Evaluation of Destructive e-Banking Users’ Loyalty by Applying RFM

Notash Maryam1* and Harounabadi Ali2

1University of Islamic Azad, Computer System Architecture Engineering, Dezful Branch, Iran. 2University of Islamic Azad, Central Tehran Branch, Iran.

Authors’ contributions

This work was carried out in collaboration between both authors. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJARR/2019/v7i130163

(1) Dr. Shih-Chien Chien, Associate Professor, Department of International Business and Trade, Shu-Te University, Taiwan.

(2) Semra Erpolat Taşabat, Mimar Sinan Fine Art University, Turkey.

(3) Marius Iulian Mihailescu, University of Bucharest, Romania.

Mustapha, Saidi Atanda, Lead City University, Nigeria.

Complete Peer review History: http://www.sdiarticle4.com/review-history/46513

Received 02 January 2019
Accepted 06 March 2019
Published 04 November 2019

ABSTRACT

World economy has encountered money laundering phenomenon and its destructive effects on economy of countries over the last decades. Money laundry detection is one of the fields in which data mining tools can be very helpful in detecting it. Nowadays, recognizing credible customers to present banking facilities to them is of high importance. On the other hand, by increasing cheating in banking, detecting the fraud customers is also important. In this study, the decision tree was being trained by providing a fuzzy decision tree and users’ behavioral vectors. The output of fuzzy tree can signify users’ risking behaviors. Some features of customers’ accounts need to be extracted in order to identify the people with high risks. For instance, the variance of money transaction and money transfer can be done. In another part of the study, RFM (Recency, Frequency, Monetary) features and MLP (Multi-Layer Perception) classifications were used to identify the loyal customers. The three-fold features of refreshment, frequency, and shopping amount was completely discussed for every customer, whereby the customers’ scores were established as well. This classification aimed to categorize the credible users of neural networks. The results of current research indicate that the represented techniques possess high precision values, in comparison with previous techniques.

*Corresponding author: Email: mnotash2@yahoo.com, maryam.notash1397@gmail.com;
Keywords: E-banking; fraud; credible customer detection; fuzzy decision tree.

1. INTRODUCTION

Money laundering is a clustered, constant, complicated, and long term procedure which is usually done in long scales that causes for the change of dirty money earning from committing a crime into legal and legitimate shapes, in a way that it would be difficult to detect its criminal origin. On the other side, by considering e-banking development and recognition of these techniques, behaviors of the money launderers, becomes gradually complicated. Based on the large amount of data in a bank, recognition of these behaviors would not be possible, without using anti-money laundering systems. In this regard, using a suitable system for recognizing people or money laundry networks is necessary. During recent years, the fraud detection techniques, not only have detected the fraud and cheating happening in an organization and have analyzed them, but also have aimed to predict recognize the users and customers' behaviors by recognizing their subsequent behavior and has decreased the risk of phishing. Since the expenses of direct and indirect phishing are high, banks and financial institutes are seriously seeking the quickness in detecting the fraud and money laundering activities. Banks are included in these organizations that are directly interacting with customers. During the recent years the increase in access to customers' data and improvement of data analysis by smart techniques has caused different actions to analyze customers' behaviors. Money laundering prevention is of high importance which has not been academically worked on yet. In this paper by studying the users' profiles, some features are extracted. These features can be, for instance, money transaction with high amount in high risk domain in terms of money laundry, withdrawal or deposit with high and multiple amounts in a limited period of time, restarting of stagnant accounts with considerable amount, etc. in this study by providing a fuzzy decision tree and customers' behavior vector injected into it, the network training is conducted. The network output can signify the alarming behavior of users. Some features of customers' accounts need to be extracted in order to detect the high risk customers.

In the following sections, the decision tree and fuzzy systems are comprehensively explained. Meanwhile, in section 3, recent corresponding studies and researches are studied as the main background. Section 4 of this article is allocated to the explanation of represented techniques. Finally, results of the evaluation techniques are completely discussed and represented.

1.1 Research Field

In this section, a short introduction of decision tree and fuzzy systems is presented.

1.2 Decision Tree

Decision trees organize all samples by classifying them from root node towards leaf node. Every internal node in tree examines one feature of the sample and every branch which comes out of that node is the corresponding possible amount for that feature. Also each leaf node is attributed to a classification. Each sample is classified by starting from the tree root node and the feature examination which is signed by this node and the transfer in the corresponding branch with the amount of the feature in sample. This procedure is repeated for every sub-tree which is the new node of its root.

In general, decision trees reflect a seasonal combination of constituent combination on the amount of the sample features. Every path from the root of the tree to a leaf is corresponding with the constituent combination of examination features existing in that path and the tree itself is also corresponding with constituent combination.

The decision tree structure in machine learning is a predictive pattern which shows the observant fact of a phenomenon in comparison to understanding of the amount of a phenomenon. Machine learning technique for deducing of a date decision tree is called decision tree learning which is one of the most common data mining techniques.

Every corresponding internal node of a variable and every edge to child reflect a possible amount for that variable. One leaf node, by having the variable amounts which is reflected by a path from the tree root to leaf node, shows a predicted amount of goal variable. A structural decision tree shows that leaves are indicative of classification and branches reflect the seasonal combination of features which are resulted from these classifications. Learning a tree can be done through separating of a data set to test-
based sub-set of one feature. This procedure is repeated in every subset resulted from separating in a return way. The return action is completed when the separation is not helpful anymore or when a classification can be applied to all existing samples of a subset.

Decision tree can produce comprehendible features from existing relation in a data set for human and can be applied for fields such as identifying disease of plants classification and customer finding strategies.

1.3 Fuzzy Systems

A system which formulates a map from input to output by using a fuzzy logistic is known as fuzzy inference system (FIS). FIS is also called rule-based system. Because these systems are from by “If – then” phrases. Such systems are called fuzzy controller when appear in a controlling role. Rules base: include some rules and “If - then” phrase.

Database: Definition of membership functions

Decision unit: Applying operation on fuzzy rules

Fuzzy making relations: Transferring the real input into fuzzy sets

Non-fuzzy making relation: Transferring the fuzzy results into real amount

The two bases of data and rules are together known as a knowledge base. Fuzzy deduction systems are divided into three classes of “mamdani”, “sugeno” and “takagi”.

Most of the FISs are regarded as mamdani fuzzy model, in which the members for output fuzzy set are predicted. Meanwhile, in sugeno model, the members of output fuzzy sets are either in linear relation or fixed.

Takagi and Sugeno and Kung together introduced the fuzzy model of Sugeno in 1985. In this model the members of the output fuzzy sets are either in linear relation or fixed. A phrase or fuzzy rules can be: “if the first input is x and second input is y, then the output is z=f(x,y) ”.

If f(x,y) is a first grade multinomial, then FIS is called a fuzzy model type 1. If f(x,y) is fixed, then FIS is called fuzzy sugeno model of type 0. In sugeno fuzzy model, the total output is computed out of the average weight.

Sometimes in order to decrease the FIS learning time, the sum of output weight is used instead of weight average.

3. RELATED WORKS

In reference [1] the FIF neural network models, which is based on APCIII (Adaptive Pattern Classifier) clustering algorithm, the return algorithm of the least squares is represented for prevention of money laundering. APC III (Adaptive Pattern Classifier) clustering algorithm is used to assign the parameters of radial function in hidden layer and the return algorithm of the least squares of RLS is used to update the communication weight between hidden layer and output layer. It can be observed that the issue of money laundering is clear and needs immediate remedy. Today some detection techniques are used in money laundering prevention which are represented in reference [2,3] and decision tree classification and outlier analysis tools are introduced in detection of suspicious money transactions. In references [4,5,6] some techniques are mentioned such as clustering analysis tools, clustering analysis tools, back-up vector machine, link analysis, intelligent agents and neural networks.

The outlier detection technique is used for detecting data thing which is not in accordance with general data features but it cannot recognize the suspicious behavior of peer comparison.

A back-up vector machine can have good results but its time expense is high. According to the large data in financial institutes and the high rate of risk detection, there will be a serious need for a detection technique with high precision in financial domain. Since RBF (Radial Basis Function) neuron networks can compute from time to time as to their own measures, they can define that if money flow included money laundering actions. RBF does not include complicated process but has a big time saving in tracking the money laundry activities. In reference [7] RBF method is used. RBF can, to a great extent, overcome longer learning time and the problem of determining the units of post distributing BP of hidden layer.

In reference [8] the bank transaction reports which may be related to criminal activities are used for identifying the suspicious transactions. Since some activities like money laundering may include complicated organizational plans, machine learning techniques which are based on
individual interaction analysis, may work poorly when used for recognizing suspicious transactions. In this paper a new machine learning technique for graph mining interaction is represented. This represented technique creates a graph model which may include suspicious transactions. The model used for this study is parametrical with fuzzy numbers which shows the detected transactions and graph transactions parameters. Since money laundry can be transferring money through different accounts, the presented model of transaction graph is parameterized according to structural features. Opposite some other techniques of graph mining in which the isomorphism is used to adapt data to graph model, in technique of this reference a fuzzy adaptation of graph structure is presented, by using the data of the publisher of a credit card, the neural networks based on checking detection system is trained and is tested on dataset of “hold out” which this dataset includes all account activities of two months after that period of time. Neural networks are trained on samples of cheating considering missing cards, stolen cards, program cheating, mail-order and NRI cheating. In this reference, network performance in this dataset is discussed in terms of detection precision and quickness of cheating detection.

This system is installed in an IBM 3191 (International Business Machines) in Mellon Bank and currently is used to detect cheating in CMLIT (Comparative Literature) card samples of that bank. In a strictly controlled test on real world data of Mellon Bank sample credit cards, the neural networks-based fraud detection systems are shown to present considerable developments both in precision and quickness of fraud detection.

In [9] neuro-fuzzy system is presented to find invalid accounts and to predict them which has facilitated these accounts detection with a relatively high precision. In this study the history of the committed crime in system and also the information related to the people who have problems redeeming their mortgage are used.

In [10] a neural network is presented to detect the crime in e-banking by the help of supervision learning procedure and the use of learning sets for building models of deceiving e-banking transactions. By helping from a big set of transactions the presented network is designed to detect the illegal and criminal activity pattern.

Also, another technique used in detecting the crime is data mining procedure, which focuses on statistical analysis and customers’ behavior and users’ pattern in crime detection [11]. This technique is based on special ruling and learning, being able to detect deceiving behavior indexes from large transaction database. These indexes are used to create monitoring systems to record customers’ unusual behaviors and detect their suspicious behavior. Eventually the output of these systems can be used to warn different users in reference [4]. Association rule is also one of the best data mining techniques for creating such models. In [12] this technique is used to extract knowledge and to gain unusual behavior patterns from a large set of users’ transaction in database of credit card transaction in order to detect and prevent crime. Another technique which is already used to recognize and detect crime is the artificial neural networks which is capable of extracting pattern from databases that include the customers’ past transactions. This network can be trained and is adaptive to new kinds of crimes (12).

In reference [13] the combination of fuzzy systems and neural system features is the objective of creating a fuzzy neural network with capacity of learning from environments. One of the new methods of combining these two systems is using fuzzy neural networks which its usage development depends on capabilities and high flexibilities of fuzzy agents which cause fuzzy neural networks flexible or FNN.

In reference [14] another new technique of neural network combination, which is able to learn from the environment, organizes its own input-output pairs of structure and adapts its interaction in a way that creates the adaptive fuzzy neural network of Safety.

4. SUGGESTED TECHNIQUES

In this section, represented techniques of the present study are explained Meanwhile, total RFM features, artificial neural network algorithm and fuzzy decision tree are precisely discussed. In the current research, RFM technique along with artificial neural network is used to recognize loyal customers and also cheating customers will be detected, by using fuzzy decision tree.

The researcher has applied MATLAB software, in order to analyze the data. Accordingly, by developing a fuzzy decision tree and injecting the behavioral vectors of users into it, the network
has been proceeded. Network output determines the risk of users' behaviors. Therefore, in order to identify the risky individuals, features of customer accounts are extracted through the evaluation of user profiles. These features include high-risk financial transactions for money laundering, and withdrawals, plus the large-value deposits over a limited period of time, by starting the re-establishment of stagnant accounts with significant amounts of money. For this reason, the variance of financial transactions plus the place of money transfer, namely the free zones, has been applied. Thus, the higher variances of these transactions are, the greater the likelihood of money laundering will be. With due attention to the abovementioned precision, risky individuals have been evaluated through applying fuzzy decision tree approach. The criteria have been validated by using RFM technique. In this research, by adapting a systematic structure, an innovative fuzzy system is proposed, through applying neural networks. Meanwhile, the researcher has attempted to identify the loyal customers in the banking system, by using RFM features and MLP category. By applying RFM method, three novelty features of Recency, Frequency, and Monetary are evaluated for each customer. Accordingly, every customer was scored based on abovementioned ratings. This category has been used to classify loyal users, within neural networks. The researcher has proposed an innovative methodology for the research, by obtaining related information about organization’s customers. Therefore, she has applied RFM model for extraction of customers’ behavioral characteristics. Pertinent features were grouped by applying customers’ MLP, based on customers’ loyalty scores in each cluster. According to the proposed algorithms of this innovative method, suggested parameters of R, F and M were injected into the network. Finally, by the extraction of network’s output, the rate of customer's credit was determined and loyal customers were identified. This innovative method is very accurate, compared with the methology of background studies.

4.1 Using Fuzzy Decision Tree to Detect Cheating Users

Fuzzy decision tree is used to detect fraud users. By utilizing the fuzzy tree, the rules of different groups of customers are provided that the cheating users are included in these groups. In current study, the following features are used to illustrate the fuzzy tree:

- Age
- Number of transactions
- The amount of transactions

In order to define the rule of cheater, based on the proposed three criteria, as the researcher choice was established, the researcher has implemented the following procedure:

By the extraction of the fuzzy decision tree, behavioral vectors were drawn. The output of fuzzy tree signified users’ risking behaviors. In order to identify the individuals with high risks, the features of customers’ accounts were extracted. Meanwhile, the variance of money transaction and money transfer was accomplished as well. Then, RFM (Recency, Frequency, Monetary) features and MLP (Multi-Layer Perception) classifications were used to identify the loyal customers. Accordingly, three-fold features of refreshment, frequency, and shopping amount is completely discussed for every customer, whereby the customers’ scores were established as well. This classification aimed to categorize the credible users of neural networks. Finally, the researcher has produced the rule of cheater, according to the abovementioned criteria.

By using entropy, the fuzzy decision tree is illustrated and mamdani fuzzy rules are extracted.

4.2 Extraction of Mamdani Fuzzy Rules

In this section by applying data mining techniques, the researcher has followed a searching process through a large volume of data, using clustering techniques (K-means, Fuzzy K-means, Subtractive) to acquire relevant and significant data in pattern recognition; and fuzzy logic from inference system (Mamdani and Takagi-Sugeno-Kang Type) based techniques to extract mamdani fuzzy rules. The subtractive clustering technique in conjunction with the FIS methods (Takagi-Sugeno-Kang and Mamdani) in all sample tests showed a better performance than any other technique, because it best optimizes the objective function. Meanwhile, the value of the root mean square error (RMSE) minimizes enormously, presenting the best results. The following steps were proceeded, in order to extract pertinent rules:

**Step 1:** The researcher has grouped input values, using clustering techniques (Kmeans, Fuzzy K-means, Subtractive), in order to
calculate centroid and standard deviation. By the formulation of related parameters, antecedents membership function values were derived.

**Step 2:** She has calculated the consequents with Mamdani fuzzy reasoning.

In order to find the consequent membership function values, the researcher has used the approximation method or minimum square method, resulting a centroid matrix of the rule consequents.

**Step 3:** She has extracted the rules, based on antecedents membership function values and Mamdani FIS rules consequents.

**Step 4:** The researcher has evaluated Mamdani FIS with input values, to get outputs, by the final calculation of root mean square error.

Accordingly, at final stage, the researcher has extracted the following rules:

A. If age is young, number of transactions is low & the amount of transactions is high, then the user is a cheater

B. If age is young, number of transactions is low & the amount of transactions is low, then user is a non-cheater

C. If age is old, number of transactions is high & the amount of transactions is high, then user is a cheater

D. If age is old, number of transactions is low & the amount of transactions is low, then user is a non-cheater

**4.3 Credible Users’ Recognition**

In the current technique, credible users are recognized by neural networks’ classifications. The software which researcher has used in the present research is MATLAM. In this study, the level of customers’ loyalty is assigned by transaction computation, in a way that the number and the procedure for customers’ transaction are valued in one month. This classification ranks from the most loyal to the least loyal customers. The way of computing the loyalty is in a way that if the customers have more transaction more than the threshold in one month and these transactions cause the increase of such accounts. Therefore he’s a loyal customer, while a customer who doesn’t have any transaction in one month is considered as the least loyal one. This classification is conducted by MLP (Multi-Layer Perception); the features of RFM (Recency, Frequency, Monetary) are extracted and computed, by giving them to MLPas the input. RFM output is given to neural networks, and then these neural networks classify the customers, based on the learned data. This classification is conducted in neural networks and loyal customers will be recognized as well. Additionally, Multi-layer perceptron networks are of the feed forward neural network which is one of the most useful models of artificial neural network in modeling such criteria. In multilayer perceptron network, each neuron belongs to a layer and coincidentally, it is connected to all the neurons of previous layer. These networks are completely interwoven to each other. About recognizing credible
customers, the neural network needs to be able to maintain the past interactions. Because of the discussed fact and by considering the abilities of perceptron networks and training capabilities for proper learning of it, using this kind of neural network for detecting credible users is considered in the related issue. In this survey according to the usage of multi-layer feed, the forward perceptron networks in prediction issues and their high capabilities in generalizing the results, these networks are used as the presented techniques.

The measure of a hidden layer is gained experimentally. For a neural network of a logical size, the amount of hidden neuron is chosen with a proportion to the number of inputs.

If the MLP network doesn’t converge to the desirable answer, the number of hidden layer neurons will increase and if the network converged and had a proper generation, if possible, the smaller number of hidden neurons will be examined.

4.4 Datasets

In this study the real data of 600 users of the sample bank is used. These data have different features which some of them are as following:

- Personal information(first name, sure name, ID number)
- Account information: account number, kind of account, the number of accounts
- The transactions information: the number of transactions, the date of transaction

These data are driven from the central bank and it is called as the sample bank in order to keep the bank identification. These data are tested by different methods and algorithms which will be illustrated in the following.

This survey is accomplished in one of the governmental banks of Iran. Meanwhile, customers of aforementioned bank are classified and thereby, the level of their loyalty is assessed and analyzed. To do so the transactions of the current account of 460 customers with the bank value for 18 months are gathered. Then the data was examined and redundant and faulty data were eliminated. After cleaning operation, the information and transaction of 450 customers was prepared for the next level which their number was about 440000 records.

5. EVALUATION OF THE PRECISION RESULTS

In order to evaluate the precision results, obtained by analyzing the two criteria of recall and precision, the researcher has firstly explained the method of analysis in the following:

In the pattern recognition, information retrieval and binary classification, precision or “Positive predictive value” is the fraction of relevant instances among the retrieval instances, while recall or “sensitivity” is the fraction of relevant instances that have been retrieved over the total amount of relevant instances. Accordingly, the instances are documents and the task is to return a set of relevant documents given a search term or equivalently, to assign each document to one of two categories, “relevant” and “not relevant”. Both precision and recall are therefore based on an understanding and measure of relevance. Accordingly, precision is “how useful the search results are”, and recall is “how complete the results are”. In another words, precision can be seen as a measure of exactness or quality, whereas recall is a measure of completeness or quantity. In a classification task, the precision for a class is the number of the positives; i.e. the number of items correctly labeled as belonging to the positive class divided by the total number of elements labeled as belonging to the positive class: i.e. the sum of true positives and false positives, which are items incorrectly labeled as belonging to the class. Recall in this context is defined as the number of true positives divided by the total number of elements that actually belong to the positive class; i.e. the sum of true positives and false negatives, which are items that were not labeled as belonging to the positive class but should have been. Often, there is an inverse relationship between precision and recall, where it is possible to increase one at the cost of reducing the other. The criteria for selected and relevant elements of recall and precision are illustrated in Fig. 2.

In order to calculate these two parameters, the researcher has derived the following equations:

Recall\(=\frac{T_p}{T_p+F_n}\)  \(\text{(1)}\)

Precision\(=\frac{T_p}{T_p+F_n}\) \(\text{(2)}\)

Where \(T_p\) is the number of the customers who were identified incorrectly as loyal disloyal \(F_n\) is the number of customer who were not identified
incorrectly as loyal disloyal, $F_p$ is the number of the customers who were identified as loyal.

The criteria for determining the precision of analysis implemented by the proposed method are compared to the implications of previous accomplished RFM methods. Fig. 3 illustrates the analogy of these criteria in a diagram.

In this level, the amount of loyalty of each group of customers is computed. To do so, the first the normalized average amount of recency ($C_{jr}$) and the normalized average frequency ($C_{jf}$) and also the normalized average of the money value ($C_{jm}$) of each cluster of customers are separately computed.

Then the loyalty level of each cluster of customers is computed. The Table 1 illustrates the loyalty level of each cluster of customers in represented technique.

According to Table 1, cluster 7 with 27 customers show the most loyal customers of the bank. Also cluster 8 with 50 customers has the least loyal customers in ranking.

In [15], according to the conducted survey about RFM model, after defining the value and scoring different variables of RFM, it is used as the inputs of classification. In this paper the variables have the equal weights. The RFM model output includes 3 fields for each customer regarded as: frequency (F), recency (R), money value (M).

![Fig. 2. Selected and relevant elements of recall and precision](image)

### Table 1. Measuring the loyalty level of each cluster of customers

| Cluster  | No customers | $C_{jF}$ | $C_{jM}$ | $C_{jR}$ | $C_{jI}$ | Ranking |
|----------|--------------|----------|----------|----------|----------|---------|
| Cluster1 | 156          | 0, 0074  | 0, 0024  | 0, 7425  | 0, 5387  | 4       |
| Cluster2 | 94           | 0, 0124  | 0, 0243  | 0, 6954  | 0, 5256  | 5       |
| Cluster3 | 124          | 0, 0214  | 0, 0147  | 0, 6475  | 0, 4737  | 6       |
| Cluster4 | 77           | 0, 0024  | 0, 0010  | 0, 7854  | 0, 5687  | 2       |
| Cluster5 | 19           | 0, 0015  | 0, 0009  | 0, 6289  | 0, 4553  | 7       |
| Cluster6 | 53           | 0, 0045  | 0, 0041  | 0, 7468  | 0, 5431  | 3       |
| Cluster7 | 27           | 0, 0859  | 0, 0687  | 0, 8941  | 0, 6672  | 1       |
| Cluster8 | 50           | 0, 0063  | 0, 0057  | 0, 5487  | 0, 3986  | 8       |

### Table 2. Classification of users in terms of destructiveness

| Classes | Number of users | Number of interactions | Amount of interaction | User’s condition | Rank |
|---------|-----------------|------------------------|-----------------------|------------------|------|
| class1  | 284             | less than 1            | more than 10000       | normal           | 8    |
| class2  | 193             | more than 1 less than 5| more than 20000       | normal           | 4    |
| class3  | 108             | more than 5 less than 10| more than 50000       | normal           | 3    |
| class4  | 15              | more than 10 less than 15| more than 100000      | normal           | 2    |
| class5  | 1               | more than 15           | less than 100         | normal           | 1    |
The RFM model results are used for ranking the customer. For clustering with normalized variables, RFM and K-means algorithm and two phases are used. Two-phases clustering algorithm is one of the clustering models which recommends the number of efficient clusters. By using this model, 4 efficient clusters are computed. But, in k-means algorithm, number of proper clusters is computed by using sum of the error squares. And after using these two algorithms, C5 model is used on both two-phases and algorithm k-means.

The results show that the loyalty mainly depends on good condition and also on culture of different domains. Finally, precision of created rules with C5 algorithm is on two phrases and k-means algorithms. After analysis and evaluating the gained rules from C5, it is concluded that applying C5 model on k-means clustering algorithm in detecting the high and average loyalty works poorly and has a low precision for loyalty detection on two-phase clustering algorithm.

5.1 Evaluating the Cheater-user Detection System

The ranking technique should be used to detect the destructive users. In this study the fuzzy tree is used. To recognize such users, especial features need to be examined. Some of them are as follows:

- The amount of user’s stagnant account
- User’s account transaction variance
- The amount of transactions and the way of doing transactions

The main goal of ranking to detect the destructive users is the high number of transactions with the high number of transactions and low expense was added to the data to examine the performance of this algorithm and the ranking. As it is clear one imaginary destructive user was added (class 5) was detected. Users with 100 daily transactions and the cost of 20 Rials was detected as a destructive user. In class 4 transactions were found as suspicious due to the large number of transactions. In this class 15 users had 10-15 transactions each day. These users are known as the suspicious users.

5.2 Detecting the Cheating People in Malaysian Islamic Banks

In [1] the designed technique includes the population of all Islamic banks in Malaysia. The
questionnaire includes two parts called respondent profile and the effect of fraud prevention and technique detections and the effect of practical application/software on detecting and preventing from fraud.

He respondents were asked to show their opinions on the level of effectiveness of each technique or strategy which was according to Likert Scale which was from "not very effective" to "very effective". Applied techniques to detect the cheating people is: training the morality principle, observing the asset form, especial phone line of the fraud, password back up, continuous auditing, the reference staff review, data mining. Through evaluating the answers, by showing the level of their agreement in four sections of Likert scale which are intended to prevent the fraud and to detect techniques by analyzing the back-up software or practical application, it is observed that the most effective items in fraud decreasing strategies are computed with the other six groups of variables. The control procedure, organizational policy, constant monitoring, communication devices of the staff, comprehensive control of fraud, supervision and revision. In this table bank compromising was ranked ninth as the most effective technique according to the respondents. Meanwhile, due to particular reasons, digital analysis is considered as the least effective technique. One of these reasons which is the unfamiliarity of this analysis technique that respondents showed less interest in that.

6. CONCLUSION

World economy has encountered money laundering phenomenon and its destructive effects on the economy of countries, over last decades. Money laundering is a clustered, constant, complicated, and long term procedure, which is usually done in long scales that causes for the change of dirty money earning from committing a crime into legal and legitimate shapes; in a way that it would be difficult to detect its criminal origin. Money laundering prevention is of high importance, which has not been academically worked on yet. In this regard, using a suitable system for recognizing people or money laundry networks is necessary.

In this study, the researcher has identified malicious users in electronic banking system, by applying RFM developed method, in order to evaluate customers’ loyalty. Therefore, by studying users’ profiles, some of the features are extracted. These features can be, for instance, money transaction with high amount in high risk domain in terms of money laundry, withdrawal or deposit with high and multiple amounts in a limited period of time, restarting of stagnant accounts with considerable amount, etc. In the present research, by providing a fuzzy decision tree and customers’ behavior vector injected into it, the network training is conducted. Accordingly, the decision tree and fuzzy systems are comprehensively explained and the results of the evaluation techniques are completely discussed and represented.

Moreover, RFM features and MLP classifications are used to identify the loyal customers. The three-fold features of refreshment, frequency, and shopping amount is completely discussed for every customer, whereby the customers’ scores were established as well. This classification aimed to categorize the credible users of neural networks. Results of current research indicate that represented techniques possess high precision values, in comparison with previous techniques.

According to the real time data banking systems, future banking areas will be selected authentically. Due to the statistical computations, authorities predict that the number of banking records in every area will reach the threshold of 5000, by primary notifications. There exist many represented fields that are comprehensively drawn by the economists and statistical survey running experts. Such records which are documented in the abovementioned fields include amounts, time, date, and number of transactions, plus the account number, origins and destination of successful transactions. The abovementioned transactions are acquired through gaining the real bank data transmission records. In addition, by analyzing these records, more efficient data outputs are obtained. In the present survey, due to the existence of a large number of transactions and data systems, the researcher has only acquired 400 data running tests in order to obtain the required data analysis results for the overestimation of comprehensive conclusion.

The results of accomplished studies on the assessment of banks’ loyal customers indicate that recognizing and keeping loyal customers by
using data mining techniques is costly and more expensive than attracting new customers. According to the above-mentioned results, disregard of having or not having Islamic Identity, no organization is safe from fraud. Meanwhile, it ought to be monitored by the senior-managers and the banks should not be dependent on one single technique for overcoming the fraud. Respondents have found that bank reformation is the most effective technique for overcoming the fraud, according to the high number of transactions, on large amounts of cash stolen. Therefore, having a regular number of compromises is a way to ensure that the stolen money will act as a means to recognize and correct both the accounting and non-banking interactions.

7. SUGGESTIONS FOR FURTHER RESEARCH

According to the obtained results and findings of the present study, the researcher has described a proposal for the future researches. The substantial components are explained as follows:

1. Using multi-criteria decision-making software, such as TOPSIS to weigh the features
2. Authors must use other hybrid methods such as the genetic algorithm or decision tree, to obtain the fuzzy rules,
3. Using parallel algorithms is very practical, and by combining this algorithm with other computational processes for the selection of features, the pertinent speed will be increased.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Rahman RA, Anwar ISK. Effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks. Procedia-Social and Behavioral Sciences. 2014;145:97-102.
2. Tianqing Z. An outlier detection model based on cross datasets comparison for financial surveillance. Proceedings of the Asia-Pacific Conference on Services Computing, IEEE. 822-822:0228.
3. Wang SN, Yang JG. A money laundering risk evaluation method based on decision tree. In 2007 International Conference on Machine Learning and Cybernetics. IEEE. 2007;1:283-286.
4. Gao S, Xu D. Conceptual modeling and development of an intelligent agent-assisted decision support system for anti-money laundering. Expert Systems with Applications. 2009;36(2):1493-1504.
5. Gao S, Xu D, Wang H, Wang Y. Intelligent anti-money laundering system. In 2006 IEEE International Conference on Service Operations and Logistics, and Informatics. IEEE. 2006;851-856.
6. Xuan L, Pengzhu Z. An agent based anti-money laundering system architecture for financial supervision. In 2007 International Conference on Wireless Communications, Networking and Mobile Computing; 2007.
7. Lv LT, Ji N, Zhang JL. A RBF neural network model for anti-money laundering. In 2008 International Conference on Wavelet Analysis and Pattern Recognition. IEEE. 2008;1:209-215.
8. Michalak K, Korczak J. Graph mining approach to suspicious transaction detection. In 2011 Federated conference on computer science and information systems (FedCSIS). IEEE. 2011;69-75.
9. Huang YP, Lu CC, Chang TW, Horng MS. An intelligent approach to detecting the bad credit card accounts. In Proceedings of the 25th conference on Proceedings of the 25th IASTED International Multi-Conference: artificial intelligence and applications. ACTA Press. 2007;220-225.
10. Herrera F, Lozano M. Fuzzy adaptive genetic algorithms: Design, taxonomy, and future directions. Soft Computing. 2003;7(8):545-562.
11. Quah JT, Sriganesh M. Real-time credit card fraud detection using computational intelligence. Expert Systems with Applications. 2008;35(4):1721-1732.
12. Sánchez D, Vila MA, Cerda L, Serrano JM. Association rules applied to credit card fraud detection. Expert Systems with Applications. 2009;36(2):3630-3640.
13. Yamakawa T. A fuzzy neuron and its application to pattern recognition. Proc. of IFSA’89. 1989;30-38.
14. Jang JSR, Sun CT, Mizutani E, Ho YC. Neuro-fuzzy and soft computing—a computational approach to learning and
machine intelligence. Proceedings of the IEEE. 1998;86(3):600-603.

15. Qiasi R, Minaei-Bidgoli B, Amooee G. Developing a model for measuring customer’s loyalty and value with RFM technique and clustering algorithms. The Journal of Mathematics and Computer Science. 2012;4(2):172-181.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle4.com/review-history/46513

© 2019 Maryam and Ali; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.