necessarily action will be taken. Naïve Bayes has the following probability formula:

$$P\left(\frac{A}{B}\right) = \left(P\left(\frac{B}{A}\right) \times P(A)\right)/P(B)$$

Where,

$P(\frac{A}{B})$ is the posterior probability: probability of the hypothesis A on the observed event B.

$P(\frac{B}{A})$ is likelihood probability: probability of the evidence given that the probability of hypothesis is true.

$P(A)$ is the prior probability: probability of hypothesis before observing the evidence.

$P(B)$ is the marginal probability: probability of the evidence.

5.4 Benefits of Proposed System

(a) Decrease the number of dirty or fraud transaction.
(b) High chances of identifying the transaction which is involving Money Laundering.
(c) No need to manual checking awareness of banking transaction.
(d) Very useful for government and cyber department for detecting fraud in transaction.

6. CONCLUSION

The Proposed Framework aims to find Money Laundering accounts among the large number of financial transactions. This system reduces the transaction involve in Money Laundering. In order to improve efficiency of this framework we calculate the turnover of each account. If the amount transferred from that account is greater than their regular transaction it will be treated as a suspicious. This system train and test itself, so there is no need to manual awareness. Our preliminary experimental results show a high degree of accuracy in detection of ML accounts.

7. REFERENCES

[1] Fatf-gafi.org – 'Money Laundering - Financial Action Task Force (FATF)' , 2016. [Online]. Available: http://www.Fatf-gafi.org.

[2] Fatf-gafi.org, 'Money Laundering - Financial Action Task Force (FATF)', 2014. [Online]. Available: http://www.fatfgafi.org/faq/moneylaundering/.

[3] Neo4j Graph Database, 'Neo4j, the World's Leading Graph Database', 2014. [Online]. Available: http://neo4j.com/.

[4] A. C. Bahnsen, A. Stojanovic, D. Aouada, and B. Ottersten. Improving credit card fraud detection with calibrated probabilities. In SDM, 2014.

[5] M. Gupta, J. Gao, C. C. Aggarwal, and J. Han. Outlier Detection for Temporal Data. Morgan & Claypool Publishers, 2014.

[6] J. Tang, Y. Chang, and H. Liu. Mining Social Media with Social Theories: A Survey. ACM SIGKDD Explorations Newsletter, 15:20-29, 2014.

[7] W. Li, V. Mahadevan, N. Vasconcelos. Anomaly detection and localization in crowded scenes. IEEE Tran. on Pattern Analysis & Machine Intelligence, 36(1):1, 2013.

[8] K. Sim, V. Gopalkrishnan, A. Zimek, and G. Cong. A survey on enhances subspace clustering. Data Min. Know. Disc., 26:332-397, 20.