
Dr. G. Krishnapriya

Abstract—Money laundering transaction is to be identified in the real world financial application; a new method can be proposed for detection. In this system, a laundering detection is based on the social network using transaction flow analysis system wetop-quality an appropriate classifying strategy to determine typical money laundering patterns and money laundering rules. From that state, we can quickly identify the abnormal transaction data. A part of a larger chain transactions in money laundering is to be such risk. For to overcome that risk we use a social network to connect missing links in potential transaction sequences. A financial sector independent risk assessment can be provided to submit the transaction. The potential participants can be connected to a social network. The transformation of vast quantities of data into a huge number of reports is not a perfect detection for to overcome that we use a Transaction Flow Analysis. From distributive box and collective box, the transaction mining system is to detect the money laundering. In this system, we can also use a Financial Action Task Force (FATF) to avoid a money laundering. From social network analysis money laundering of terrorist financing. We can also detect the criminal activities involve in the money laundering. The FATF can provide a static assessment of money Laundering.

Keywords—The Financial Sector, Money Laundering, Potential Transaction, Sequence Mining.

I. INTRODUCTION

Money laundering is the process of converting the illegal money is turned into the judicial proceedings through a cyclic operation. The money laundering detection problem was proposed to correlation analysis. In this system we use a Financial Action Task Force (FATF) is to be used to avoid the money laundering. The vast volume of the official financial market is to be hidden in suspected transaction. Transaction Flow analysis can prevent it. From TFA we can interactively and automatically analyze the financial flow in money laundering.

The grouping of transaction activities based on histogram segmentation. The money laundering Crime can be used to detect the money laundering by using a financial flow. Many steps can involve in money laundering are as follows. High Transaction: If some deposit a bulk of money in the bank in the form of cash, the bank report as high-value transactions. So the money can be broken into the smaller amount and then placed in the bank. By having the operation log, the path of fund transfer can be identified. For each path determined or the amount being transferred, we can generate the pattern. The pattern has a source, destination, the amount being transferred, and the number of time has been performed. By making such model for each of the beneficiaries the presence of money laundering can be identified. The process of money laundering will not be performed at each time window, but it will be carried out in the particular time frame. Any user has set of habits in transferring the amount to other accounts by using the internet. They may make the assignments at a given time which helps to identify the presence of money laundering. In the case of rule-based approaches, the method uses sumestates to perform money laundering detection. The rule has various account types and range values for each account. For example, a rule may be with the account type of savings and the field value within one lack.

Similarly, there may be N number of standards for each type of account and each type of transactions possible in the banking sector. Based on the state the current transaction is monitored to perform money laundering. The combination of the operation with separate accounts gives an overall view of these statements on their economic action. This view demonstrates the degree of connotation among various accounts based on occurrences of their transactions. At the establishment level, the same client (business or individual) may have numerous reports. A merging of these accounts may show that an establishment possibly in ML distrustful and may involve multiple accounts connected to different people. The last level examines the ML involving various institutions, facilities, and customers.

II. RELATED WORK

A lot of research effort has been completed on graph data mining. Graph data removal is the task of discovery novel, useful, and comprehensible patterns in a graph depiction of data. In a lot of everything, graph data mining is secondhand for discovery frequently happening constructions, such as in molecular biology, people are absorbed in finding individual assemblies including of some elements[1]. The Subdue organization to find repetitive patterns. Subdue scheme is the process of incrementally squeezing frequently occurring infrastructures into units until accomplishment the pattern occurring incidence. This algorithm achieves DFS to find
frequentsubtrees, and this procedure uses strings to encrypt the tree structures [2].

Active Knowledge via Consecutive Design with Requests to Detection of Money Laundering is planned an active learning process using following Bayesian models to identify the doubtful accounts [3]. The method uses a combination of stochastic approximation and D-optimal designs to select the accounts for an investigation [4] judiciously. The progressive nature of the technique helps to identify the doubtful accounts with negligible time and effort [5].

An outline on developing a brainy discriminating system of anti-money cleaning, a layer model to recognize money laundering. Dissimilar layers play different roles during the analyzing procedure [6]. Data of Operation layer and Account Layer are acquiesced from the root bank branches and have collected the important sources. Only foreign intelligence may be resulting from the perspectives of both inner layers [7]. Group layer and Link layer deliver views to take a complete and aggregate discerning and analyzing process to all data involved in various banks, areas, and subdivisions, to check, contrast, mine, justice and derive in all those data composed of different frequencies. The following layers have much more compensations during macro condition judgment and appropriate cases investigation [8].

Money Laundering Detection using Synthetic Data, they present an analysis of the difficulties and considerations of applying machine learning techniques to this problem [9]. We deliberate the pros and cons of using simulated data and challenges and compensations inherent in the group of such a data set. They are using a case study and recommend an approach based on Multi-Agent Grounded Simulations [10].

III. PROPOSED SYSTEM

The primary purpose of the system (TFA system) is to analyze financial flows to detect money laundering processes automatically. From this system, we can analyze the money laundering by grouping method.

This analyze method is called the Bi-Directional method. Check whether the collection pattern could be correct or not. If there is much less memory in group model, compare to previously collected closed pattern data it does not need to maintain the set of historically closed design, From that, we can scan very well with the collection of the frequently closed pattern. An online fashion is used to output the number of the often closed design. The output pattern can be made by using the Bi-Directional extension.

A. Grouping

From Group we can transfer money. In flow condition the gathering amount of money can be moved into a single account, it can be set in small size. Grouping elements can be treated as the operation in money laundering. The user can
specify the value of the amount from the cashflow. The money flow is to be maximum or minimum flow. The transfer money can be converted into single currency because the movement of money can be from the different currencies. Exchange of money rates can be automatically noted by using given URL address. Grouping can be started only when the account could treat as empty when the balance is not greater than zero. If the balance is greater than zero, it is not the zeroing system.

B. Group Module of Money Laundering Detection System

A data collection as a result of a tree, it is used to fulfill the condition imposed by a user supplied. The sequence of elements is used to connections between the two bank accounts. In this, the graphical method can also use to discover the result of any suspicious operation. By this approach, we can also track the various transaction process it not to be connected with each other, but it can link to a money laundering process.

Algorithm

Input: transaction
Output: Null
Step 1: Start
Step 2: Read the Transaction Log Tl.
Step 3: Receive incoming transaction It.
Step 4: Extract the sequence Forwarding
   \[ SF = \int_{transaction \in Tl} \cdot It \]
Step 5: Extract the pattern= \[ \int_{SF \in Pt} \]
Step 6: Generate a log Tli = \{Pf, Sn, Time\}.
   \[ Tl = \Sigma Tl_i + Tl_i \]
Step 7: Stop.

A single transaction of money operation can be done in frequent sequences it does not matter. Based on the criminal analysis we want to build our project in many stages. We can adapt the report scope, and formula condition is too based on data provided.

C. Sequence Maintaining the Database based on Bi-Directional Extensional

By the prefix Span method, the sequence of collecting database can be preserved. It is used to mining the standard course. A search space directional method does not be contained in this function. The pseudo code projection is applied for to speed up support computing for sequencing the collection of data. Each projected Sequence, a set of the pointer could be recorded. At each project sequences, the corresponding each starting point of project series could be noted. Prefix growing function uses a set of its locally various items.

Algorithm

Step1: start
Step2: Initialize Bi-direction transaction Bt, traffic log Tl,
Step3: Read Transaction log Tg
Step3: while right
Split Tl into time sequence transaction Tg
For the current time transaction TTi
For each next laundering Nl
Compute laundering rate \[ L_n = \frac{\sum P_I(N) \epsilon Tl}{Total \ no \ of \ transaction} \times B \]
If Tg < Bth then
Generate Transaction Control Message TCM.
Identify distinct laundering Dsrc = \[ \int f (\frac{Tl(src) \cdot Dsrc}{Tl \epsilon Nk}) \]
Identify current transaction= \[ \int f (\frac{Tl(dest) \cdot Dsrc}{Tl \epsilon Nk}) \]
Compute number grouping transaction details
   \[ TD = \frac{\sum Tl \epsilon (Dsrc, Ddest, Nk)}{1} \]
End
End
End
Step 4: Stop.

The non-empty prefix is to be added to the final list. The database is scanned again and again to build a new project database. The mine closed frequency sequence can be used by BI-Directional Extension. It can be created by adding a sequence miner among others. And also we have check whether the sequence has forward and backward -extension.

IV. RESULT AND DISCUSSION

The planned process has been appraised using various transactional set collected after different banking subdivisions, and we have detached the accounts which are connected to different banks. To conclude, we have received 8000 accounts from various banks having 14 million transactions. The projected method has formed practical results, and discovery accuracy is also higher.

Graph 1: Shows the Efficiency of Identifying Money Laundering

The graph1 demonstrates the abilityto detect money laundering on some transaction used. It is clear that the effectiveness increased if the size of the transaction is increased. The proposed methodology produces an efficient result by increasing the size of the operation.
The graph shows the comparison of money laundering detection accuracy between different methods. It shows clearly that the proposed method has produced more efficiency in money laundering detection.

V. Conclusion

Their overall characteristics were presented from a perspective of incorporating them into a system for police analysts. We can clearly see why data mining problems are non-trivial and why searching for a better solution is always necessary. Construction of A Financial Action Task Force (FATF), as well as their performance, were compared, for the last one. The MLDS consists not only of these four algorithms but a lot of other algorithms are still tested and added to the system for example Financial Action Task Force (FATF) algorithms.

References