The International Journal Of Engineering And Science (IJES)
||Volume|| 3 ||Issue|| 01 || Pages || 43-47 || 2014 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

An Multi-Variant Relational Model for Money Laundering Identification using Time Series Data Set

[1,] G.Krishnapriya M.C.A., M.Phil, [2,] Dr.M.Prabakaran
[1,] *Research Scholar, Bharathidasan University,Trichy-620001.*
[2,] *Assistant Professor, Department of Computer Science Government Arts College, Ariyalur, Tamil Nadu, India.*

----------ABSTRACT----------

Money laundering an unfair money transaction activity which threats the finance industries in higher rate. The illegal commercial peoples and terrorist, transfers huge amount into a single or many accounts, and it follows a big chain of accounts to reach the destination to which it has to be sent. Generally the financial banks enforce many restrictions to transfer amounts between accounts where they are done between internal or external accounts of the country. Identifying money laundering is a challenging task where the origin of transaction could not be identified easily when it follows a big chain or transferred as number of small amounts. There are methods discussed, which detects MI based on amount transferred and other factors. They suffer with the accuracy of MI detection and time complexity values. We propose a relational model which uses multiple factors and metrics to detect the money laundering. The proposed method uses time series data and identifies one-many and many-one relation between transactions to select vulnerable accounts. Identified vulnerable accounts and transactions of those accounts are split into different time frames and analyzed at each time frame to identify the presence of money laundering. The proposed method has produced higher accuracy in MI detection and has less time complexity which improves the performance of the method proposed.

Index Terms: *Network security, Money Laundering, Relational Model, Multi-Variant*

Date of Submission: 24 December 2013 ⟺ Date of Acceptance: 10 January 2014

I. INTRODUCTION:

Money Laundering represent the capability of the central government and the faith of the nation, as well as an important measure fighting organized crimes and forestalling the flooding of nation-crossed corruptions. However, the construction of an effective AML mechanism is just at its startup which is far from perfect. Money laundering threatens the economic and social development of countries. The threat is due to the injection of illegal proceeds into the legitimate financial system. Due to the high amount of transactions and the variety of money laundering tricks and techniques, it is difficult for the authorities to detect money laundering and prosecute the wrongdoers. Thus, it is not only the amount of transactions, but the ever changing characteristics of the methods used to launder money that are constantly being modified by the fraudsters, which makes this problem interesting to study.

Money laundering (ML) is a process of disguising the illicit origin of "dirty" money and makes them appear legitimate. It has been defined by Genzman 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 or to conceal or disguise the nature location, source, ownership, or control of these proceeds. Through money laundering, criminals try to convert monetary proceeds derived from illicit activities into “clean” funds using a legal medium such as large investment or pension funds hosted in retail or investment banks. This type of criminal activity is getting more and more sophisticated and seems to have moved from the cliché of drug trafficking to financing terrorism and surely not forgetting personal gain. Today, ML is the third largest “Business” in the world after Currency Exchange and Auto Industry. According to the United Nations Office on Drug and Crime, worldwide value of laundered money in a year ranges from $500 billion to $1 trillion and from this approximately $400-450 Billion is associated with drug trafficking. These figures are at times modest and are partially fabricated using statistical models, as no one exactly knows the true value of money laundering, one can only forecast according to the fraud that has already been exposed. Nowadays, it poses a serious threat not only to financial institutions but also to the nations. Some risks faced by financial institutions can be listed as reputation risk, operational risk, concentration risk and legal risk. At the society level, ML could provide the fuel for drug dealers, terrorists, arms dealers and other criminals to operate and expand their criminal enterprises. Hence, the governments, financial regulators require financial institutions to implement processes and procedures to prevent/detect money laundering as well as the financing of terrorism and other illicit activities that money launderers are involved in. Therefore, anti-money laundering (AML) is of critical significance to national financial stability and international security.

The relational model is one which represents the transaction using relational concepts. For example in an organization they maintain address of different employees and here the employee's names have relation with the address of the employee which shows the one-one relation. If we group the employees in form of department they work, then all employees in the group are related with the department which shows the many –one relation. In case of money laundering we can say that money laundering could follow one of the above discussed functional models.

Identifying the money laundering frauds using single feature will not be effective because at any point of time the single valued attribute fails to identify the money laundering. We use multiple attributes to identify the money laundering.

Banks collect detailed personal information from their clients as well as information such as the relations between clients and the association between clients and certain companies. Data mining systems are used to extract interesting and valuable information from the large database. Relations among clients and companies, accompanied with monetary transaction histories, could be used as effective indication of suspicious money laundering activities.

Related works:

Research on anti-money laundering based on core decision tree algorithm [9],presents a core decision tree algorithm to identify money laundering activities. The clustering algorithm is the combination of BIRCH and K-means. In this method, decision tree of data mining technology is applied to anti-money-laundering filed after research of money laundering features. We select an appropriate identifying strategy to discover typical money laundering patterns and money laundering rules. Consequently, with the core decision tree algorithm, we can identify abnormal transaction data more effectively.

Laundering Sexual Deviance: Targeting Online Pornography through Anti-money Laundering [1], concentrates on cyber-pornography/obscenity, which encompasses online publications or distribution of sexually explicit material in breach of the English obscenity and indecency laws. After examining the major deficiencies of the attempts to restrict illegal pornographic representations, the authors aim to highlight that the debate regarding their availability in the Internet era neglects the lucrative nature of the circulation of such material, which can be also targeted through anti-money laundering. Rising profits fuel the need to recycle the money back into the legal financial system, with a view to concealing their illegal origin. Anti-money laundering laws require disclosure of any ¡suspicion¢ related to money laundering, thus opening another door for law enforcement to reach the criminal.

Combining Digital Forensic Practices and Database Analysis as an Anti-Money Laundering Strategy for Financial Institution [11], propose an anti-money laundering model by combining digital forensics practices along with database tools and database analysis methodologies. As consequence, admissible Suspicious Activity Reports (SARs) can be generated, based on evidence obtained from forensically analyzing database financial logs in compliance with Know-Your-Customer policies for money laundering detection.

The State of Phishing Attacks, [12], discusses about phishing which is a kind of social-engineering attack where criminals use spoofed email messages to trick people into sharing sensitive information or installing malware on their computers. Victims perceive these messages as being associated with a trusted brand, while in reality they are only the work of con artists. Rather than directly target the systems people use, phishing attacks target the people using the systems. Phishing cleverly circumvents the vast majority of an organization's or individual's security measures. It doesn't matter how many firewalls, encryption software, certificates, or two-factor authentication mechanisms an organization has if the person behind the keyboard falls for a phish.

Event-based approach to money laundering data analysis and visualization [13], discusses crime specific event patterns which are crucial in detecting potential relationships among suspects in criminal networks. However, current link analysis tools commonly used in detection do not utilize such patterns for detecting various types of crimes. These analysis tools usually provide generic functions for all types of crimes and heavily rely on the user's expertise on the domain knowledge of the crime for successful detection. As a result, they are less effective in detecting patterns in certain crimes. In addition, substantial effort is also required for analyzing vast amount of crime data and visualizing the structural views of the entire criminal network. In order to alleviate these problems, an event-based approach to money laundering data analysis and visualization is proposed.

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names [14], explore this unique characteristic further, using heuristic clustering to group Bitcoin wallets based on evidence of shared authority, and then using re-identification attacks (i.e., empirical purchasing of goods and services) to classify the operators of those clusters. From this analysis, we characterize longitudinal changes in the Bitcoin market, the stresses these changes are placing on the system, and the challenges for those seeking to use Bitcoin for criminal or fraudulent purposes at scale.

Concurrently with the Evaluating User Privacy in Bitcoin [2] applied a similar analysis, but focused more squarely on privacy concerns. Unlike Ron and Shamir, their analysis attempts to account for the complexity of "change" accounts which are central to how Bitcoin is used in practice.

Proposed Method:

The proposed money laundering identification method uses relational factors and other metrics, which has been collected from the transactional data set. It has three stages namely: Preprocessing, Relational Mapping, Multi-Variant ML Identification. We discuss each of the process in coming chapters.

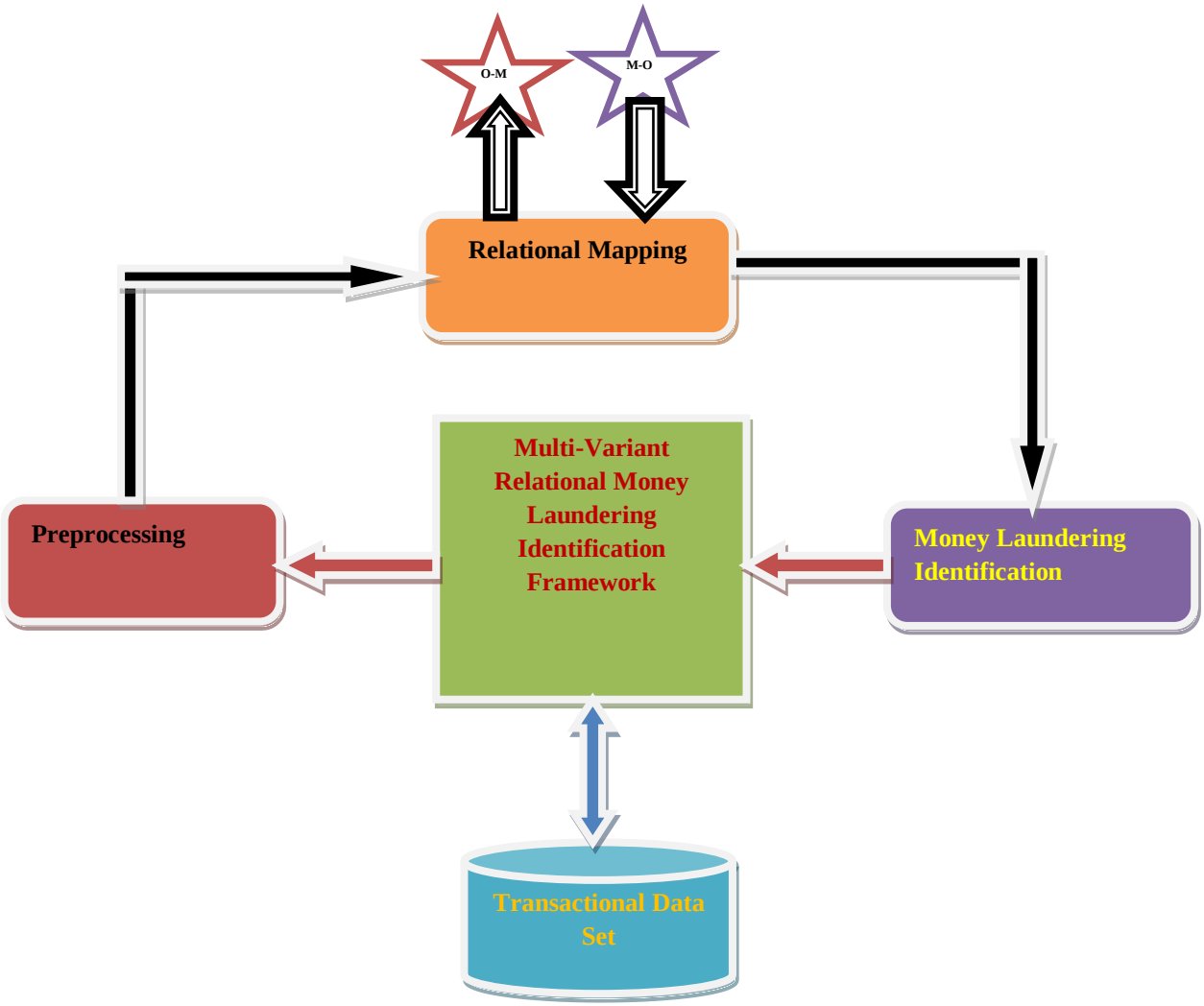


Figure1: shows the proposed system architecture.

II. PREPROCESSING:

The transactional data set has many attributes and the log size is heavier to process. The retrieved log will be a noisy one to process, so that we remove the incomplete log to make it compatible for processing. The transactional log of different banking sectors has different attribute set and different pattern. The preprocessor has a general pattern for processing and the retrieved patterns are converted into the generalized form. Because an banking log may have the account identity as the last attribute and the customer id as the first attribute in its log , but will differ in another bank log. The converted transactional data sets are taken to the next stage of money laundering identification process.

Algorithm

Step 1: start
Step 2: read transactional data set T_s , Attribute set A_s.
Step3: initialize generalize pattern Tp.
Step 3: for each transaction T_i from T_s.
For each pattern p from T_s
Extract attribute $Tp(A_i)$.
$TP(A_i) = Ô(T_i(A_i))$.//Ô-Index of the Attribute A_i.
If T_i € A_i then
Else
$T_s = ø(T_i(T_s))$.
End
End
End.
Step 4: end

III. RELATIONAL MAPPING:

The relational mapping is performed on the preprocessed data set. We separate the transactions which are distinct to unique accounts. From the separated set of transactions, for each of the account identified we collect the set of accounts linked to the particular account. We compute relational metrics as one-to-many which indicates the number of transactions sent from this account and many-to-one specifies the number of account from where there is money transfer.

Algorithm:

Step1: start
Step2: initialize relational set Rs.
Step3: read transactional set Ts.
Step4: select distinct account DA from Ts.
DA = Õ(Ts).
Step5: for each account DA_i from DA
Identify subset of transactions related to DA_i.
ST_s = Ü(DA×DA_i).
Identify relational mappings Im.
Im = Ø(ST_s).
$Rs_{(i)}$ = Im.
End.
Step6: stop.

IV. MONEY LAUNDERING IDENTIFICATION:

The process of money laundering identification is performed based on Number of transactions and amount transferred at each time frame. The transactional data set is a time series data which can be used to detect the money laundering identification. The relational mappings generated at the previous stage are used as an input to this process. From the relational mapping Rs , we split the transactions which is performed at each time frame TF. We compute the overall amount transferred at one-to-many and many-to-one relations based on which the transaction is decided as a vulnerable one. At any time frame if the number of transaction or the amount is higher than the Transactional Threshold TT, Transactional Amount Threshold TAT then the transaction is considered as a vulnerable one. In one too many cases the Transactional Threshold which implicates the maximum number of transactions can be performed at each time frame is considered with the maximum cumulative amount based on TAT is used.

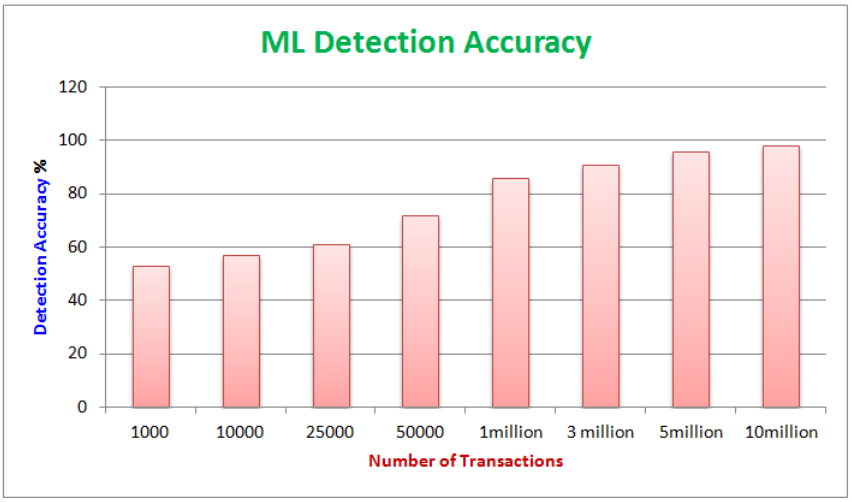
Algorithm:

Step1: start
Step2: initialize TAT, TF, TT.
TF=24 Hours.
TAT = 50,000.
TT = 100.
Step3: read Relational Mapping Rs.
Step4: split the transactions from Rs according to time frame TF.
TFT = $(Rs×Ts).
Step5: compute no. of outgoing transaction OT.
OT = ð(TFT).
Compute overall money transferred mt.
Mt = $\Sigma OT(amount)_{1...N}$
If Mt> TAT then

Back Track the transaction using back propagation.
end
Step6: compute no. of incoming transaction IT.
IT = ð(TFT).
Compute overall money transferred mt.
Mt = $\Sigma IT(amount)_{1...N}$
If Mt> TAT then
Forward Track the transaction using traversal.
End
Step7: stop.

V. RESULTS AND DISCUSSION:

The proposed method has been evaluated using various transactional set collected from different banking sectors and we have separated the accounts which are linked through different banks. Finally we have collected 5000 accounts from different banks having 10 million transactions. The proposed method has produced efficient results and detection accuracy is also higher.



Graph 1: shows the efficiency of identifying money laundering

The graph1 shows the efficiency of identifying money laundering with respect to number of transaction used. It is clear that the efficiency is increased if the size of transaction is increased. The proposed methodology produces efficient result by increasing the size of transaction.

VI. CONCLUSION:

We analyze various methodologies to identify money laundering crime. We identify that all methods have scalable in accuracy and efficiency. We proposed a multi variant relational model which uses time variant transactional data. The proposed method has produced higher efficient results and with accurate findings. The proposed method has produced results with less time complexity.

REFERENCES:

[1] John Hunt. The new frontier of money laundering: how terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them. Information & Communications Technology Law, 20(2):133{152, June 2011.

[2] L I U Junqiang. Optimal Anonymization for Transac tion. Chinese Journal of Electronics, 20(2), 2011.

[3] P.J. Lin, B. Samadi, Alan Cipolone, D.R. Jeske, Sean Cox, C. Rendon, Douglas Holt, and Rui Xiao. Development of a synthetic data set generator for building and testing information discovery systems. In Information Technology: New Generations, 2006. ITNG 2006. Third International Conference on, pages 707-712. IEEE, 2006.

[4] C M Macal and M J North. Tutorial on agent-based modelling and simulation. Journal of Simulation, 4(3):151{162, September 2010.

[5] Dan Magnusson. The costs of implementing the anti-money laundering regulations in Sweden. Journal of Money Laundering Control, 12(2):101{112, 2009.

[6] J Pavon, M Arroyo, S Hassan, and C Sansores. Agent-based modelling and simulation for the analysis of social patterns. Pattern Recognition Letters, 29(8):1039-1048, June 2008.

[7] Agus Sudjianto, Sheela Nair, Ming Yuan, Aijun Zhang, Daniel Kern, and Fernando Cela-Daz. Statistical Methods for Fighting Financial Crimes. Technometrics, 52(1):5{19, February 2010.

[8] Yabo Xu, Ke Wang, Ada Wai-chee Fu, Hong Kong, and Philip S Yu. Anonymizing Transaction Databases for Publication. International Journal, pages 767-775, 2008.

[9] Rui Liu, Research on anti-money laundering based on core decision tree algorithm, IEEE Conference on Control and Decisions , pp:4322-4335, 2011.

[10] Odense, Laundering Sexual Deviance: Targeting Online Pornography through Anti-money Laundering, European Intelligence and Security Informatics Conference, 2012.

[11] Bucharest, Combining Digital Forensic Practices and Database Analysis as an Anti-Money Laundering Strategy for Financial Institutions, Third International Conference on Emerging Intelligent Data and Web Technologies, 2012.

[12] Jason Hong, The State of Phishing Attacks, Communications of the ACM, Vol. 55 No. 1, Pages 74-81, 2012.

[13] Tat-Man Cheong, Event-based approach to money laundering data analysis and visualization, Proceedings of the 3rd International Symposium on Visual Information Communication, ACM , 2010.

[14] Sarah Meiklejohn, A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, ACM 2013.

[15] E. Androulaki, G. Karame, M. Roeschlin, T. Scherer, and S. Capkun. Evaluating User Privacy in Bitcoin. In Proceedings of Financial Cryptography 2013, 2013.

[16] I. Miers, C. Garman, M. Green, and A. D. Rubin. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In Proceedings of the IEEE Symposium on Security and Privacy, 2013.

[17] T. Moore and N. Christin. Beware the Middleman: Empirica Analysis of Bitcoin-Exchange Risk. In Proceedings of Financial Cryptography 2013, 2013.