A Model for Identifying Relationships of Suspicious Customers in Money Laundering using Social Network Functions

Abdul K. Shaikh, Amril Nazir, *Member, IAENG*

***Abstract*— The impact on the development of the national economy is mostly dependent on the flow of money in the country. The suspicious transactions of money within financial institutions affect the national economic system and compromise the impression of country's reputation. Identifying an individual suspicious transaction and individual suspicious customers within transactions are evident by using basic statistical rules. Other than such traditional rules, this paper proposes a model that discusses the identifications of association and relationships within transactions and customers using Social Networks Analysis (SNA). With the help of this model, groups and gang mafia can be identified who mainly play a vibrant role in money laundering activities**

***Index Terms*—suspicious customers, relationship, Association, Relational analysis, data analysis, AML, Anti-Money Laundering, Finance application**

I. INTRODUCTION

MONEY laundering activity is one of the structured crimes in the world that causes an adverse impact on the development of the national economy. Due to increasing integration of financial sectors, it has become a global concern that should be dealt with the implementation of effective technological measures [1]. AML data analysis [2] to identify suspicious transactions that are different from the pattern of normal transactions, and report to financial intelligence unit (FIU) and other law enforcement agencies for further investigation. AML system provides a solution that identifies suspicious customers and illegal transactions in money remittance. The solution works based on specified rules on transactions trends that identify suspicious customers who involve in money laundering. The ultimate goal for the solution and data analysis are to detect and prevent money laundering and potential terrorist financing by reporting of suspicious circumstances/transactions to authorities. Our previous work [3] proposed a novel dynamic approach to identify suspicious customers in money transactions. The approach works based on the dynamic behavior of customer transactions that measures the customer own transaction history, profile features and identifies suspicious transactions. Currently, most of the Anti-Money Laundering (AML) solutions provide determination of suspicious individuals. However, to identify relationships, association, linked group or mafia of suspicious individuals is rarely come under consideration. However, it is very significant in order to control money laundering from the group involved. Keep focusing on the above issue, we extend our above referred earlier research in to identify the relations and associations of suspicious customers by utilizing Social Networks Analysis (SNA) as recently, the popularity of SNA is increasing significantly. These relationships help authority to identify gang and mafia involved in the money laundering. The relationships can be family, friends and business relationships or even common owner; we use some social networking functions such as degree of centrality, closeness centrality betweenness centrality and ego group. A social networks are nodes of individuals, groups, organizations, and related systems that tie in one or more types of interdependencies: these include social contacts; kinship; conflict; financial exchanges; trade; joint membership in organizations; and group participation in events, among numerous other aspects of human relationships [4]. The overall effectiveness of our proposed models depends on customer's profile information that is provided at the time of opening a bank account. We have developed rules that execute under customers profiles and helps to identify existing relationships with supercilious customers.

The main contributions of this paper are (i) proposed a model to identify relationships of suspicious customers in money transactions and (ii) employed social networking functions to identify association of suspicious customers

The remaining sections of the paper are organized as follows:

Section 2 briefly reviews existing related research. Section 3 explains the methodology of the proposed approach and system architecture is explained in section 4 Finally, Section 5 concludes the paper with possible future work.

II. LITERATURE REVIEW

This section provides an overview of existing related research and highlights their limitations.

A research [2] proposed a system that provides a integration between customer relationship management (CRM) and anti-money laundering (AML) suspicious data reporting in commercial banks to increase the initiative of suspicious transaction identification, reduce the false reporting rates, and improve the intelligence quality.

Manuscript received March 30, 2018; revised April 10, 2018.
A. K. Shaikh, Department of Information Systems,
Sultan Qaboos University, Sultanate of Oman
(email: shaikh@squ.edu.om).
A. Nazir, Department of Computer Science,
Taif University, Al-Hawiya, Saudi Arabia
(email: amril@tu.edu.sa).

ISBN: 978-988-14047-9-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

However the system requires an additional Customer background checking which is conducted by operational layer of CRM system that helps in customer analysis, including front-office customer identification, customer business analysis, and customer visiting but not cover the suspicious relationships in order to identify whether the illegal transaction involve a mafia or individual. The paper [5] focuses the use of social network that cab be applicable to social learning include detection of communities within networks such as network neighborhood where the group of people to whom he or she is linked — has been shown to have important consequences in a wide range of social support. So it is very significant to identify those groups within network as they can have some kind of same characteristics. They typically include family members, co-workers, and friends of long duration, distant acquaintances, potentially a spouse and other relatives. An important issue for this type of analysis of social networks is to use features in the available data to recognize this variation across types of relationships

The paper [6] presented a system that identifies money laundering activities by using core decision tree algorithm. Decision tree is a data mining technique that helps in the classification of the data objects through a top-down approach. To identify the abnormal information, the system applies classification rules and then establishes the core decision tree step by step. With the core decision tree, similar data object can be clustered together. The author concludes that the data clustering is just one way to identify the abnormal activities and efficiency is very limited. However, author suggests that the proposed method can give better accuracy if the algorithm use with other Data mining algorithm.

A research paper [7] proposed an automated system for identifying a suspicious groups in a financial transaction network. The system integrates of network analysis and supervised learning to identify suspicious activities in money laundering. The system is designed for use in a live intelligence environment at the Australian Transaction Reports and Analysis Centre (AUSTRAC). The system works based on Network analysis combining financial transactions and supplementary relationships. They analyze both explicit transaction relationships and implicit relationships derived from supplementary information. The system extracts small, meaningful communities from this network in manner that allows existing business knowledge to be considered in the process. Two supervised learning algorithms, namely, a support vector machine (SVM) and a random forest are then applied to these communities to obtain trained classifiers. The network analyzed and recognized multiple relationships, represented using typed edges. It is not only identify individual where remittance serves but also recognize parties that may be linked by shared accounts, shared use of agents and overlapping geolocations. The limitations of the system includes 1) only considering the dynamics of each community through analysis of transaction time-series as it does not try to capture relationships between the structure and particular edge. 2) Always there is a need of expert knowledge to set the parameters values.

The recent research work [8] proposes a novel approach which applies clustering method to detect potential ML groups among large volumes of financial data in an efficient and accurate manner. In this approach, a framework that applies case reduction methods to progressively reduce the input data set to a significantly smaller size. The framework then scans the reduced data to find pairs of transactions with common attributes and behaviors that are potentially involved in ML activities. The preliminary experimental results demonstrate the effectiveness of the framework. More recent work [9] which use real data from transactions undertaken by more than 600 companies from a particular sector to analyze behavioral patterns using supervised learning. They apply cost matrix and SMOTE to different detecting patters methodologies: logistic regression, decision trees, neural networks and random forests. The objective of the cost matrix and SMOTE is to improve the forecasting capabilities of the models to easily identify those companies committing some kind of fraud. The results obtained show that the SMOTE algorithm gets better true positive results, outperforming the cost matrix implementation.

The research work [10] proposed a semantic-based framework that translates social network-related information using ontology. The framework recognizes relationships among users and resources within a social media. According to author claim, they can extract many inferences about the above kinds of relationships by using reasoning. However, the paper more focuses on access control rather than identifying the linked between the nodes.

The paper [11] compared different types of social networks and specified the challenge in extraction of the social concepts from a noisy and incomplete knowledge on semantic web even well-defined ontologies.

By inspiring from existing research challenges, we propose the model that analyses transaction data and customer profiles and identify hidden relations and links of suspicious customers. The detail of our proposed model is explained in the next section.

III. Methodology of the Proposed Model

In this section, we explain the details of the proposed model including our approach method, system architecture, flow chart and its working: Our approach aims to find a much more effective technique that can identify maximum relationships and also measure the strength of the relationships of suspicious customers which are entirely based on suspicious profile data. We build associate network using semantic network graph and social network functions such as degree centrality, clustering etc. These functions facilitate to identify explicit relationships of each suspicious customer within a Network. The details of the above functions including examples are as follows:

A. Degree Centrality

The Degree centrality function of social network provides insight into how important or central a node is in the group. It uses number of edges of a node as a proxy of importance.

degreeCentrality (node_i) = numberOfEdges(node_i) / (N – 1)

Where N: the total number of nodes in the network

In our proposed model, N is total number of customers and Total number of edges is counted based on the total

ISBN: 978-988-14047-9-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

relationships of the specific customers with other customers in the network.

Algorithm Degree Centrality

```
degree-centrality {
NM = get neighbor matrix
LN = get the list of nodes
For each node_i from LN {
valueofDegreeCentrality=call AG API actor-degree-
centrality (node_i  LN NM);
add triple (node_i  hasDegreeCentrality
valueofDegreeCentrality)
 }
Add status
}
```

B. Clustering

The aim of the clustering is to separate groups with similar characteristics or based on some specific criteria of the nodes and assign them into different clusters within a Network. Social network clustering analysis, divides objects into classes based on their links as well as their attributes [12]. In our proposed model, based on suspicious customers profile we identify suspicious customers within a social network and cluster them separately. The purpose is to predict the money laundering activities within specific group in the future

Photographs and grayscale figures should be prepared with 300 dpi resolution and saved with no compression, 8 bits per pixel (grayscale).

IV. System Architecture of the Proposed Model

This section provides the system architecture and flow chart of the proposed model and explains its working.

Fig. 1 shows the architecture of the proposed model where the AML Analysis module generates the list of suspicious customers and it is adapted from our previous research (shaikh et al. 2017). The module provides the input values of those suspicious customers who are identified as suspicious under some criteria. We take the profiles of these suspicious customers and store the data in the alert table. Alert table is updated periodically. We convert the data into AML knowledge base where other normal customer's data is already resided. In order to identify relations and association of suspicious customers, we execute visual analytics module that takes input data from AML KB that has semantic data of both normal customers and suspicious customers and provides the links of suspicious customers. These can be various types of association such as Family, Relatives, Spouse, Siblings, and Common Owner etc. In this way, we can identify mafia or groups involved in the money laundering activities. We have developed the rules in prolog language [13] and merge the data into AML Knowledgebase. Finally, we have stored the links data in AML knowledge base where we can display existing links using any dashboard. The flow chart of the proposed system is explained in the following section

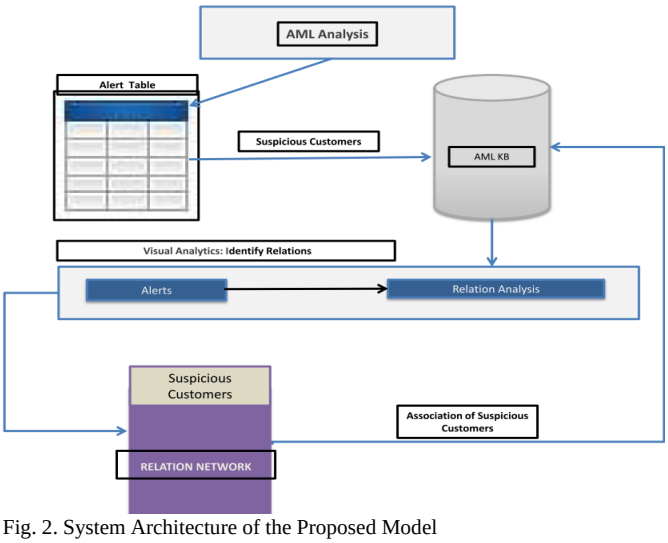

Fig. 2. System Architecture of the Proposed Model

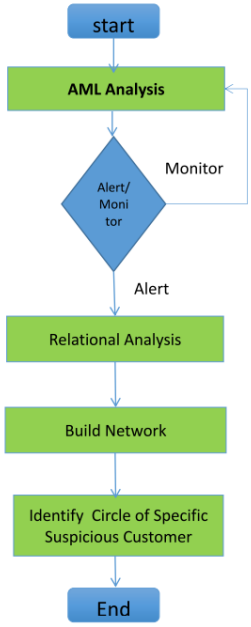

Fig. 1 Flow chart of the Proposed Model

Fig. 1 shows the overall flow chart of the proposed system where AML analysis module process Alert and Monitor lists of the suspicious customers. However the relational analysis module takes only alert customers as an input whereas monitor customers return back to the AML analysis until and unless they become alert they cannot enter the relational network module. Relational Analysis module is executed to identify relations and association based on criteria defined in relational identification section. Based on the results, a social network is built that shows the circles of each suspicious customer. We explain relation analysis

Relation Analysis Module

The relational analysis module extract the relations and associations of suspicious customers based on some criteria of social network conditions. The relationships are identified based on profile information such as suspect last name, address, age, race etc. The flow chart of relational analysis is explained here:

ISBN: 978-988-14047-9-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

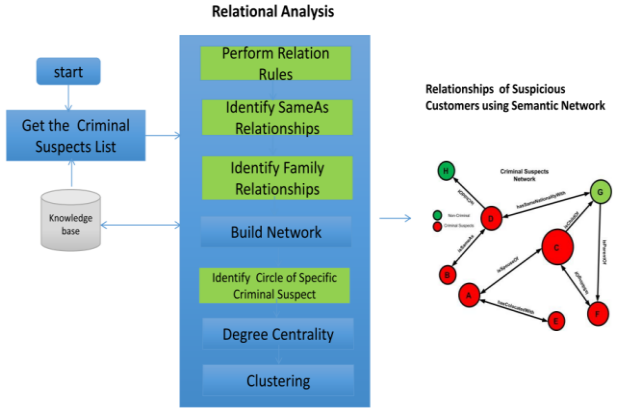

Fig. 3 Relational Analysis

Fig. 3 shows that how relations are identified through relation identification strategies such as prolog rules and network analysis functions. The module produces various types of relations such as Common Owner, Family relations and business relations by the following Relation identification criteria:

Relation Identification

The model uses the following criteria and conditions to identify the various types of relationships. All rules are implemented in prolog to produce semantic data which is stored in AML knowledgebase and further uses through dashboard for visualization purpose.

TABLE I
RELATIONAL RULES

Rules	Conditions	Outcomes
1	∃ t(A1,A2) && if A1 ∩ A2 || A1 = A2 -> Ro(O(A1) , O(A2))	Common Owner relationships
2	∃ t(A1, A2) && if (A1 ∥ A2) ∈ Type B -> Rb(O(A1) , O(A2))	Business Relationships
3	If address and surname are same && agediff= low range	Spouse/sibling
4	If address and surname are same && age diff = midrange	Spouse/Sibling
5	If address and surname are same && age diff = high	Parents /Child
6	If surname and dateofbirth are same && race same	SameAs
7	If surname and address are same && race same	Family
8	If namematch= 50% and address are same && race are same but gender are different	Spouse

.

V. Conclusion and Future Work

After identifying the list of suspicious customers and transactions on financial transactions, it is challenge to identify the relationships and associations among these illegal activities. To address this challenge, the paper has proposed a model that identifying specific relations among illegal transactions and suspicious customers. The relationships such as business relationship, parent relationships, spouse relationships, friend relationship, siblings' relationships etc. are identified using social networking functions. The future research can be extended to implement the proposed model using real bank dataset to validate and test the efficiency of the proposed model. Also, we have planned to test this model in call log data to identify association among illegal calls activities.

References

[1] Vaithilingam, S. and M. Nair, Mapping global money laundering trends: Lessons from the pace setters. Research in International Business and Finance, 2009. 23(1): p. 18-30.
[2] Tang, J. and L. Ai, The system integration of anti-money laundering data reporting and customer relationship management in commercial banks. Journal of Money Laundering Control, 2013. 16(3): p. 231-237.
[3] Shaikh, A.K., Nazir, A A novel dynamic approach to identifying suspicious customers in money transactions International Journal of Business Intelligence and Data Mining IJBIDM-5876 Sep 2017((In Press)): p. 1-21
[4] Serrat, O., Social Network Analysis, in Knowledge Solutions: Tools, Methods, and Approaches to Drive Organizational Performance. 2017, Springer Singapore: Singapore. p. 39-43.
[5] Shum, S.B. and R. Ferguson, Social learning analytics. Journal of educational technology & society, 2012. 15(3): p. 3.
[6] Rui, L., et al. Research on anti-money laundering based on core decision tree algorithm. in Control and Decision Conference (CCDC), 2011 Chinese. 2011.
[7] Savage, D., et al., Detection of money laundering groups using supervised learning in networks. arXiv preprint arXiv:1608.00708, 2016.
[8] Soltani, R., et al. A new algorithm for money laundering detection based on structural similarity. in Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE Annual. 2016. IEEE.
[9] Álvarez-Jareño, J.A., E. Badal-Valero, and J.M. Pavía, Using machine learning for financial fraud detection in the accounts of companies investigated for money laundering. 2017, Economics Department, Universitat JaumeI Castellón (Spain).
[10] Carminati, B., et al. A semantic web based framework for social network access control. in Proceedings of the 14th ACM symposium on Access control models and technologies. 2009. ACM.
[11] Jamali, M. and H. Abolhassani. Different aspects of social network analysis. in Web Intelligence, 2006. WI 2006. IEEE/WIC/ACM International Conference on. 2006. IEEE.
[12] Sharma, S. and R. Gupta, Improved BSP clustering algorithm for social network analysis. International journal of grid and Distributed Computing, 2010. 3(3): p. 67-76.
[13] FranzInc. Allegro Prolog. 2017 [cited 2017 19 July]; Available from: https://franz.com/support/documentation/6.0/doc/prolog.html.

ISBN: 978-988-14047-9-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)