Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Method to Enhance Money Laundering Detection Using Link Analysis

Ch. Suresh*, K. Thammi Reddy
Department of Computer Science and Engineering,
GIT, GITAM University, Visakhapatnam, Andhra Pradesh, India

Abstract— Money laundering is a process by which a person attempts to conceal the nature, location, source and ownership of the processing of their criminal activities. Traditional approaches to anti money laundering follows a labor intensive manual approach. The stages of Money laundering are identification of money laundering incidences, detection, avoidance and surveillance of money laundering activities. A heuristic base approach that uses decision rules for link analysis is presented in this paper. The techniques of Multi-table joins through bit mapped join indices to reduce the processing time is considered so as toincrease ease of accessing of transaction list that can be analyzed for various reports needed by enforcement directorate. As the volume of transaction is huge this work helpsthe expertsin providing possible money laundering transactions.

Keywords— Money Laundering, Data Mining, Link Analysis, Join Indexing, Banking Transactions, Anti Money Laundering.

I. INTRODUCTION

Money laundering is a process by which a person attempts to conceal the nature, location, source and ownership of the proceedings of their criminal activities [9][14]. The Money Laundering is operated in three stages. In first stage, the illegal funds or assets are brought into the financial system called placement and then in second stage layering of the money by the way of distributing into multiple bank accounts through intermediaries look as if it is legitimate. In the third stage laundered funds are re-enter into the legitimate economy and made available as apparently legitimate funds called integration

The estimated amount of money laundered globally in one year is 2-5 percent of the global GDP [17]. Money laundering activities are getting more and more sophisticated taking the advantage of digitalization era of banking system that increased the density of the transactions within seconds. This again cause increase to the criminal activities that raise proceeds for personal benefits, drug, terrorism, high profile corruption cases, scams and smuggling that effect the financial growth of a country as well as the development.

Anti money laundering is defined as a set of procedures, rules and regulations designed to stop the practice of generating income through illegal actions. To assist law enforcement agencies, Prevention of Money Laundering Act became law in 2002 and with it a provision was included that freezing the Indian based assets of any suspected organization and individuals involved in money laundering, For the bank's failure to meet anti money laundering regulations or to allow suspicious transactions to get undetected can have severe impact on any financial entity including damage to its reputation, market capitalization. To detect potential money laundering schemes, the financial institutions are relying on rule based systems.

II. RELATED WORK

Financial institutions are using technology to reach the unreached by the way of Information communication Technology ,but it leads to increase in the volume of data and increase in the use of digital currency. Through credit and debit cards made transactions easy for customers that leads to exponential increase of transactions of data. This increase of data that can be handled by the institutions makes findings of money laundering activities hidden that gives ease for criminals to use financial institutions for these laundering activities to hide the illicit origin.

Traditional approaches to the Anti money laundering followed a labor-intensive manual approach. These approaches can be classified into identification of money laundering incidences, detection, avoidance and surveillance of money laundering activities. Indeed, given that the volumes of banking data and transactions have increased in several ways, such approaches need to be supported by automated systems for detecting money laundering's pattern. The first step is to identify the core functionality necessary in Anti money laundering compliance system to avoid legal and regulatory issues. That must satisfy the regulatory requirements by detecting all the suspicious transactions. As most of the Anti money laundering systems are normally rule based that make the decisions using some sets of predefined rules and thresholds. The technique that focuses on Anti Money Laundering are association rules and anomaly detection. The association rules method uses patterns and associations in the data to create the rules. The rules which are not defined properly can have higher false positive rate. By the association rules having a dataset of millions of transactions, the

models mine transactions of data to find signals that is the patterns that occur frequently for true cases of money laundering, but are rarely present for legitimate customer transactions, where as anomaly detection is well suited for problems with exponentially large and multidimensional datasets such as millions of money in money laundering believe to occur each year [16]. Recently, several suspicious transaction detection techniques have been developed that are based on machine learning algorithms such as Bayesian Networks and clustering. The machine learning techniques will help in acquiring knowledge specific to a particular application. The success depends on the data that is available. In some of the applications the data is added is dynamically causes some more techniques like support vector machine that includes clustering and probability gives the prediction of money laundering activities which are dynamic in nature. Money laundering involved in transactions at four levels, transaction, account, institution, multi-institution.

A simple rule based system can be capable of identifying the initial levels of transactions, accounts and to the max of institution level with the stringent rules construction. To enhance this and identifying the most complex structure of multi institutional we adapt the techniques of Multi-table joins through bitmapped join indices[3] .To link the identified suspicious transaction that reduce the processing time and increase ease of accessing. Bitmap indexing reduces the processing time over hash and tree indices.

III. PROPOSED SYSTEM

Identifying Money Laundering is very difficult task due to vast number of bank transactions were involved .To overcome this problem this paper aims at developing a system which makes use of link analysis to establish the chain of activities that is taken place among the accounts.

We present a heuristic base approach that uses decision rules for link analysis by adapting the techniques of Multi-table joins through bitmapped join indices [3].that reduce the processing time and increase ease of accessing gives transaction list that can be analysed for various reports needed by enforcement directorate. As the volume of transactions is huge this work helps experts by giving possible money laundering transaction.

In this proposed system each individual bank monitors the transaction of the customer accounts and identifies the transaction that poses with the rules of suspicion. The main components of the present approach as shown in figure1 comprising of following major steps.

1. Reporting of identified suspicion transactions.
2. Data pre-processing.
3. Link analysis.

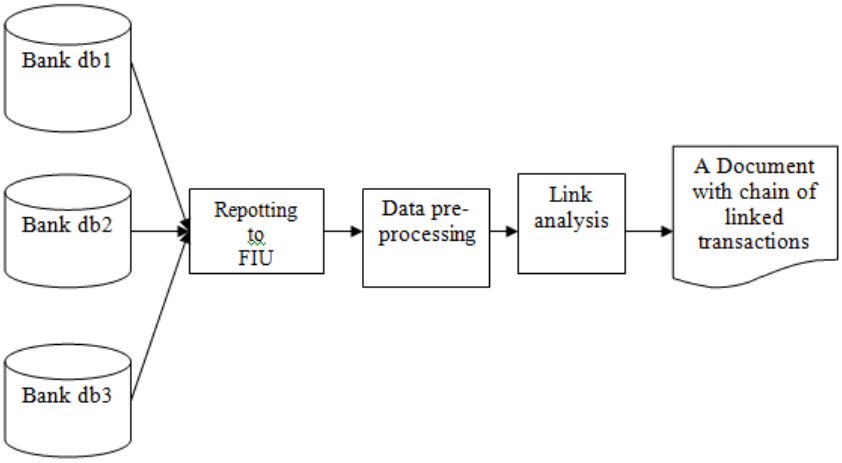

Fig. 1 System Model of a Method to enhance Money laundering detection using Link analysis

3.1 Reporting of Identified Suspicion Transactions:

In this step the identified suspected transaction using the rules of suspicion are reported to the financial intelligence unit by each individual bank regularly. The reason for suspicion of a transaction is due to the value of transaction and the transaction history.

In this system it identifies the transaction of large amount that are debited immediately after being credited to account including the frequent debit transactions of large amount and a customer makes credit/debit transactions that are less than threshold while the sum is equal to a large amount. Frequency of the transaction is taken in a week period

The financial institutes/banks are maintaining the records pertaining to the customers, their transactions and timely identification reports to the Reserve bank of India.

3.2 Date Pre-processing:

In this step the transactions which are identified as suspicious by the financial institutions are reported to the financial investigation unit. The financial investigation unit database consists of multiple transactions from various financial institutions containing information about the customer and his/her details. For further process only few fields are necessary from the transactions. In the Data pre processing the suspicious transactions are cleaned from noise inconsistency and incompleteness of various techniques are applied on the transaction dataset by removing irrelevant attributes, noise etc.

The financial datasets are managed in distributed manner .The privacy and security of the data needs to be provided .To achieve data quality we need to pre-process the financial data set.

In the transaction database the irrelevant information is removed by selection of only required fields for identification of suspicious transaction and linking correspondingly. For example details like amount, transaction_id, from_account, to account, frequency are considered of identifying suspicious transaction. The reported transactions are grouped into a timing window of 15 day, In the project implementation we considered a suspicious_15 table, suspicious_today and history tables for the grouping data for the given transaction date.

As described above for the linking of transactions to identify suspicious account, the attributes we consider are given below

Table 1: Linking of transactions to identify suspicious accounts

From Account	To Account	Transaction Date	Amount	Transaction ID
53410953	39246848	6-May-14	47592	16636
56871851	53410953	19-Apr-14	48027	14380
69697333	56871851	15-Apr-14	68873	14022
75368211	69697333	6-Apr-14	52398	13001
51075762	75368211	7-Apr-14	56300	13108

3.3 Link Analysis:

Link analysis identifies and measures how closely an account is connected with known suspicious accounts. The flow and connections of transactions among various accounts are traced and the authenticity of transactions is questioned. For example in the case of suspicious Money laundering money originates from one account to various accounts and integrated back to a single account. Often these accounts share common characteristics, such as phone numbers or work addresses. Using link analysis, even subtle connections between accounts can help identify suspicious relationships. This linking of transaction benefits the experts to study the common characteristics of the transactions.

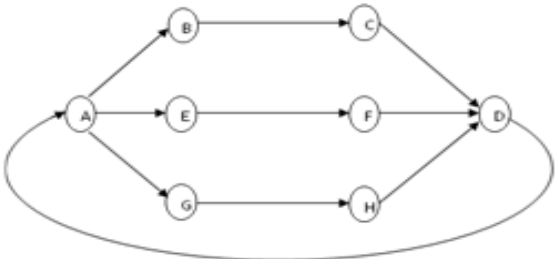

Fig 2: Process of Money laundering Activity if a cycle exists we can say Money laundering was occurred

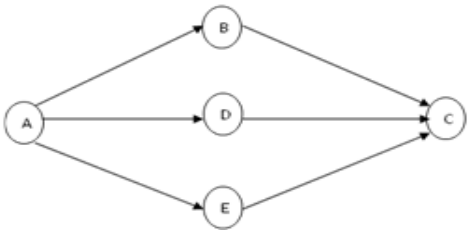

Fig 3: Process of Money laundering Activity in case of non cyclic transactions further study are needed

The transaction lists received at financial intelligence unit are analysed with the transaction that happened earlier so as to link the money laundering activities. Every transaction in the database are treated as a node, each node is linked with the past transaction by checking the too and fro transactions. Transactions are thus linked to give the suspicious accounts.

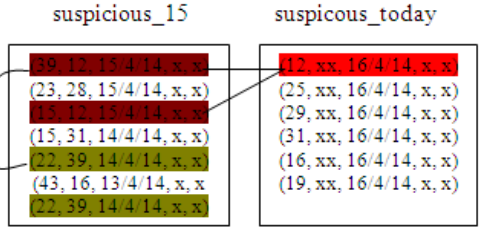

Fig 4: Suspicious transactions tables

In the above figure suspicious_today is a table with current day suspicious transactions in which the first transaction is considered as a node, in this we check the from_account_id search and maps it to the to_account_id of suspicious_15 table and repeats this until it is done with all the 15 days transactions, through this links or edges we can construct a graph where the flow of the transactions is discovered.

Algorithm 1: Finding Suspicious Transaction
Input Transaction dataset, 'd'
Output: list of suspicious transactions, 's'
Step1: for each transaction entry e Є do
Step2: check the amount and cal (week, freq);
Step3: Count Trans_id)
Step4: If freq_diff=0 Add(e)
Step4: On saving: updated and stored on DB
Step5: On reporting: transaction list is moved to FIU

The transaction reported at financial intelligence are grouped into a fixed timing window that are used to link with each current day transactions to originate the transactions by forming chain of transaction that can be analyzed to know the money laundered happened.

Algorithm 2: Linking the Suspicious Transaction
Input: List of suspicious transactions, 's'
Output: linking of given suspicious transactions, 'l'
Step1: for each suspicious transaction e ∈ do
Step 2: originatingaccount = currentAccount
Step3: for each suspicous transaction t in 15 days
Step4: if t.toaccountnumber = currentaccountnumber
Step5: if t.fromaccountnumber = currentaccountnumber
Step6: add (link)
Step7: repeat until there is no 's'

IV. EXPERIMENTAL ANALYSIS

The proposed system considers 20000 transactions of multiple banks over a period of 120 days. A suspicion of the transaction is flagged by considering the rules given in "The prevention of Money Laundering Act, 2002(PMLA)"i.e Activity in account, Identity of client, Background of client, Multiple accounts, Nature of transactions, Value of transactions. These flagged suspicious transactions are reported to the law enforcement cell that stores and groups the transactions using a fixed timing window, say 15 days to 30 days.

Linking enhances the identification by measuring the connection between the known suspicious transactions. A suspicious transaction of a current day is linked with known suspicious transaction in a fixed time frame.(i.e. transaction that are directed to the recent suspicious transactions) constructing a chain of transactions helps investigators in analysing and generating reports of Money Laundering.

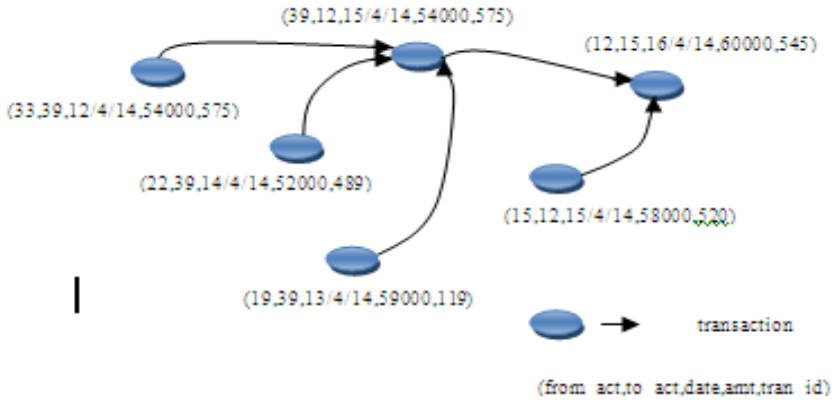

Fig 5: Suspicious transactions linking

In the above figure, the transactions are linked to form a chain in which the abstract details of the suspicious transactions are viewed which helps the investigators in identifying the flow of money which can be used as evidence. Know your customer (KYC) data is maintained by banks in connection with each client is used as domain-Knowledge to

construct a ontology that can derive the possible social relationship among the player by the logical reasoning developed through details of client In experiments the output of suspicious transaction is studied by testing the developed application with the data set of different size, and suspected number of transaction are figured.

Table 2: No of transactions found suspicious

S.No	Size of dataset	Legal	Suspected
1	5000	4547	453
2	10000	8857	1143
3	15000	13049	1951
4	20000	15504	2496

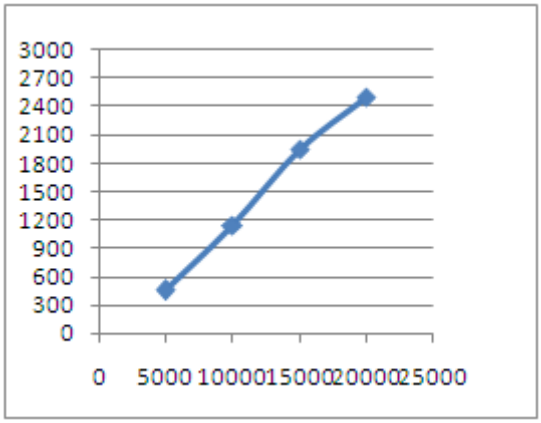

Fig 6: Graph shows suspected transactions

From the graph, it is clearly found that when number of transactions is increased there is an increase in the number of suspicious transactions also. It can be observed that it is linear in nature; it means there is a great chance of money laundering which can be future investigated

In experiments for linking the above identified transaction the output for each suspicious transaction linking the number of linked transaction is studied over the different size of timing window. We can increase the size of timing window (n+1) to check the clean transaction of timing window (n) which can give further validation to the suspicious transactions.

Table 3: No of transactions linked

S.No	Size of window in days	Number of links
1	7	89
2	15	179
3	30	386

From the graph, it is clearly found that when the size of the window is increased there is an increase in number of links also. We can increase the size of the timing window (n+1) to check the clean transaction of timing window (n) which can give further validation to suspicious transactions involved in money laundering.

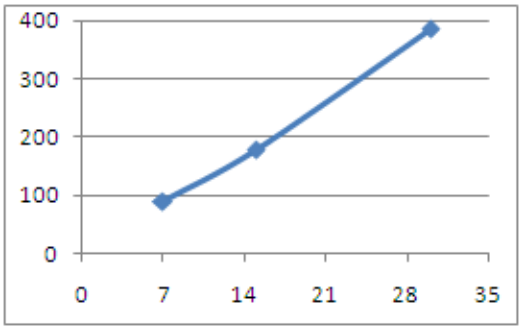

Fig 7: A Graph for linking of transactions

V. CONCLUSION

The link analysis based Anti money laundering system proposed by the authors can able to identify the suspicious transactions successfully. This method adopts a system of linking of transactions such a way that a cycle is formed. Using which the link, can be established among the accounts. A timing window of 7, 15, 30 days were considered on a 20,000 transaction data base. The results achieved by the proposed system were successful in identifying the cases of money laundering

REFERENCES

[1] EoghanCasey,"Digital Evidences and computer crime". Elsevier publishers, 2011.
[2] John R Vacca,"Computer Forensics Fundamentals". y Charles River Media publishers,2005.
[3] Patrick O'Neil, Goetz Graefe, "Multi-Table Joins Through Bitmapped Join Indices", *Microsoft corp SIGMOD Record, Vol.24, No.3, September 1995.*
[4] Nhien An le Khac,SameerMarkos,M.TeharKechadi,"A data mining based solution for detecting suspicious money laundering cases in an investment bank",*IEEE computer society 2010*
[5] Nhien An le Khac, M.TeharKechadi,"Applications of Data mining for Anti-Money Laundering Detection: A Case Study", *IEEE International Conference on Data-Mining workshop 2010*
[6] R.CoryWatkins,K.MichaelReynolds,RonDemara,"Tracking Dirty proceeds:Exploring Data Mining Technologies as tools to investigate Money laundering",*police practice and Research 2003*
[7] PankajRichhariya,Prashant.K.Singh,EnduDuneja,"A Survey on financial fraud detection methodologies",*International journal of commerce business and management 2012*
[8] Krzysztof Michalak,JerzyKorczak,"Graph Mining Approach to Suspicious TranscationDetection",*Computer science and information system IEEE 2011*
[9] Nhien An le Khac,SameerMarkos,M-Teharkechadi ,"An efficient search tool for an Anti-Money Laundering:Application of an Multi-national banks dataset", world Academy of Science,Engineering and Technology 2009.
[10] HenryG.Goldberg,RaphaelW.H.Wang,"RestructuringTranscational data for link analysis in the Fincen AI system",AAAI Technical report 1998
[11] NhienAn Le Khac, SammerMarkos, M. O'Neill, A. Brabazon and M-TaharKechadi. "An investigation into Data Mining approaches for Anti Money". IACSIT Press, Singapore, International conference on computer Engineering & Applications IPCSIT vol.2 2011
[12] Zhongfei (Mark) Zhang, John J. Salerno. "Applying Data Mining in Investigating Money Laundering Crime".IEEE International Conference on Data Mining Workshops,, 2010.
[13] Quratulain Rajput1, NidaSadaf Khan1, Asma Larik1 &Sajjad Haider1"Ontology Based Expert-System for Suspicious Transactions Detection". Canadian Center of Science and Education , Computer and information science, Vol. 7, No. 1; 2014
[14] Gordon Ho,"Money Laundering Detection". Ac 626 Term Report, Springer 2008
[15] Rajesh Menon,SanjayaKumar,"Understanding the role of Technology in Anti Money Laundering Compliance",Infosys white paper 2005
[16] "Anti-Money Laundering:Enhancing effectiveness with anamolydetection,rules and Link analysis",Opera solutions 2012

