Asian Journal of Information Technology 14 (6): 239-245, 2015
ISSN: 1682-3915
© Medwell Journals, 2015

The Fraud Detection in the Bank Payments and its Methods

Roohollah Fallah Nejad
Department of IT, Faculty of Engineering, Islamic Azad University,
Electronic Branch, Tehran, Iran

Abstract: The aim of this research is to investigate the fraud detection in the bank payments and as well as some of its methods for creation, distribution and sharing of knowledge in this context. With the increasing use of modern banking systems and the increasing number of banking transactions has been found more financial abuses and fraud in these transactions. These abuses in addition to reduce the significant financial resources leads to reduce customers' confidence to the use of modern banking systems and therefore, the reducing of the effectiveness of these systems in the optimal management of capital and financial transactions. Therefore, it is needed the ways to identify suspicious transactions and be prevented of doing them. This research, while is examined and considered a variety of existing and potential methods in the field of bank payments, is discussed the fraud detection in the bank payments and also some its ways for creation, distribution and sharing. This research is considered the combination of this document and volume analysis of the website libraries according to the website information and biometric for data collection. The results of reviews show that economy and technology growth as provides new fields of services for bank customers also causes the increasing of the scope of bank frauds. Therefore, the software analysts can be used a suitable systems to detect and prevent of fraud with proper understanding of the banking systems and a variety of structural and process shapes.

Key words: Fraud detection, abuse bank, fraud in the bank payments, fraud detection methods, libraries

INTRODUCTION

Today, fraud which has a history as the human's life is considered a multi-million dollar business in the world and its financial volume is on the increasing day by day. In recent years, the development of new technologies has opened many ways for defrauders and criminals which can commit fraud. The creation of a new information system in addition to the all benefits which has may be put more opportunities to commit fraud available for criminals. The fraud detection techniques, in addition to detect and analyze happened frauds and scams somehow by understanding users and costumers' behavior is trying to predict their behavior and decreases the risk of doing frauds. Due to the high cost of direct or indirect fraud, banks and financial institutions are looking for acceleration and speed in recognition of the activities of fraudulent and swindlers. This issue is valid and reliable because of its direct effect on service to the customers of these institutions, the reducing of operating costs and remain as a financial services provider.

MATERIALS AND METHODS

The bank payment systems: The payment system is included a mechanism which van be transferred money from an account in a bank to the account in the other bank. And therefore, the role of the payment system in the economy is such vessels which deliver money to the different economic agents. Thus, the guide and supervision on the right, precise and flawless performance of the payment system in the monetary sector of country is one of the main tasks of central banking in today's world.

Transaction: These days everything which do in the internet bank, mobile bank and SMS of your bank is related to transaction. In fact is added to the number of times which see and hear this word day by day but what is the meaning of transaction and what is its work? The action of implementation orders in the database management system is called transaction. In the simplest word, transaction is the action of implementation of user orders in the database bank. In the recent years, Iran had dramatically growth in the number of banking transactions. Figure 1 shows a comparison of the number of credit card transactions on ATM and sales terminals from 2008-2013.

As is visible from the figure, the number of these transactions in 2013 toward 2008 have been along with the growth >5 times. With considering the increasing of the use of modern banking systems, the probability of

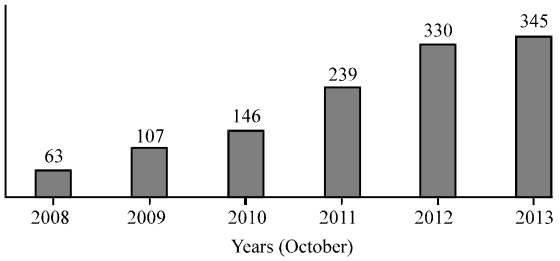

Fig. 1: The number of credit card transactions on ATM and sales terminals from 2008-2013; number of done transaction by ATM and electronic scales

occurrence of fraud and financial abuses will be also more. Therefore, is needed the methods to detect suspicious transactions as online and be prevented from their performance.

Fraud: For the word fraud in articles and scientific resources is expressed the different meanings but what is common and same in all these definitions is that the fraud is a kind of misuse of resources in the direction of personal interests deliberately and completely illegally. Fraud in general concept is included the distortion of the significant facts by who knows his subject is not true and or the offering of facts with complete disregard with respect to their accuracy and with the intent to deceive others. In other definition, the fraud word is included that misuse of an organization's profit without necessarily leads to its legal consequences (Ghosh and Reilly, 1994). In the other definition, fraud refers to the process which one or more persons deliberately and secretly deprive others of anything of value for their personal interests.

Fraud in bank payments: Today, with the development of modern technologies and the global communications, fraud is being increase dramatically and imposes the huge costs to businesses (Dorronsoro and Gruz, 1997). As a result, the identifying of fraud has become an important issue. Financial systems based on information technology because of the high potential which have in the direction of possibility of the money theft in the high content, most are easy targets for attackers which is used authentication defect of multiple identities and or available weak points in the implemented security models in the services and is implemented their goals. The weak authentication identity which happens by signed mechanisms, pin code, password and security code card causes becoming easier the illegal financial transactions from attackers and through the implementation of the innovative system attacks.

In Table 1 is shown total financial losses of institutions and bank of England through bank cards from 2004-2007 and during 4 year. In 2004, financial institutions

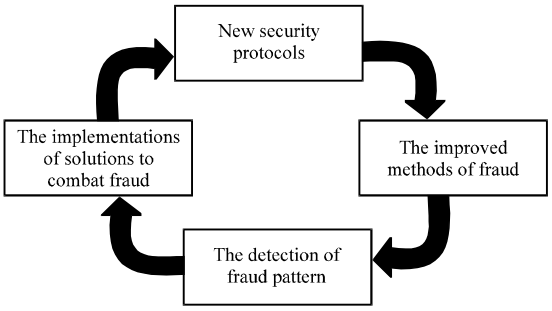

Fig. 2: Life cycle of financial fraud

Table 1: Total financial losses of institutions and bank of England through bank cards

Type of fraud	±(06/07) (%)	2007	2006	2005	2004
Telephone, internet and email (the frauds without the availability of card)	+37	29.05	212.7	183.2	150.8
Forging card (including mantling and copying)	+46	144.3	98.6	96.8	129.7
Fraud through the lost or stolen cards	-18	56.2	68.5	89.0	114.4
The stolen of ID cards	+7	34.1	31.9	30.5	36.9
Emails without a receipt	-34	10.2	15.4	40/0	72.9
Total	+25	535.2	427/0	439.4	504.8

Table 2: Simultaneous change and the growth of fraud in services area on the online and electronic banking

Type of fraud	±(06/07) (%)	2007	2006	2005	2004
Fraud in the electronic banking (online frauds)	-33	22.6	33.5	23.2	12.2
Fraud in the checks bank	+10	33.5	30.6	40.3	46.2

and banks took an active step in order to decrease statistics of fraud and swindling through card, in this way that from available methods which was based on the customer's signature are switched toward authentication identity method with help of pin code in all POS devices.

Similarly, in Table 2 also is shown simultaneous change and the growth of fraud in services area on the online and electronic banking during 4 years. During this period, the number of carried out phishing attacks by fraudulent from 1713 cases in 2005 has reached to 14156 cases in 2007. This issue is caused the creation of capital in this area in the name of "the convert of customers with poor knowledge in the field of online security protocols to the customers with the top online security information". While, the increasing of customer awareness of such methods in 2007 lead to the reduce of charlatan's success in the phishing operation and in the online area, the agility behavior of fraudulent from 2004 onwards also has caused the increasing of growth rates of frauds in the field of check. These figures show that the ability of fraudsters not only is enhanced as creatively and to attack more complex systems, but is also developed as quite active and adopting their methods to deploy security. According to Fig. 2, generally fraud in the lifecycle of fraud can be used as a model, in a way that

with analysis it an appropriate response is given to this fraud and again with the development of knowledge and the offering of solutions and new protocols is opened the way for the cheaters and are formed the new methods of fraud and likewise continues the life cycle of fraud.

The emerging process of financial frauds, generally is diagnosed through the analysis and the extraction of information (data analysis) from the information bank transactions from financial institutions which will be marked and this issue helps to develop policies and security protocols and new attain identity. In return, cheaters also change their methods by implementing new security policies and also the identifying of opportunities for alternative fraud on new platforms and then methods and new patterns of fraud which is obtained as a result of implementing new security policies has been identified again and is anticipated and applied the strategies to prevent from their occurrence.

The identifying of fraud: Is a long time which the tradition methods of data analysis are used as a method for fraud detection. This work needs the complex and time-consuming researches and require the use of various fields of knowledge like financial, economic, business methods and legal issues. To operations collection or the actions which based on procedures or methods are trying to detect happened or are being occurrence frauds is called fraud identifying. Financial institutions are looking for fast action in recognition of activities of fraudulent and cheaters (Chan and Prodromidis, 1999). This issue is valid and reliable due to its direct impact on service to the customers of these institutions, the reducing of operating costs and remain as a financial services provider.

Fraud detection techniques: According to the anomaly detection approach and abuse detection is performed several techniques in order to detect fraud which is referred to some of them in the following.

Expert systems: The expert systems is attributed of computing systems in a way which have the ability to provide and argument in some rich fields of knowledge with looking at solve problems and giving the solution (Majumdar, 2006). The detectors of expert systems are coding the knowledge if then in the form of legislation. That means are specified if then by the help of law in what state, what event should be happened. As an example, the NIDES system which is implemented by SRI Company is used expert systems approach in order to identify attacks by the help of online monitoring of user activities. The NIDES system is included statistical analysis components in order to detect anomalies and as well as the analysis tools of rules in order to detect misuse.

Boron Hashtee: The mechanisms of Boron Hashtee is mean the view and extract of deviations which is determined the differences with the other observations. This mechanism is divided into two types of without supervised and with monitoring. The unsupervised approaches do not need to the previous knowledge and the history of events and the previous transactions in the databases, but with the same attributes have the ability to detect changes in the unusual transactions behavior and can identify any changes which leads to fraud. In the monitoring techniques are designed the models which can be distinguished difference between the behaviors like fraud and normal and actual behaviors. These methods need the accurate identification of like fraud transactions in the history of the information bank. In other words, in order to use these methods certainly should be had the history of information in the information bank which can by comparing these data is identified unusual behaviors. Therefore, the mechanisms based on these methods just only can recognize the frauds which are occurred at least once in the past and their history is also available in the information bank. The advantage of using unsupervised methods compared to monitoring methods is that in this method, there is also the possibility of detecting the undiscovered frauds and this issue is for this reason that in unsupervised method is not needed to the history of information in the information bank. For this reason, generally is used the monitoring methods to identify and detect frauds and the illegal transactions which is identified already and is available in the information bank.

Neural networks: A neural network is a set of connected nodes which are designed by mimicking of the function of human's brain. Each node has a weighted communications to several other nodes in the adjacent layers. In the neural networks is designed the data structure in the case of software which can act like neurons to these data structures is said node. Then, by creating a network between these nodes and applying a learning algorithm to it are trained the network. In this memory or neural networks, the nodes have two active modes (on or 1) and inactive (off or 0) and each synapse (the relationship between the nodes) has a weight. Synapses with positive weight causes stimulate or enable of the next inactive node and synapses with negative weight are disabled or inhibited the next connected node (if be active). An artificial neuron is a system with a lot of input and only one output. Neurons have two cases, education case and performance case. In the education case, the neuron learns that is excited against the specific input patterns and or so-called is fired but the emerging process of the financial frauds generally is diagnosed through the analysis and extraction of information (data

analysis) from the information bank of the financial institutions transactions which will be marked and this issue helps to develop policies and security protocols and the attaining of new identity, in the performance case when an input detected pattern enter, is presented its corresponding output. If the input is not component of the detected inputs, the fire rules decides for its arousal and deficiency. First time, Braves and Langsdorf are offered the combination of role-based continuous systems with approaches based on neural systems. Falcon Fraud Management system which is a very powerful tool in order to prevent the fraudulent activity in the misuse of debit and credit cards is used neural network algorithms. This system forecasts the possibility of fraud on an account by comparing the current transaction and the past activities of card holder. If this system is recognized such a fraud transaction on card, immediately will be taken a call with the card holder and if the card holder is approved the fraud on the card in order to prevent the occurrence of fraud, the card will be blocked immediately. If the Falcon system is identified any fraud but is not possible the possibility of call with the card holder in order to ensure from the occurrence of fraud, the card is blocked temporarily and the card holder should be pursued the condition by phone with call center of bank and the card will be blocked until the card holder is not registered contact with the call center. This system is able by using the neural networks is trained the spending pattern of card holder and is diagnosed any inconsistencies in the method and how to pay the money and is considered as fraud. In design and development of Falcon prediction system are contributed techniques and machine learning technologies, the recognition of adaptive pattern, neuron networks and statistical models. Another example of application of neural networks is MLP Neural algorithm. This algorithm is acted just only on the information of a transaction and the moment previous history of same transaction and is no need to use previous stored information history of card holder on the information bank. Another example of application of neural networks is the grain parallel neural networks method which is used fuzzy neural networks and role-based approaches simultaneously. One of the detection systems of the attacks which work based on the neural networks is NNID system which is an anomaly detection system which is implemented by the corporation neural network and under the UNIX operating system. The performance of this system in such a way that is assessed the users' behavior during the day decides based on it. Because this system is used daily log data and in the case of offline, the using of it is very convenient and low cost. Artificial neural networks provide the possibility of detection of unseen future behaviors of users in both approaches of anomaly detection and abuse detection. These methods ae implemented based on neural networks corporation.

Model-based reasoning: The model-based reasoning is a detect abuse technique which are recognized the attacks through the visible activities which is deducted through an attack signature. For this purpose is needed to the one information bank of the attack scenario and include signature or the sequence of attacks behavior. Exactly similar to procedures of antivirus software which is realized the virus from the signature of any virus on the files, this technique also through signature and the information bank which holds, identifies the attack. The system which works based on this collect the evidences of the attack and do this work consistently and repeatedly to some extent which reach to the threshold. At this point is detected one attack and will be announced immediately. The pattern-matching approach which was suggested by Komar and Spaford is recognized the abuse attacks based on colored Petri nets. This pattern is implemented under Linux environment and is used an audit trail for input.

Rules-based approach: This method is a combination of the absolute analysis applications and differential in the differential analysis, a set of flexible criteria can be implemented to identify any changes in the details of a user's behavior history. Rules-based approaches generally have best performance with the users ID which are included a clear information and in them the fraud criteria point out to the rules. The managing of this method is very difficult work and this issue is because of the proper configuration of rules is needed the programming of the best solution in the identification systems of fraud, integration and combination of detect abuse approaches and anomaly detection. One of the produced tools by this approach is PDAT which is prepared by Siemens ZFE company and is a fully flexible tool by a widely application in order to detect fraud in the mobile phones.

RESULTS AND DISCUSSION

Data analysis: Today the data analysis methods are known as the best solution for automatic identification of fraud in the different areas. In the systems, data analysis is defined as the process of discovering and extracting of hidden patterns from the high volume of data. Most of the data analysis methods is used to identify and discover of fraud and financial abuse. One of the wonderful benefits of data analysis methods in the attacks detection is the possibility of implementing of a class of models which can

identify and provide the new attacks before human intelligence is recognized them and or is seen by professionals. Also classified models with the algorithm of association rules and repeated events as well as are used in order to detect anomalies. This approach can create concise and accurate detection models for the large volumes of information automatically. Although, this method require a very large volume of audit information in order to create a set of characterized rules of any user. In addition, this learning process is a continuous and accurate study from a system of attack detection because of the set of used rules by detection modules which are not fixed in a period of time basically.

The analysis of transition: This method is an abuse detection technique which in it the attacks is displayed as the sequence of transient monitoring system. The activities which are happened in an attack are defined a transition between cases. Attack scenarios also are defined in the form of state transition diagrams. In these diagrams, the nodes are as the cases of the system and arcs also are as related actions. In any case, if reach to an extreme case this will be meant that when will have attack. STAT system is a very famous rule-based expert system which is designed from the multi-user computer system in order to search known exploits in an audit trail. As well as, USTAT is also a primary sample of STAT which has been designed under the UNIX Operating system.

The use of intelligent systems in the detection of fraud: With the expansion of the field of science in field of information systems the intelligent practical programs which deal to solve the problem according to the existing legislation in the area of human knowledge is increased dramatically. The techniques used in these systems are known as the artificial intelligence mainly. Intelligence systems have a wide activity but in here is tried to explain their use in the detection of fraud. Such systems is detected the situations which there is the possibility of outbreak of fraud and are offered necessary warnings to stop it. With the development of electronic networks and the increasing of transactions the investigation of data has been very hard by human (Liu, 2004). The use of human in the investigation of information is required time and relatively high cost. This is in the way that the customers need the increasing of speed of transactions and the offering of services. The intelligence systems with the available knowledge in the customer behavior patterns make easy this issue somewhat. In this study, to familiarity with the method of help of these systems, is selected and explained two industries of insurance and banking. According to happened researches, in the most customers' requests there are key words which can cause the creation of suspicion in relation with a false claim. In the intelligence systems the questions or information which is seen in the time of occurrence the fraud is proposed for the customers and with investigation of past behavior patterns are declared the suspicious cases. In these cases, the assessing indexes are designed in the system which can estimate the possibility of occurrence of fraud by using these indexes. The applicants should be answered to 10-15 questions on their request. The reply to these questions allows the system to specify the rate of fraud. The way to get questions will be done by using the data analysis among the past demands of the customers. Whenever is discovered a new fraud, the system will be able thereafter to offer a suitable answer by using this behavior pattern. In the financial transactions is different the type of used algorithms in the intelligence systems. In the credit cards the customers behavior patterns is checked every night or every 2 h which the system can offer required notices through the discovery of deviations.

The important statistical methods of data analysis to detect fraud:

- The methods of data preprocessing to discover, acknowledgment, the error connection and filling the incomplete and missing data (forecast and estimate)
- The calculation of various statistical factors like averages, performance standards, probability distributions and, etc., for example, the averages may be contained the average call duration, the average number of calls per month (or every day) and the average of delays in paying bills
- Models and probability distributions of various commercial activities or based on different criteria or probability distributions
- The calculation of user specifications (the classification of users, customers and orders to the various classes) and the statistics indexing of these specifications (based on criteria, normal distributions and, etc.)
- The time series analysis of the time-dependent data.
- Grouping and classification to find patterns and commonalities among data groups
- The matching of algorithms for detecting unusual cases in the deals or users behavior based on known early methods and their specifications and comparison

The methods also need to remove error warnings, to estimate risk and to predict the future of current deals or users.

Important methods based on artificial intelligence to detect fraud:

- Data extraction for classification, grouping and categorization of data and automatically find commonalities and rules in data which may be mean interesting patterns and associated with fraud
- Expert systems of the expert coding to track and detect fraud in the form of laws and regulation
- Pattern recognition to explore the approximate classes, groups or suspicious behavior patterns whether automatically (non-regulatory) whether through the implementation of a given inputs
- The neural networks which can be learned the suspicious patterns of samples and are applied to discover them later

The role of genetic algorithm in the detection of fraud: At the moment the intelligence systems are entered a new field of human knowledge, in a way that will be able is learned the new fraud pattern before happening, by using the cost-benefit analyses are offered an appropriate decision instead of human. One of these methods is the genetic algorithm. The genetic algorithm which is used in order to detect malicious attacks and their isolation from the normal uses, the genetic algorithm is a method of artificial intelligence with an emphasis on problem-solving which is acted according to Darwin's theory of evolution an extensive application in the mathematics.

This algorithm is based on Darwin's theory of evolution and the answer of question is solved through the genetic algorithm is improved regularly. The genetic algorithm starts with a set of answers which are shown through chromosomes. In this algorithm the answers from population are used to produce next population which the production action (likely) will be along with crossover and mutation. In this process, it is hoped that the new population be better compared to the previous population. The selection of some answers (chromosomes) among the total responses (parents) in order to create the new answers (offspring) is based on their utility level which this work takes place by using the fitness function. It is natural that more appropriate questions have more chances for reproduction. This process continues until the establishment of condition which is determined from prior (like the number of populations or the answer improvement level).

The advantages of using the genetic algorithm:

- The genetic algorithm can be used in the issues which have a large search space
- As well as in the issues with the complex hypothesis space which are unknown the impact of its components in the general hypothesis can be used GA to search
- For discrete optimization is used more and is also available in the continuous issues
- Can be implemented the genetic algorithms in parallel easily, hence can be used the cheaper computers in parallel
- The possibility entrapment of the algorithm in the local minimum is less than other methods

CONCLUSION

The done researches in this area show that several ways have been used to detect fraud since which among this, the neuron networks method had more application. Especially, in the older researches the neuron networks method was used in different species. Also, it is seen that because lack of access to the labeled data the researches have gone toward the methods which without the use of labeled data can recognize the fraud. As well as are provided the methods which are used time series for fraud detection. But, recent researches are gone toward synthetic methods. What will be obtained from the conducted studies in this area is that the researchers in this area is faced with data problem. Since, data of banks are secret hardly can be reached the real data and there is not any Benchmark data for this purpose. Hence, in the presented researches is used a used data bank which has not been the ability to share it with the other things and in some cases is not specified the data details and or is used a simulator to create a dummy data. It seam, the researchers continues so in this area and there are more data analysis methods which are not used in this area. Since, there is the less access to the labeled data, the researches process is to the unsupervised methods. Also it is seen that in the recent researches more have been used the synthetic methods which are provided the relatively acceptable results. With regard to the benefits which the genetic algorithm has and with regard to this issue which the fraud detection in the bank payments is among the issues which has a large, complex and has a high dissociation search space. It is suggested to be used a combination of the two methods of neural networks and the genetic algorithm.

RECOMMENDATIONS

The negative effects of fraud is justified the need to design fraud detection systems. The technological advances is caused facilitate in the development of information systems of fraud detection (Majumdar, 2005). The fraud detection techniques is included the complex search techniques which is discovered the fraud patterns through the investigation of transactions, the customers' account and the customer consumption behavior and announces on time. The awareness of different types of bank frauds also can be useful to develop preventive

systems. Bank managers in the case of familiarity with different types of bank frauds can be designed a suitable monitoring processes. On the other hand, by identifying the processes which there is the possibility of doing fraud in them can be used warning systems and fraud detection in these processes in more appropriate way. Economy and technology growth as provides the new areas of services for bank customers also causes the increasing of the types of bank frauds range. The increasing of volume of information and the complexity of organizations is required proper and informed management. Hence, should be provided the better exploitation from them with full knowledge of existing conditions. The software analysts also with a proper understanding of the banking system and a variety of structural and process shapes can be used a suitable systems to detect and prevent of fraud.

REFERENCES

Chan, F. and S. Prodromidis, 1999. Distributed Data Mining in Credit Card Fraud Detection, IEEE, 14: 67-74.

Dorronsoro, G. and S. Cruz, 1997. Neural fraud detection in credit card operations. IEEE, 8: 827-843.

Ghosh, and D.L. Reilly, 1994. "Credit Card Fraud Detection with a Neural-Network", IEEE, 3: 621-630.

Liu, T.R., 2004. Artificial Immune System for Fraud Detection. IEEE, 2: 1407-1411.

Majumdar, V.S., 2005. A Game-Theoretic Approach to Credit Card Fraud Detection, Springer, 3803: 263-276.

Majumdar, K.S., 2006. Two-Stage Credit Card Fraud Detection Using Sequence Alignment. Springer, 4332: 260-275.