International Journal of Engineering & Technology, 7 (3.10) (2018) 10-13

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Dynamic Approach for Detection of Suspicious Transactions in Money Laundering

Anagha A Rao[1], Kanchana V[2]

[1, 2]Department Of Computer Science
[1, 2]Amrita Vishwa Vidyapeetham,
[1, 2]Amrita School Of Arts And Sciences
Mysore, India
[*]Corresponding author E-mail: anaghaarunbg@gmail.com[1]

Abstract

In the previous year, India has been among the most active nations in venturing up the battle against money laundering and related financial and security issues. The effort that likely got the most consideration was "demonetization" approach which intended to evacuate around 85% of the aggregate illegal cash available for use. To survey India's overall anti-money laundering (AML) system, it's more essential to center on the fundamental legitimate structure set up. In this paper, the proposed methodology is to analyze the user transactions and characterize based on their behavior of transactions. Then it focuses on the characterized transactions and obtains the connectivity among different accounts. To predict the suspicious transactions, we examine the log or trends found in previous years transactions of the user. By comparing the obtained data with the previous data, we will be able to predict suspicious transactions, providing the details are moved for further investigation.

Keywords: *Anti Money Laundering; Directed Acyclic Graph; Graphical Theoretic Approach; Hash Based Technique; Money laundering;*

1. Introduction

Money Laundering is a practice of converting illegal profits as legal; in money laundering, criminal tries to exchange financial profits originated from illegal sources to "legal or clean" profits by lawful act as such investing in large business enterprise hosted by private financial institutions. This kind of illegal actions is becoming more complex and it seems to have motivated the launders in drug trafficking, financial terrorism and undoubtedly for individual growth [1]. There are several ways of money laundering. Criminals will conceal the stock of illegal funds by investing it in real estate purchase, gambling house (casino) or in commodities like jewels, diamonds etc. In common, the money laundering process is involving three main steps: placement, layering and integration. Introducing the unclean money into the financial system through various means is the placement process. Making a series of transactions to form a complex level structure in concealing the supply of the funds is layering process. Lastly integration is the final stages were the funds are back to the launder through reputable source, the scheme of making complex transactions will mislead the investigation units. [2].

In India, most of the money laundering cases involves the well-known Politicians, shell companies, real estate, casino laundering etc. Some of the cases that have been encountered and investigated recently in India are, In February'18 Karti Chidambaram was arrested in INX money laundering case and other two people who were involved in the same. In July'17 Misha Bharti and her husband were arrested for laundering 1.2cr through shell firms, and the list goes on [3], [4]. The measures that are taken by Reserve Bank of India (RBI) to reduce the problem by providing the banks with certain guidelines:

1. "Monitoring the Transactions": The huge transactions and odd patterns in the accounts which have no noticeable lawful purpose and the ones which exceed the limits are paid more attention.
2. "Maintenance of Transaction Records": where the banks must record the nature of transactions, the sum of the transaction and the currency in which it was termed, date of transaction conducted and the parties to the transaction [5].

2. Related Works

Prashant K. Singh, Pankaj Richhariya, EnduDuneja put light upon scam recognition that is overdue to rise and quick growth of E-commerce, economic fraud cases associated with it is correspondingly growing this marks in hiding of millions of currencies globally every year. In this paper, they have given a complete review on various detection processes which involves online sale scam, credit card suspicious transaction detection, telecommunication con detection, and computer interference system. The intrusion detection system must have the exact environment to be monitored, this is the main disadvantage and the system cannot be ported from one place to another due to the above reason [6].

R.cory Watkins K. Michaelreynolds, Ron Demara documented that, from the instance of the act that frauds try to state that money that is laundered are similar resources originated from legal actions and cannot be discriminated on the whole. Usual analytical approaches that are developed to find out trends in money laundering can be separated as different types like recognition, avoidance of discovery and management, clustering algorithms for studying subset selection, information were explored with varied algorithms [7].

M.S.Chen, J.S.Parkand P.S.Yu has examined about the problem in mining association rules were huge datasets of business transactions are used. They have mentioned that the problem is raised in reducing the large dataset. It can be solved by developing the candidate item sets where only the required datasets are obtained. By using this method, the database can be successfully trimmed at the early stages of detection process at lesser cost [8].

M. Kamber and Jiawei Han in this work they focused on improvising the efficiency of Apriori algorithm, and then formulating the Hash-based technique which is used to reduce the dimension of the candidate n-item set, Nk, for n> 1 [9].

Yu Tingting and Liu Keyan projected about the identification of varying financial transaction using vector machine that supports the overall process. The use of support vector classification method that uses random collection as its parameter will disturb the accuracy of results. So they included the process of involving more level of authentication in other words cross validation to choose the suitable constraints [10].

Yang Qifeng, Feng Bin, Song Ping declared in their article that online transaction is a practical way to gain currency with the growth of e-commerce. They have developed an anti-money laundering scheme as trade unification system. The system will dynamically observe and investigate business transaction records, and also presents the opinion based on decision support for anti-money laundering scheme. Also they carry out the content based reduction in online social networks; fire wall construction is developed for the same. In this design, content mining technique is used to classify the receiving texts [11].

R.V.S. Balan and Sreekumar has investigated different information mining methods that are utilized to distinguish tax evasion, which comprises of colossal measures of keeping money exchange information from everyday exercises. They gave an understanding [12].

Xingrong Luo in his paper he proposed about the organized view of money laundering framework in data mining, and the efficiency of using classification algorithm to predict the suspiciousness in the transactions. Particularly, he views the bank transaction as data stream which is built using the frequent mining rules based on the classifiers. His experiments based on the replicated trading using real time bank transactions provide the efficiency in detection procedure [13].

Balsa J and Alexandre C propose a framework that spotlights on how monetary foundations, banks, can show signs of improvement bring against illegal tax avoidance activities. All the more particularly, we endeavor to enhance the way toward flagging suspicious exchanges and the subsequent official conclusion. For this reason, it is essential to show customer conduct and have an unmistakable meaning of various customer profiles. Since they have a genuine arrangement of bank exchange information, they will clarify in this paper how a few information mining strategies have been utilized to make the essential customer profiles and how the outcomes can be coordinated into the framework [14].

Dr.M.Prabakaran and G.KrishnaPriya in their paper they proposed a variation of time declaration utilizing behavioral models where exchange cycles are part and different threads and relying upon the client models of record. On this approach, they distinguish and suspect, as well as recognize the group exchanges that are associated with the ML [15].

Nhien An Le Khac et al. developed a solution using decision tree, genetic algorithm and fuzzy clustering. These were the different data mining techniques proposed to detect money laundering for quick identification. These articles included methods were in they proposed the significant factors for detecting money laundering in the speculation behavior and they also determined an investigating procedure depending on clustering and neural networks to detect cases which are suspicious in money laundering [16], [17], [18].

3. Methodology

In the proposed work, the aim is to detect the large cash withdrawals from a previously inactive or from an account which has just received a sudden large credit, initially the non-frequently used accounts are obtained, and then the connection of those accounts with other accounts is detected to find the total predictable amount involved. Finally, the accounts exceeding the limit with inactive usage of account with large amount are diagnosed as suspicious. Following are the steps carried to effectively predict the suspicious transactions.

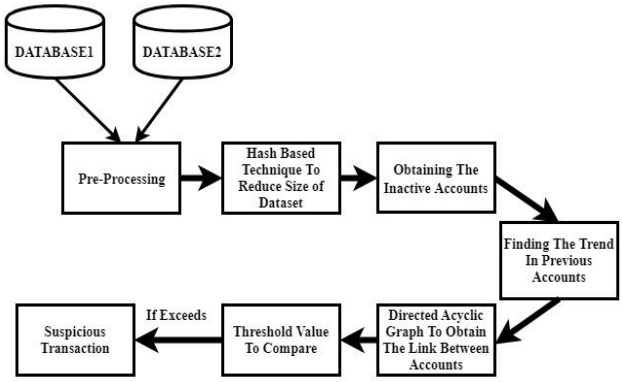

Fig. 1: Architectural diagram

3.1. Technique to Reduce Candidate 2 Item Set Using Hash Based Mining

In this article, the proposed methodology uses Hash based association rule to reduce the size if the dataset and for generating non-frequent transactional datasets. The transaction item sets in the hash table are checked with the min support count and hence the duplicate transactions are discarded. This makes the task easier to generate the no frequent item set. Transitivity rule is applied to the accounts showing only two accounts being involved in a transaction, this produces the chaining of accounts and this rule is adopted from the mathematical transitive relation i.e., if account A is related to B, the B is related to C and A is also related to C.

3.1.1. Generating the Non-Frequent Candidate 2-Item Set

Step 1: Extract the transactional dataset as per the time constrain.
Step 2: Calculate the association between all accounts using hash based technique.

$$H(A,B) = (Order\ of\ A \times 10) + (Order\ of\ B) \bmod 7 \quad (1)$$

Step 3: If (Count < minbucketcount) (2)

Step 4: Consider the reduced transactions for further identification.

Step 5: If (Support count < minsupportcount) (3)

Then, inactive transaction
Else Active

3.2. Identifying Suspicious Transactions

Identifying the transactions depends on the behavior of the user, there are many possible patterns were a user will launder money. Here inactive accounts were bulk amount is credited and within few hours the amount is debited or transferred to other account is considered. To identify such activity, the directed acyclic graphical approach is adopted. This approach helps in solving the complex dependencies between the accounts. The sequential connections between the accounts help in generating the possible longest paths were in, the accounts and the money involved can be predicted as suspicious.

3.2.1 Suspicious Behavior

Step 1: Retrieve shared information from the database (Account1)
Step 2: Tokenization of non-active accounts.
Step 3: Clustering the transactional trend followed by the user comparing with the predefined dataset (Recorded in database).
Step 4: Check for the links between the accounts.
Step 5: Identify the user as suspicious if the total transactional amount increases the threshold value specified by the banks.

Finally, we identify the common and uncommon behaviors of the user accounts. The experimental results presented in this article show the efficiency of methods in the upcoming sections.

4. Experimental Results

Table 1: Results obtained for different size of datasets

Sl no.	Dataset size	Min. Bucket count up	Min. Support count up	Number of suspicious transactions
1	29	2	2	3
2	100	3	7	8

For experimental use of the proposed algorithm, a representation dataset having the similar features of connection and relationships like a typical bank transaction has been used. Since original bank transactions are highly confidential to be used. The end result that we get at the end of the experiment using hashing method, we monitor that when the amount of transactions size increases, the complexity in finding the non-frequently used accounts increases. Yet if the support count rate is increased to a higher rate than a lesser number of transactions are obtained. With added datasets the efficiency of the tool becomes even more accurate. The graph shows Size of dataset (x-axis), Number of suspicious accounts (y-axis).

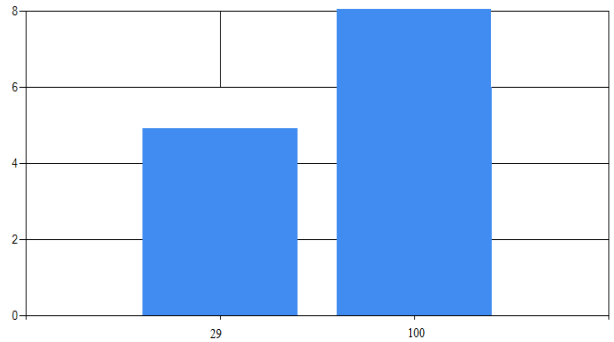

Fig. 2: Size of dataset (x-axis), Number of suspicious accounts (y-axis)

The algorithm is implemented on the connection of all the data and the algorithm outputs the common and uncommon behaviors which are used for suspicious account prediction. The framework shows precision for the model dataset with some limitations. Only the pattern which is designed to be predicted is identified. Since there are various ways in which the problem takes place not all patterns are considered. The below graph be the results for month (x-axis), Amount (y-axis) based on the varying transactions of accounts obtained from the experiment, showing their overall monthly transaction and we notice that the transactions of account 1, 3 and 5 are showing involvement of huge amount compared to the other month, this means that they are suspicious and must be reported only for further investigation.

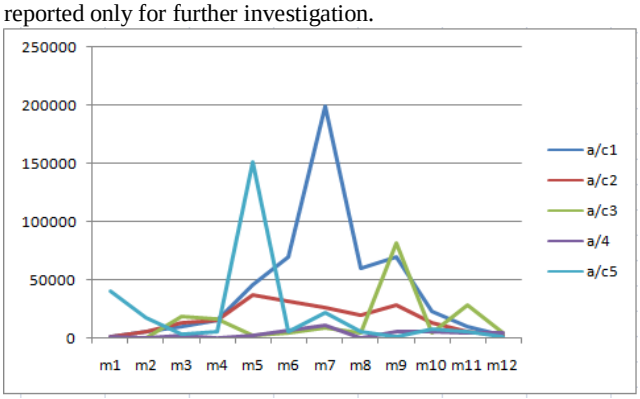

Fig. 3: Accounts with higher frequency are suspicious

5. Conclusion

The proposed work improves the effectiveness of the presented tax evasion technique which predicts the suspicious accounts using hashing method. We will consider the non-frequently transacted accounts as the constraint and have obtained connectivity between different accounts using directed acyclic graphical approach. The accounts that are obtained at the end of experiment have the possibility of being suspicious as they are involving large amount of transactions. Proposed work planned in this article is beneficial more than the other anti-money laundering tools. And will also predict if the transaction of huge amounts made is legal or illegal in case its illegal then this report must be sent to higher authority for further investigation.

Acknowledgement

Firstly, we feel extremely thankful to Her Holiness Most Respected Mata Amritanandamayi Devi (Amma) for her motivation and assistance both in unseen and unconcealed ways.
Sincerely, we express gratitude our institution, Amrita School of Arts and Sciences, Mysuru campus, Karnataka, India, for

providing the essential atmosphere, infrastructure, encouragement and for extending the support possible at each stage of project.

We express our sincere thanks and indebtedness to our parents who have bestowed their enormous assistance at suitable times by providing encouragement in planning and carrying out the project.

References

[1] Umadevi, P., & Divya, E. (2012). Money laundering detection using TFA system.

[2] Salehi, A., Ghazanfari, M., & Fathian, M. (2017). Data Mining Techniques for Anti Money Laundering. International Journal of Applied Engineering Research, 12(20), 10084-10094.

[3] http://timesofindia.indiatimes.com

[4] http:// www.newsbytesapp.com

[5] www.rbi.org.in

[6] Pankaj Richhariya, Prashant K Singh, EnduDuneja. A Survey on financial fraud detection methodologies. In International Journal of commerce business and management 2012.

[7] R. Corywatkins, K. Michaelreynolds, Ron Demara. Tracking Dirty Proceeds: Exploring Data Mining Techniques as to Investigate Money Laundering. In police practice and research 2003.

[8] J.S.Park, M.S.Chen, and P.S.Yu. An effective hash-based algorithm for mining association rules. In Proc. 1995 ACM-SIGMOD Int.Conf.Management of Data (SIGMOD'95), pages 175-186, San Jose, CA, May 1995.

[9] J.Han and M. Kamber, Data Mining: Concepts and Techniques. Morgan Kaufmann publishers, 2nd Eds., Nov 2005.

[10] Liu Keyan and Yu Tingting,"An improved Support vector Network Model for Anti-Money Laundering, International conference on Management of e-commerce and-Government.

[11] Yang Qifeng, Feng Bin, Song Ping. Study on Anti Money Laundering Service System of Online Payment based on Union-Bank mode. IEEE Computer Society 2007.

[12] Sreekumar Pulakkazhy and R.V.S.Balan,"Data Mining in Banking and its applications –A Review", Journal of computer science 2013.G.

[13] Xingrong Luo," Suspicious transaction detection for Anti Money Laundering", International Journal of Security and Its Applications 2014.

[14] Alexandre C, & Balsa, J. (2016). Integrating client profiling in an anti-money laundering multi-agent based system. In New Advances in Information Systems and Technologies (pp. 931-941). Springer, Cham.

[15] G. Krishnapriya, Dr.M.Prabakaran "Money laundering analysis based on Time variant Behavioral transaction patterns using Data mining" Journal of Theoretical and Applied Information Technology 2014.

[16] Nhien An Le Khac, Sammermarkos, M. O'Neill, A. Brabazon and M-taharkechadi. An investigation into Data Mining approaches for Anti Money Laundering. In International conference on Computer Engineering & Applications 2009.

[17] Nhien An Le Khac, M. Taharkechadi. Application of Data mining for Anti-Money Detection: A case study. IEEE International conference on Data mining workshops 2010.

[18] Nhien An Le Khac, Sammermarkos, M.Teharkechadi,. A data mining-based solution for detecting suspicious money laundering cases in an investment bank. IEEE Computer society 2010.

[19] Denys A.Flores, Olga Angelopoulou, Richard J. Self," Design of a Monitor for Detecting Money Laundering and Terrorist Financing", International Journal of Computer Networks and Applications 2014.

[20] Lopez-Rojas, E. A., & Axelsson, S. (2012, May). Money laundering detection using synthetic data. In The 27th annual workshop of the Swedish Artificial Intelligence Society (SAIS); 14-15 May 2012; Orebro; Sweden (No. 071, pp. 33-40). Linkoping University Electronic Press.

[21] Bipin Nair B J, A Recommended Classification Approach for Multilevel E-commerce Marketing Using Decision Tree Method International Journal of Computer Technology & Applications, ISSN: 2229-6093, Volume 5 Issue 2, March-April 2014.

[22] Suresh, C., Reddy, K. T., &Sweta, N. (2016). A Hybrid Approach for Detecting Suspicious Accounts in Money Laundering Using Data Mining Techniques.

[23] Ahalya, C. S., Abin, K. O., & Kanchana, V. (2017, May). Building up an information archive for putting away pesticide data. In Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on (pp. 2125-2128). IEEE

[24] Ganesha, K., Dhanush, S., & Raj, S. S. (2017, March). An approach to fuzzy process mining to reduce patient waiting time in a hospital. In Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017 International Conference on (pp. 1-6). IEEE.