



OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

SMART MONEY LAUNDERING PREDICTION AND RISK IDENTIFICATION SYSTEM

Anubhav Birendra Jha,¹ Farahanaz Maheboob Tandel,² Shailesh D Gaikwad,³ Nikhil Dilip Chaudhari,⁴
Prof.Dnyaneshwar.N.Rathod,⁵

⁵Assistant Professor, Department of Information Technology, SKN Sinhgad Technical Institute of Technology and Science,
Lonavala, Pune, Maharashtra, India

¹⁻⁴Student, Department of Information Technology, SKN Sinhgad Technical Institute of Technology and Science, Lonavala, Pune,
Maharashtra, India.

anubhav.jsk@gmail.com¹, tandelfarha42@gmail.com², shaileshgaikwad30@gmail.com³, Cnikhil2017@gmail.com⁴,
dnrathod88@gmail.com⁵

Abstract: The expression "Money Laundering" is an awful development to camouflage the black cash that changes over as the white cash. This crime represents an extreme danger to the money related organizations and furthermore to the country. There act three steps in Money Laundering Placement, Layering, and Integration. The headway of proficient component to recognize suspicious exchange is a basic issue on account of monetary exchange made in worldwide market. The framework we are creating focuses on how financial establishments can get better outcomes in hostile to tax evasion activities. The examination and recognition technique for illegal money-laundering accounts in Online Social Network OSNs exhibited that the proposed strategy accomplished high identification rates and exceptionally low false positive rates. To overwhelm this necessity we propose an adequate approach to catch out if the transactions are legal or illegal by using proposed system.

Keywords:- Money Laundering, Naïve Bayes, Risk Identification

I INTRODUCTION

Money laundering is often associated with criminal activities. Hostile to illegal tax avoidance is consequently viewed as a significant assignment in numerous nations. Money laundering has a significant consequence not only locally as well globally on the economy. Thus, corruption in financial markets can lead to a loss of public confidence in the financial protocol, increased hazard and instability, but also to sinking the development progress of the economy in general. The combination of this community data and law enforcement investigations will help to understand the detailed operations of the transnational criminal organization (TCO). This understanding can then be used by our prescriptive analytics to determine how to prime disrupt the TCO with bound resources while specifically accounting being cascading disruptions across the smuggling, money, and laundering networks resulting from interdictions. The development of the web as a worldwide, borderless correspondence stage managed a wide scope of social and monetary chances to individuals all

through the world. Lawbreakers have misused the capacity to impart quickly around the world to encourage cross jurisdictional digital misrepresentation and consequently, online cash laundering. In proposed system we analyze the risk in the transaction, money laundering recognition along with prevent from fraud transaction and money laundering in Online Social Network (OSN).

II. PROBLEM DEFINATION

It is common that money launderers divide the dirty money into multiple parts and make sequences of banking transfers or commercial transactions, manually detecting activities of money laundering is very challenging.

III. SCOPE AND OBJECTIVE

Scope

Scope of project is fraud transaction is identification from accounts details of user. Also prevent from fraud transaction in money laundering.

Objectives

- Identification of risk in the transaction
- Identification of money laundering
- Prevent from fraud transaction and money laundering

IV. LITERATURE SURVEY

Yadong Zhou et.al [1] proposed that virtual money in online social networks (OSN) assumes an inexorably significant job in supporting different monetary exercises for example, cash trade, web-based shopping, and paid games. Clients for the most part buy virtual money utilizing genuine cash. This reality propels assailants to instrument a multitude of records to gather virtual cash deceptively or illicitly with no or exceptionally low cost and afterward launder the gathered virtual cash for huge benefit. Such assaults not just present critical budgetary loss of unfortunate casualty clients, yet additionally hurt the practicality of the environment. It is in this manner of focal significance to identify noxious OSN accounts that take part in washing virtual money. To this end, we widely study the practices of both noxious and amiable records in light of activity information gathered from Tencent QQ, one of the biggest OSNs on the planet. At that point, we devise multi-faceted highlights that portray accounts from three viewpoints including account reasonability, exchange successions, and spatial connection among accounts.

Junwoo Seo et.al [2] states that different violations utilizing Bitcoin are highlighted. Among different wrongdoings utilizing Bitcoin, this paper proposes a strategy to identify illegal tax avoidance concentrating on blending administration that gives Money Laundering. This is a piece of the counter anti-money-laundering (AML) methodology, which can decide if the blender administration is utilized in specific exchanges by utilizing exchange test information utilizing blender. Illegal tax avoidance utilizing Bitcoin is frequently used to maintain a strategic distance from subsidize following in the underground world and examining it is basic in situational familiarity with finance following.

Chih-Hua Tai and Tai-Jung Kan [3] states that Money laundering is regularly connected with crimes. Against illegal tax avoidance is in this manner viewed as a significant errand in numerous nations. Notwithstanding, as usually tax criminals isolate the filthy cash into numerous parts and make groupings of banking moves or business exchanges, physically identifying exercises of illegal tax avoidance is testing. To facilitate the errand, this work builds up a two-stage shrewd strategy dependent on AI and information investigation systems for recognizing suspicious tax evasion accounts from the exchange information. The main stage underlines on recognizing each suspicious tax evasion account while the subsequent stage further recovers exceptionally suspicious ones with the goal that both the review and exactness for the distinguishing proof of tax evasion records can be to some degree dealt with. Assessed on the information given by Bank SinoPac, the set up astute technique accomplishes a review pace of 26.3%, which is multiple times the review rate (8.6%) of the Money Laundering Control Act in Taiwan, in the

primary stage, and later the accuracy rate can be expanded up to 87.04% in the subsequent stage.

Cornel Ion erban et.al [4] introducing under EU Directive 2015/849 of the European Parliament and of the Council on the counteractive action of the utilization of the monetary framework with the end goal of tax evasion or fear based oppressor financing, it is important to recognize the two people and exchanges of a specific level of hazard. The way toward recognizing the danger of the two clients and exchanges considered suspicious lies at the base of frameworks planned for counteracting tax evasion and fear based oppressor financing. Such frameworks are called AML (Anti-Money Laundering) frameworks. A significant advance in ascertaining a customer's hazard is to check his/her reality in arrangements of suspicious or conceivably suspicious people, additionally called approval records. Exemplary search strategies include huge handling abilities. Considering the commitment of every single money related organization to execute these strategies, there is a need to actualize a quick and secure inquiry stream. Consequently, the consideration was attracted to the looking methods for man-made consciousness. These sorts of strategies incorporate propelled AI forupgrading the entire looking through procedure: the framework can distinguish certain examples and recognize new ones dependent on specific attributes of the inquiry question and by distinguishing likenesses between words.

Bahulkar, A et.al [5] proposed that incorporates engaging, prescient, and prescriptive investigation that guides distinguishing and upsetting a transnational criminal association (TCO) working as related stash pirating, cash, and illegal tax avoidance systems. This kind of TCO will pirate booty over the U.S. fringe, produce incomes from illicit deals inside the U.S., and afterward utilize the tax evasion system to send the cash out of the U.S. Law implementation may have incomplete data about the fundamental interpersonal organization of the TCO yet this might be missing significant, purposefully shrouded associations between the lawbreakers. The proposed structure predicts the missing connections in the informal organization information and afterward calculations are applied to the enlarged information to recognize the networks of the TCO. Every people group serves an alternate job in the TCO and hence are essential in displaying the activities of the association. When the networks are identified, we recommend activities that apportion assets to upset the TCO tasks ideally as far as law authorization criteria.

Yaqin Jin and Zhenxin Qu [6] proposed that the account field, hostile to illegal tax avoidance has been profoundly contemplated and framed a progression of hypotheses. On the off chance that we apply these hypotheses and strategies legitimately to police examination cases, the real outcomes may not be good. From the point of view of police surveillance, this paper proposed a capital stream progressive model dependent on against tax evasion suspicious information, as indicated by the course of capital stream, the model isolated each record in information into levels, and disentangled the enormous scope arrange, to discover how cash streamed during the time spent illegal tax avoidance. Other than of this,

we utilized the entropy-weight strategy to assess each record substance, and examined the significance of every element in the tax evasion arranges. At long last, we try different things with the recreated informational collection and plot the capital stream diagram subsequent to layering, which affirms the viability of the various levelled model.

Sagwadi Mabunda [7] states that virtual monetary standards are on the ascent as is cash washing. While there are endeavour's to battle illegal tax avoidance through different intergovernmental bodies, many have communicated worry over the ascent of virtual monetary standards. A few cryptographic forms of money, for example, Bitcoin have assumed a significant job in the expansion of online illegal tax avoidance as it has qualities that crooks are attached to. Bitcoin and other cryptographic forms of money are decentralized mysterious/pseudonymous also, irreversible. They give the way to skirt the Anti-Money washing shields that have been set up.

Tatu Hyttinen and Saila Heinikoski et.al [8] introducing article talks about the harmonization of correctional arrangements concerning illegal tax avoidance in the European Union (EU), specifically, the ongoing Commission proposition for a Order on handling illegal tax avoidance by criminal law (COM(2016) 826 last). The point of view is both legitimate and political, calling attention to the distinctive lawful arrangements in the European Union and breaking down the improvement from a European mix point of view, especially as far as a so-called overflow process, whereby incorporation in one field prompts joining in contiguous fields. We set forward two primary contentions right now: We contend that all together for the overflow to prevail in a field pivotal for national sway, for example, criminal law, overflow should be supplemented with securitization and strategy washing, the last alluding to the marvel whereby issues are concurred at a global nonbinding field so as to later present these "universal benchmarks" into restricting enactment. (2) We contend that harmonization in the tax evasion setting gives an case of a fruitful overflow upgraded by arrangement washing what's more, securitization; handling illegal tax avoidance apparently requires overflowing European reconciliation additionally in the field of criminal law, a center issue of national sway. A demonstration of this is the reality that European nations have even fit their criminalization of self-washing, albeit culpable self laundering has been recently viewed as in opposition to the general precepts and standards of criminal law in numerous nations.

V. EXISTING SYSTEM APPROACH

Money laundering (ML) is a procedure toward type illegal profits appearance genuine; this is similarly the process by which offender's effort to conceal the true origin and ownership of the proceeds of their criminal activity. The Existing system method involves three stages, Which Includes Pre-processing of Data in Framework, ML Dynamic Risk Model, and Money Laundering Identification. The structure creates a system portrayal of every single coordinating exchange. Then admit a clustering approach to catch suspicious ML communities among the network. a strategy to

identify illegal tax avoidance concentrating on blending administration that gives Money Laundering. This is a piece of the counter anti-money-laundering (AML) methodology, which can decide if the blender administration is utilized in specific exchanges by utilizing exchange test information utilizing blender. The way toward recognizing the danger of the two clients and exchanges considered suspicious lies at the base of frameworks planned for counteracting tax evasion and fear based oppressor financing. Such frameworks are called AML (Anti-Money Laundering) frameworks. A significant advance in ascertaining a customer's hazard is to check his/her reality in arrangements of suspicious or conceivably suspicious people, additionally called approval records. Exemplary search strategies include huge handling abilities. Considering the commitment of every single money related organization to execute these strategies, there is a need to actualize a quick and secure inquiry stream. Consequently, the consideration was attracted to the looking methods for man- made consciousness. These sorts of strategies incorporate propelled AI for upgrading the entire looking through procedure: the framework can distinguish certain examples and recognize new ones dependent on specific attributes of the inquiry question and by distinguishing likenesses between words. Illegal tax avoidance utilizing Bitcoin is frequently used to maintain a strategic distance from subsidize following in the underground world and examining it is basic in situational familiarity with finance following. It then apply network-based algorithms into filter out unnecessary accounts along with operations. Finally, as extracted communities are reconstructs sorted and produce the output of the framework.

VI. PROPOSED SYSTEM APPROACH

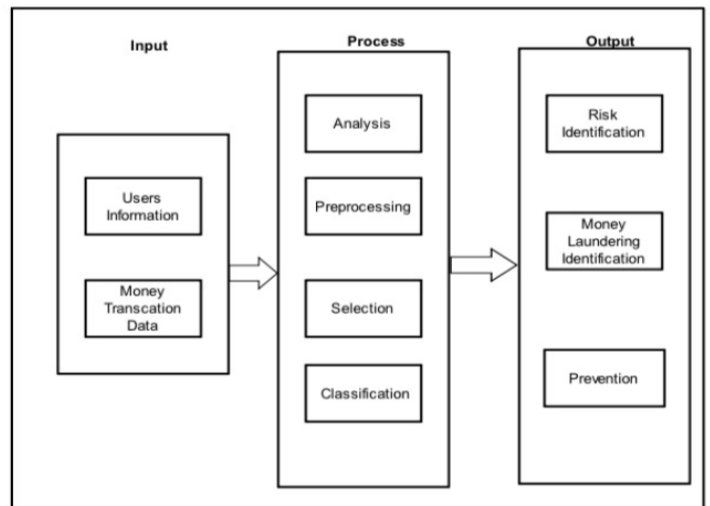


Fig.1 System Architecture of Proposed System

Money laundering is an attempt by criminals to legalize illegal income, which mainly refers to the disguise of the source and nature of illegal income through various means. In today's economic globalization and financial integration, money laundering activities are extremely harmful to the country's economy, finance and even political order and social stability. In this system online social network like a e-commerce

websites or application consist of users personal information and money transaction data. According to various user data system first analysis the data of transaction, pre-processing that data, selection of useful data with the various parameters and classification of that data according to the category Changing and moving cash was principally achieved through Web Money and Western Union on the two gatherings, just as Bitcoin, despite the fact that the utilization of the cryptographic money was moderately uncommon. As depicted in past examine on the subject of checking gatherings, cash donkeys speak to a basic component in online illegal tax avoidance conspire. In this system we seen that all transaction is divided into 2 category i.e. Proper and fraud transaction. According to the all process we can identify the risk of money transactions, Money laundering identification and also prevent the fraud transaction as well as money laundering.

Modules :

- 1) Admin Module
- 2) User Module

Modules description:

- In proposed system consist of mainly 2 modules Admin, User, Functionality of each module is follows
- Login, registration of user and Login of Admin.
- **Homepage**-User, Admin
- Admin Login with authentication, View account details, Analysis the data,pre-processing data, selection of data, classification of data, View all users information, Add precaution for money laundering, Analysis the risk in money laundering.
- User Registration and login with authentication, Transfer the amount for one account to the another account, View user account details, View precaution of money laundering, View risk of money laundering.

Implementation environment

In this system we developed the web application in java. In this project we can develop this project using MVC pattern. MVC view as Model-View-Controller.

MVC Pattern view as Model-View-Controller Pattern. This pattern is recognize for dividing application's concerns.

- **Model** - Model serve as an object or JAVA POJO varying data. They have also logic to modify controller whether the data changes. In this model contain various variable as well as getter and setter method.
- **View** - View perform as visualization of the data a particular model contains. In this contain jsp and bootstrap in css.
- **Controller** - Controller perform on both model along with view. They controls the data flow toward model object with updates and view whether data changes. As of keeps view along model separate. In controller call as a servlet in project.

VII. ALGORITHMS FOR SYSTEM

In our system naïve bayes is used for classification of account

Naïve Bayes: - For Classification of amount

- **Input :-** Transaction of amount
- **Output:-** Classification of amount according to category .

The proposed methodology text categorization using Naive Bayes can be analyzed for its implementation details with the below-mentioned steps.

Step 1: Dataset collection in which one is the dictionary that contains a set of the words corresponds to each class. Other dataset consists of tweets for training and testing.

Step 2: Pre-processing - Once the tweets are extracted, it is pre-processed. To remove unwanted text and symbols.

Step 3: Naive Bayes here all pre-processed tweets are taken as input and each word of a tweet is considered as a token. Compare the token to the words in the dictionary. If any word is a match then find the probability of word with respective

$$P(x/c_i) = \prod_{j=1}^n P(x_j/c_i)$$

class
----- (1)

$$= P(x_1/c_i) \times P(x_2/c_i) \times \dots \times P(x_n/c_i)$$

----- (2)

□ Where $i \leq j \leq m, j = i$

Step 4: classify number into class.

Step 5: Repeat the process.

VIII. MATHEMATICAL MODULE

- **System Explanation:**
- **Mathematical Model:** Let Assume S as of system for automatically recommends vehicle to customer. $S = \{F, I, O, e\}$
- **INPUT:**

Identify a inputs $F = f_1, f_2, f_3, \dots, f_n$ — F is set of functions which execute instructions.

- **I** = i_1, i_2, i_3 Sets of inputs to the function set
- **O** = o_1, o_2, o_3 Set of outputs through a function sets,
- **e** = End of a program flow.

$S_1 = I, F, O$

- **I** = Query submitted through the User, i.e.as a query
- **O** = Output of the aspects query, i.e. desire Transaction classification conferring to category
- **F** = Functions implemented for obtaining the output, i.e. Classification

A] Mapping Diagram

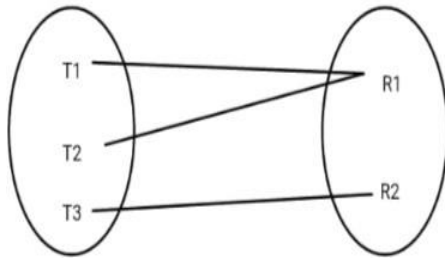


Figure 2. Mapping Diagram

Where,

T=Transaction Amount

R=Classification query.

T1=Transaction 1

T2= Transaction 2

T3= Transaction 3

R1=Proper category classification Query

R2=Wrong category classification Query

4. Set Theory

$$S = \{s, e, X, Y, \Phi\}$$

Where,

s = Start of the program.

1. Log in with webpage.
2. View classifications through transaction class according •

transaction values.

$X = \{T1, T2..Tn\}$

X = Input of the program.

Where, T1, T2..Tn = Transaction amount

Y = Output of the program.

e = End of the program.

Retrieve all transaction details with different categories.

User can search transaction according to category.

- **Failures or Success conditions.**

Success:

1. Proper classifications based on transaction data or information are available.
2. User gets instant result according to their needs.

Failures:

1. Huge database lead more time consumption to retrieve information.
2. Hardware failure.
3. Software failure.

II. COMPARATIVE RESULTS

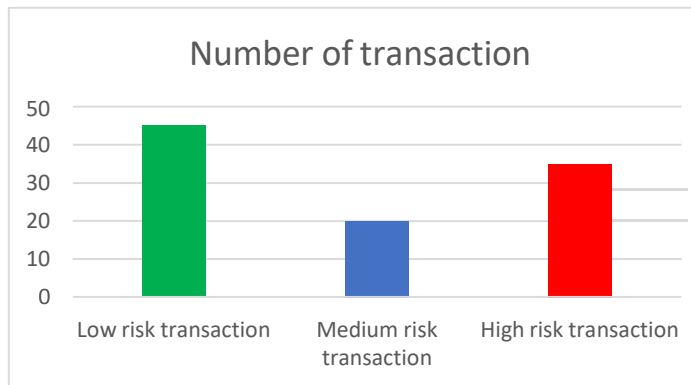
In our experimental setup, as shown in table 6.1, the total numbers of transaction were 100. These transactions were then divided into three main categories of risk of fraud transaction; among which 45 were low risk transaction, 20 were medium risk transaction and 35 were high risk transaction

Sr. No	Category	Number of Transaction
1	Low risk transaction	45
2	Medium risk transaction	20
3	High risk transaction	35

Table 1: Classification of transaction category

- Technical study of system hardware requirements with software requirements i.e. technical requirements of this project in order to inform a management and users of this application that these many resources are required. According to all specified requirements and environment this project is sufficient technically feasible. To run our project we required a hardware system which is feasible for our project like Intel I3 processor, 2 GB RAM, 20GB Hard disk. We also need standard keyboard, Mouse, LED Monitor. The system can use Microsoft as the operating system platform. System also makes use of certain GUI tools. To run this application we need JDK 1.7 and above as java platform and Apache tomcat as server. To store data we need MySQL database.
- Operational feasibility review as willingness is the organization for support the proposed system. This may probably the much difficult to feasibility for gauge. It must necessary to understand the management responsibility for proposed project, to obtained operational feasibility. Thus request is initiated through management which hold that there is management support and the system will be accepted and used. Thus may also important that as employee base would be accepting for the change. Identification of money laundering, Prevent from fraud transaction and money laundering and Identification of risk in the transaction all this operations are feasible.

From above data, as shown in graph 7.1, the transaction found into 3 main category i.e. low risk transaction, medium risk transaction and high risk transaction. According to category we seen that 45 transactions were low, 20 transaction were medium and 35 transactions were high.



Graph 1: Number of transaction

III. CONCLUSION

Financial Institutions are imposed by central and local banks to have an effective anti-money laundering system. The automated system for money laundering is still a big challenge. Many data mining solution are used to detect money laundering by analyzing the transaction. In this system we seen that all transaction is divided into 2 category i.e. Proper and fraud transaction. The contribution of the system is in the automation process and finding the suspicious transaction. The enhancement to be made is the chaining of accounts which leads to a system which identifies the relationship between these illegal accounts. This proposed system can identify the risk of money transactions, Money laundering identification and prevent the fraud transaction as well as money laundering in Online Social Network (OSN).

Acknowledgment

This work is supported in advanced and smart money laundering identification system of any state in india . Authors are thankful to Faculty of Engineering and Technology (FET), for providing the facility to carry out the research work.

REFERENCES

[1] Yadong Zhou, Ximi Wang, Junjie Zhang, Peng Zhang, Lili Liu, Huan Jin, Hongbo Jin **Analyzing and Detecting Money-Laundering Accounts in Online Social Networks** 2019 Ministry of Education Key Lab for Intelligent Networks and Network Security.

[2] Seo, Mookyu Park, Haengrok Oh, Kyungho Lee **Money Laundering in the Bitcoin Network: Perspective of Mixing Services** 2019 International Conference on Information and Communication Technology Convergence (ICTC)

[3] Chih-Hua Tai and Tai-Jung Kan **Identifying Money Laundering Accounts** 2019 International Conference on System Science and Engineering (ICSSE).

[4] Cornel Ion erban, stefan Mocanu, Cosmin Popa, Daniela Saru **Dedicated algorithms for risk minimization in suspicious financial transactions** 2019 22nd International

Conference on Control Systems and Computer Science (CSCS).

[5] Bahulkar, A., Baycik, N., O., Sharkey., T. Shen, Y., Szymanski, B., & Wallace, W. (2019). **Integrative Analytics for Detecting and Disrupting Transnational Interdependent Criminal Smuggling, Money, and Money-Laundering Networks** 2019 IEEE International Symposium on Technologies for Homeland Security (HST).

[6] Yaqin Jin ; Zhenxin Qu **“Research on Anti-Money Laundering Hierarchical Model”** 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS).

[7] Sagwadi Mabunda **“Cryptocurrency: The New Face of Cyber Money Laundering”** 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD).