Data Mining for Fraud Detection

Arwa Abu Shmais, Rana Hani

Prince Sultan University, Saudi Arabia

207410181@pscw.psu.edu.sa

207410187@pscw.psu.edu.sa

***Abstract* – The advent of new technologies and the fast base of technological development have created new possibilities as well as imposing new challenges. Fraud, which is one of the greatest challenges for businesses and organizations, has been equipped with new technologies to take new and unconventional forms that are stealthier and more difficult to recognize than the traditional forms of this crime. Therefore, the techniques for detecting fraud had to develop as well to provide more efficient protection. The most recognized and effective technology that has been implemented for fraud detection is data mining. This research paper will explore some of the most effective data mining techniques for detecting different types of fraud. These techniques will first be categorized according into supervised and unsupervised methods. Those techniques will be explored in the fields of mobile telecommunication fraud, credit card fraud, medical insurance fraud and computer systems intrusion detection. In addition, a real life case will be presented to illustrate the application of one of the techniques in credit card fraud detection.**

I. INTRODUCTION

The advancement in technology and communication has created new opportunities for committing fraudulent acts. These acts impose serious threat to organizations on the financial, operational and psychological levels. In addition to the monetary losses, fraud can have a staggering effect on the organization's reputation, goodwill and customer relations. Therefore, organizations try to implement a variety of techniques to detect and prevent fraud. Among those techniques is data mining.

This research paper explores some of the data mining techniques used for mobile telecommunication, credit card and medical insurance fraud detection as well as the use of data mining for intrusion detection. In addition, it presents a case in which data mining techniques were successfully implemented to detect credit card fraud in Saudi Arabia. Before going into the details, a brief description of fraud and data mining is introduce to pave the path.

II. FRAUD

There are many definitions for fraud that vary depending on the perspective of interested parties [29]. In its simplest definition, fraud is the criminal activity of misrepresenting information to achieve unjust gains [10]. The Institute of Internal Auditors' International Professional Practices Framework (IPPF) defines fraud as "… any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage."

The process of detecting and preventing fraud can be very challenging due to the characteristics and nature of fraud. Calculating the actual costs of fraud for businesses and corporations is a formidable task because of the stealthy nature of fraud. The detected fraud cases represent only the "tip of the ice berg" of all the frauds that go unnoticed [11]. In addition, fraud can be very complex and has some temporal characteristics and patterns that need to be identified [10].

Studies and research have proven that traditional fraud detection techniques, such as internal control systems, external audits, risk management systems and whistle-blowing hotlines, might not be effectively applicable for the new trends in fraud. The most efficient and effective method for fraud detection is to use data mining and analysis techniques [3].

The next section provides a brief definition of data mining and highlights the most widely recognized classification and fraud detection techniques in data mining.

III. DATA MINING

A. Fraud Detection Techniques in Data Mining

Witten and Frank defined data mining as the process of discovering patterns in data. The process must be automatic or (more usually) semi automatic. The patterns discovered must be meaningful in that they lead to some advantages, usually an economic advantage. The data is invariable present in substantial quantities [3].

In other words, we could describe data mining as the use of sophisticated data search in order to discover patterns and connections in large pre-accessible databases. Fig 1shows an

illustration of the process of extracting knowledge from data using data mining.

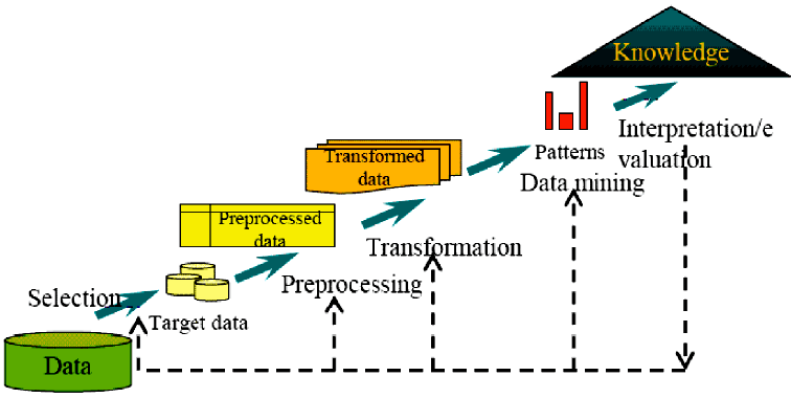

Fig. 1. The transition from raw data to valuable knowledge[1]

In general, data mining techniques can be classified into two categories according to the type of the machine learning techniques as:

1) Supervised Learning for Fraud Detection: This method uses supervised learning in which all the available records are classified as 'fraudulent' and 'non-fraudulent'. Then machines are trained to identify records according to this classification. However, these methods are only capable of identifying frauds that has already occurred and about which the system has been trained [3][30].

2) Unsupervised Learning for Fraud Detection: This method only identifies the likelihood of some records to be more fraudulent than others without statistical analysis assurance [3][30].

B. Summary of the Most Significant Fraud Detection Techniques

The table below provides a summary of some of the most widely known data mining techniques for fraud detection. Choosing the right method for a specific implementation depends on trial and error [37].

TABLE I[2]

Technique	Description	Use
Neural Network	It can be taught to implement sophisticated machine learning algorithms and pattern recognition to make predictions from historical data.	Mobile phone networks financial statement fraud and intrusion detection.
Fuzzy Neural Network	Use traditional association rules	Financial Reporting
Hybrid-Based System	Expert Knowledge is integrated with statistical power	Medical Insurance Fraud
Supervised Hybrid	Series of data mining techniques	Cellular clone fraud
MADAMID	Mining Audit Data for Automated Models for Intrusion Detection	Intrusion Detection
Fraud Signature	A signature is derived to concisely describe caller's behavior.	Telecommunication Fraud
Rule-Learning	A rule is used "if this and this and this then this" along with its accuracy and recurrence.	Credit Card Fraud
Decision Tree Analysis	A predictive model that is based on a sequence of decision	Credit Card Fraud
Link Analysis	Relates known fraudsters to other individuals	
Peer Group Analysis	Detects individual objects that begin to behave in a different way	Credit Card Fraud
Break-Point Analysis	Observation where irregular behavior for a particular account is detected	Credit Card Fraud
Three-level Profiling	Points any significant deviation from an account's normal behavior	Telecommunication Fraud
Predictive Analysis	Integrates a variety of techniques from mathematics, statistics with data mining to analyze current and historical facts to make predictions about future events	Credit Card Insurance Fraud Financial Statement Fraud

[1] Source: [12]
[2] Sources: [3], [28], [30], [34], [36], [37], [38],

IV. SELECTED FRAUD DETECTION TECHNIQUES

This section explores a selection of data mining techniques for mobile telecommunication, credit card and medical insurance fraud detection.

A. Mobile Telecommunication Fraud Detection

Telecommunication fraud has caused huge losses for telecommunication industries. According to the Communication Fraud Control Association (CFCA), it is estimated that the annual global fraud losses are in the range of $72 - $80 billion worldwide [13].

There are many forms of this fraud that can be classified under two umbrellas. The first type is subscription fraud in which fraudsters obtain telecommunication accounts without paying for the service. The second type is called superimposed fraud, in which the fraudster takes over the account of a legitimate subscriber and all the call charges are billed to that legitimate subscriber. It includes cellular cloning, calling card theft and cellular handset theft [14]. This form of telecommunication fraud is considered to be the most challenging type for telecommunication companies. Therefore, most telecommunication companies, such as AT&T have dedicated research to develop effective detection methods for this type of telecommunication fraud [15]. This part will highlight the superimposed telecommunication by explaining the most widely used method and then explaining cellular cloning fraud as an example.

Using data analysis techniques for telecommunication fraud is a challenging process due to the characteristics of telecommunication. First of all, there are huge amounts of data in billions of records that are kept in telecommunication databases from around the world [31]. Another challenge is the form of raw data from call details and network data which is not suitable for data mining. These data take the form of time series that represent individual event. To enable using them for data mining, they must be summarized according to previously defined summary features. A third challenge is the rarity of events and instances of telecommunication fraud. Finally, the continuous nature of data [16] indicates that any learned rules or modules must be applied in real time [14].

The most common method for identifying superimposed telecommunication fraud is to use different detection techniques for compariong the users' current calling behavior against past calling behaviors [14]. After considerable reading and researching, signature-based methods were found to be most clearly illustrating the basic ideas of superimposed telecommunicatio fraud detection. TABLE I shows other examples of methods that were breifly presented in the previous section of this paper.

1) Signature-based Methods: These methods are considered supervised/unsupervised hybrid [17]. Signatures are simply telecommunication accounts summaries that are time driven and capture the behavior of a credit card or computer user including frequency of use, type if use, length of use and location of use [16]. As Ferreira et. al define it [15], a signature is a "vector of feature" whose variables are obtained from the coded fields of a collection of Call Detail Records (CDRs). Each CDR is in turn a vector of features that can be discrete, such as the calling city, or continuous, such as the calling duration [35]. Examples of those fields from the CDR include [16]:

- Data of call
- Length of call
- Destination of call (example: 39-0382-506224)
- Time of call
- Origin of call (example: 973-360-8430)
- Payer of call (example: 973-360-8430)

Components of a Signature

The variable contained within a signature can range from simple atomic values, such as integer or real or average values [18], to complex values consisting of two codependent statistical values, the average and the standard deviation of a give feature [15] depending on the needs and complexity of the data and calculations.. A list of variables that can be included in the signature is shown in Fig. 2.

Description	Type
Duration of Calls	Complex
Number of Calls - Working days	Complex
Number of Calls - Weekends and Holidays	Complex
Number of Calls - Working Time (8h-20h)	Complex
Number of Calls - Night Time (20h-8h)	Complex
Number of Calls to the Different national networks*	Simple
Number of Calls as Caller (Origin)	Simple
Number of Calls as Called (Destination)	Simple
Number of International Calls	Simple
Number of Calls as Caller in Roaming	Simple
Number of Calls as Called in Roaming	Simple

Fig. 2. Variables that can be included in the definition of signature.[3]

Updating Signatures

Signatures must be updated continuously in an event driven manner to be able to recognize fraud as it happens [31]. In general, there are two variations of signatures[33][18]. The first type of signatures has a time-oriented processing in which users' actions are accumulated, kept and processed during a time unit for later analysis. This type is usually referred to as "summary". These summaries have a shorter time span such as an hour, half a day or a complete day. The second type of signatures uses action-

[3] Source: [18]

oriented processing, which are simply called "signatures". This type of processing makes the direct comparison between current actions related to the CDR against the signature. In order to capture the different behaviors in different situations, the signature needs longer time window which could be a week, a month or even half a year. The former type of processing is less costly considering the processing requirements of massive volumes of data used in the signature [18]; however, the later type is more effective and will be explained in further details.

Creating and Implementing Signatures

According to Cortes and Pregibon [16], there are two methods for using signature in fraud detection. In the first method, which is anomaly detection, the subscriber's signature is compared to subscriber's traffic itself so that any abnormal changes would indicate fraudulent behaviors. This is the method used by AT&T for telecommunication fraud detection [16]. Since not all changes in behavior indicate fraud, profile-based detection can be used. In this method, a library of generic fraud profiles is stored so that they will be compared with current traffic to identify fraudulent behavior.

The steps for implementing a signature using the anomaly detection method can be summarized as follows:

First of all, the signature is defined as ***S***, which can be obtained from Equation (1):

$$S = \varphi(w) \tag{1}$$

Where φ consists of a set of functions, and w is the selected time unit (time window) based on the type of signature processing. [15]

We wish to process a set of CDRs to identify abnormal behaviors. Let us assume that the set of CDRs is ***C***.

We need to extract from ***C*** the feature variables that compose the signature. This processing will be referred to as ***Pc***.

Now we have two vectors of feature variables for comparison: ***C*** and ***Pc***

Next is the determination of the distance between those two vector functions. Since the signature has a group of variables of different types, each one is given a sub-function to compose the final distance function. The processed distance function is

$$\boldsymbol{dist(S, C)} \tag{2}$$

The fraud analyst can control certain values within this function to give more or less importance to the variables.

Finally, this distance is compared to a threshold $\boldsymbol{\xi}$ defined by the analyst.[30] In the case of the following inequality

$$\boldsymbol{dist(S, C) > \xi} \tag{3}$$

An alarm will be issued. [18]

In more recent studies, dynamic clustering can be implemented where each signature is given a cluster membership and fraud can be indicated by the change in the signature's cluster membership.[14]

2) Cellular Communication Cloning:

As mentioned above, cellular cloning is a type of superimposed telecommunication fraud. Whenever a cellular phone is operating, it transmits two identification numbers that are unique to that customer's account which are Mobile Identification Number (MIN) and Electronic Serial Number (ESN). Cloning fraud occurs when those numbers are programmed into another phone that doesn't belong to the user [19]. In this method, fraudsters cannot be linked to the cloned accounts, which make them untraceable.

Traditionally, the MIN and ESN were transmitted without encryption, which made them more vulnerable to fraudsters. Then, the Global System for Mobile Communication (GSM) was introduced with the Subscriber Identity Module (SIM) card that contains user's account information which is programmed into the mobile phone once the card and authentication number are inserted. Nevertheless, Fraudsters were able to invent techniques and equipment to find ways to acquire user's accounts by copying and decrypting SIM cards [20]. Cloning may cause congestion of cell sites and a denial of service for legitimate users [19].

Experience has proven that any methods that depend on pre-call authentication, such as fingerprinting and authentication are not reliable and require changes in the hardware infrastructure. Therefore, post-call and user profiling methods have been more widely used.

There are different variations of Post-call method. One of those methods is collision detection in which call data are analyzed to identify overlapping calls by detecting the MIN-ESN of the calling cell phones.

Another post-call method is velocity check, which analyzes consecutive calls to see whether they have been placed by a single user travelling at a reasonable speed by measuring the time difference between calls and distances between their locations. For example, if a call has been made from New York and then another call from Los Angeles from the same account in a time of 20 minutes, this can be a sign of account cloning [19][32]. A disadvantage of the previous two methods is that individuals with low usage rates will not cause collision or velocity [19].

A third post-call method can be the dialed digit analysis which builds a database of the numbers dialed by the fraudster during the fraudulent activity to be compared against another database of the numbers called by legitimate user. An alarm is issued when the number of hits is about the dialed digit hits threshold [19].

In user profiling, which is the second method, machines are taught to identify "bandit" or fraudster calls by analyzing the calling behavior of the account itself. This makes it easier

to detect velocity and collision for customers with low usage rates [19]. Fig. 3 shows that by comparing the time, duration and location of each call, systems can identify the bandit's calls. The seventh and eighth rows in the table show that two calls with overlapping durations were made at the same time to different destinations.

Date & Time	Day	Duration	Origin	Destination	Fraud
1/01/95 10:05:01	Mon	13 mins	Brooklyn, NY	Stamford,CT	
1/05/95 14:53:27	Fri	5 mins	Brooklyn, NY	Greenwich,CT	
1/08/95 09:42:01	Mon	3 mins	Bronx, NY	White Plains, NY	
1/08/95 15:01:24	Mon	9 mins	Brooklyn, NY	Brooklyn, NY	
1/09/95 15:06:09	Tue	5 mins	Manhattan, NY	Stamford, CT	
1/09/95 16:28:50	Tue	53 sec	Brooklyn, NY	Brooklyn, NY	
→ 1/10/95 01:45:36	Wed	35 sec	Boston, MA	Chelsea, MA	BANDIT
→ 1/10/95 01:46:29	Wed	34 sec	Boston, MA	Yonkers, NY	BANDIT
1/10/95 01:50:54	Wed	39 sec	Boston, MA	Chelsea, MA	BANDIT
1/10/95 11:23:28	Wed	24 sec	White Plains, NY	Congers, NY	
1/11/95 22:00:28	Thu	37 sec	Boston, MA	East Boston, MA	BANDIT
1/11/95 22:04:01	Thu	37 sec	Boston, MA	East Boston, MA	BANDIT

Fig. 3. A sample of user profiling showing a cloned account[4]

B. Credit Card Fraud Detection

Credit card fraud detection is the process of monitoring the behavior of the customers' transaction level through a period of time [1].

1) Types of Credit Card Fraud:

The first type which is the most common is the application fraud. The individual will falsify an application to acquire a credit card. The individual will give false information about his/her financial status in order to receive a credit card [1].

The second type is assumed identity. Assuming someone's identity has been in the long-run form for credit card fraud. The individual will falsify a name with a temporary address [7].

The third type is financial fraud which happens when an individual wishes to gain more credit than he/she currently has. They will apply for a credit card under their own name, but the information regarding their financial status will be false [8].

The fourth is skimming technology. Magnetic card skimming is a small handheld device with the sole purpose of collecting and storing the information on any credit card [8].

The fifth type is never received issue. This type of credit card fraud involves the theft of the card while still in transit. This involves the theft of the card from the holder's mail [8].

2) Data Mining Techniques for Credit Card Fraud:

The first technique is the Peer Group Analysis. This type of analysis is an unsupervised method for monitoring customer behaviors over a period of time. For each individual that has a credit card account, a 'Peer Group' of accounts is created that exhibit similar behavior. As time goes by, the behavior of an account is tracked by those accounts in its peer group. If an account has subsequent behavior which deviates strongly from its peer group is thus considered to have behaved anomalously and is flagged as a potential fraudulent [5].

The second technique is the Break-point Analysis. This technique distinguishes spending activities supported from transaction information in a single account. Current transactions are matched up with prior spending activities to spot features, such as rapid spending and an increase in the level of spending, which would not essentially be captured by outlier detection [1].

C. Medical Insurance Fraud Detection

Data mining gives an employee the power to combine systematic techniques with someone firsthand business knowledge to turn data that has been attained into the insight you need to identify instances of insurance fraud and abuse [2].

By creating models from historical information, you can accurately pinpoint fraudulent claims out of the millions of claims that medical insurance companies receive each year. These data mining models lower the cost of fraud and abuse while saving your adjusters time [4].

Data mining empowers a variety of insurance providers with the ability to predict which claims are fraudulent so they can effectively target their resources and recoup significant amounts of money. Data mining helps medical insurance company to focus, for example, on claims with high percentage of recoverable fraud, isolate factors which indicates a payment request has a high probability of fraudulence, develop rules to use them to flag only claims likely to be fraudulent, and ensure adjusters could review claims that are not only likely to be fraudulent but also have the greatest adjustment potential [6].

The following scenario demonstrates how one insurance provider – in this instance a medical insurance provider – used data mining to build models based on previously audited claims to identify potentially fraudulent claims. With these models in place, the provider's claim audit selection will be more exact, generate more money through claim adjustments and save time and manpower.

A large insurance provider needs to accurately determine which claims are fraudulently filed so it can concentrate on preventing revenue loss. Over the years, this organization collected audit results on insurance claims. The organization seldom used historical records to identify probable fraudulent

[4] Source: [19]

claims in the future. Their previous methods often missed opportunities to collect money and adjusters spent too much time reviewing legitimate claims.

Data mining now enables this company to predict which insurance claims are likely to be fraudulent. This gives adjusters the power to determine what returns they should target, thereby, recouping millions of dollars otherwise lost and saving adjusters many hours of valuable time.

The insurance company's fraud detection office used IBM SPSS Modeler, the leading data mining workbench, to get results. Modeler examines each line entry on claims, compares the line entries against the amount of fraud dollars detected, ranks claims in the order of likely fraudulence and displays the results back.

Modeler's visual programming interface makes examining and modeling the audit records straightforward. Records used to model medical claims might include medical insurance billing records with detailed information such as recipient/provider codes and county of residence, diagnostic codes, admission source, length of stay and total charges claimed.

An important step in the data mining process is to continually ensure you are using the right data to solve your business problem. You must ensure data doesn't disproportionately represent any provider or exclusively associate any provider with one particular diagnostic code.

Modeler easily adds new variables to each record in the dataset. Then we can route data to a node that will build a web graphic to examine how frequently (and for which diagnostic codes) each provider filed claims for out-of-county services. This information might prove useful further along in our analysis.

In this step, we model the total charges on an insurance claim, using the admissions source, length of stay and diagnostic codes as inputs. We chose a modeling procedure called rule induction because it is easy to understand. When we insert the model into the stream, the model will read the inputs (admissions source, length of stay and diagnostic code) for each record, and then produce a projected value for total charges. We'll use this new value later on.

To examine the difference between the actual charges recorded on each insurance claim and the charges that our model projected, we will graph one against the other in a plot graphic. As part of the graphic, we could add a graph of the line. If the actual charges equal the projected charges on a particular record, that records point should fall on this line. On the other hand, if the record's actual charges were greater than the model projected, its point would be above this line.

To further drill down on the differences between actual and projected charges, we derive a new variable to add to our data. This new variable, "miss," is then graphed in a histogram. It shows that the majority of records in our data had a miss value clustered very close to $0. However, few records have a miss value that extends to $10,000 and beyond. Now we can narrow our attention to only those latter records.

Suppose that two providers had disproportionately high claims values. Exploring the types of claims submitted might uncover very suspicious activity for one of the claimants. They filed claims exclusively for one diagnostic code. The business analyst can easily identify this highly suspicious behavior and investigate the claims. Data mining proved useful for two reasons. First, it yielded valuable information about potential cases of fraud in the records currently on file. Although by no means an open-and-shut case of fraudulent claims submittal, the evidence we gathered can now be passed to investigators.

Plus, the model we built can be applied to future claims. The model will compute total projected charges on incoming claims. These projections can be compared against actual charges, and the system will "flag" questionable claims for investigation. With the information uncovered through data mining, adjusters can focus on claims that may yield larger adjustments, and are less likely to waste time investigating legitimate claims. With data mining, your adjusters can focus on recovering money so your organization's bottom line is less affected by fraud.

And, because circumstances change over time, you can periodically review the models and update them so they continue to be effective and deliver the best results. Modeler is the only data mining product that empowers organizations to continually modify the data mining process to keep decision makers updated.

Once you have models that predict fraudulent activity, you need to strategically deploy your results to the people who can use that information to eradicate fraud and recoup money. Strategic deployment means integrating models into your company's daily operations. Strategic deployment empowers you to put timely, consistent information into the right hands. Everyone in your organization is on the same page and can act more quickly to recoup the most money for your organization.[4]

D. Data Mining and Intrusion Detection

Intrusion detection is the process of analyzing and monitoring the events on a computer system to detect any security breaches that would compromises the availability, confidentiality or integrity of data [25]. Although many intrusion prevention techniques have been implemented, such as firewalls, authentication and encryption, these methods are not sufficient any more due to the increased complexity of systems and the increased possibilities for system vulnerabilities and weaknesses [22]. Therefore, a variety of

data mining techniques can be implemented for Intrusion Detection Systems (IDSs) [28].

Intrusion Detection Systems:

An intrusion detection system (IDS) can be host-based to analyze operating system audit trails, system logs or application logs. Another type of IDSs is the network-based IDS, which will be the focus in this paper. Network-based IDSs analyze network packets that are captured in a network. [23] [25].

Intrusion Detection Techniques:

As with telecommunication fraud detection, intrusion detection has two types [30]:

The first type is called Misuse Detection. This method depends on searching and tracing will known patterns of attacks or intrusion such as more than three consecutive failed logins within 2 minutes in a penetration attempt. Therefore, it is efficient for identifying attacks that leave characteristic traces which can be repeated by general pattern matching models [24].

The second method is Anomaly Detection. In this method, models of the normal user behavior to identify significant deviations in the new behaviors; for example, monitoring the CPU usage and the frequency of system commands [24]. Those models are called "user profiles" and they enable the detection of unknown attacks [23].

In general, data mining can be implemented in IDSs in one or more of the following techniques:

- Data summarization which included using statistics and identifying outliers.
- Visualization of graphical summaries of data.
- Clustering the data in to natural categories.
- Association rule discovery by defining normal activities to discover anomalies.
- Classification by predicting the category to which a record belongs [12].

V. CASE STUDY

In 1999, Riyadh Bank's customers were outraged when most of their accounts were hacked and in this mess their money was stolen. Since the establishment of Riyadh Bank, they have never faced such danger as in 1999. They came close to losing all of its customers and eventually close down their business permanently. Later that year Mohammad Rabea, first deputy chairman of the bank, released a statement that an investigation is under going for the multiple credit card fraud that happened to their users. Interview was done with the customers whose accounts were stolen from and they were asked to give a detailed transaction of their spending going back to 6 months. They felt that Riyadh Bank let down their promise by providing a safe environment for their customers. By the year 2001, Riyadh Bank was hopeless in finding the culprits and offered its customers a new account and with identification information. It was not until the year 2002 that the fraud problem was solved. Once again Mohammad Rabea released a statement saying that the company did an instinctive research as to see how their customers got caught up in these frauds. They later found out an analysis that is most commonly used nowadays in America, Break-point Analysis. The employees monitored their customers' recent spending transaction with previous spending behaviors. With the help of this analysis, Riyadh Bank was able to put a stop on the credit card epidemic that has awakened on its customers. Nowadays, Riyadh Bank follows the Break-point analysis in all of their customers to see their behavior spending level [9].

VI. CONCLUSION

Fraud remains a challenge for businesses and organizations in many fields. Data mining is an effective method for detecting various types of fraud including mobile telecommunication, credit card and medical insurance fraud as well as detecting intrusion to computer systems. This research paper has presented only a selection of the various data mining fraud detection techniques used in different fields. Some of those techniques have persisted and proven to be successful, while others are in the process of development and enhancement to better apply to new fraudulent acts. After all, it is not the organization alone who suffers from the consequences of fraud, but all the individuals and stakeholders related to that organization will be victims. Therefore, organizations are entirely accountable for learning the best practices and choosing the best method that matches their needs in order to safeguard against fraud.

REFERENCES

[1] D. A. Montague, *Fraud Prevention Techniques for Credit Card Fraud*. NY, New York: Spring-field Press, 2006.

[2] B. Thuraisingham, L. Khan, M. Awad, and L. Wang, *Design and Implementation of Data Mining Tools*. Florida, USA: Auerbach Publication, 2009

[3] M. Jans, N. Lybaert, and K. Vanhoof. (2009). [Online]. Available: http://docs.google.com/viewer?a=v&q=cache:lsCwIlYLA4oJ:doclib.uhasselt.be/dspace/bitstream/1942/7886/1/paperMilwaukee.pdf+Jans,+Lybaert,+%26+Vanhoof&hl=en&pid=bl&srcid=ADGEESgxbL9laTb1m4fqaU5ArvUDkBuBVT7QEoG8OFmd7K9vETepM8wj4zdUurdcT4z90-dTRtnK4wKlRVe1eNliIdMaVdIWmoev1WKsgaD-GxpDf-JIH3P1UeXc9VDxk9c6arqnSocA&sig=AHIEtbTRZoDo3JS60McQOP8jJa7IPUg4tw

[4] IBM Company. (2010). [Online]. Available: http://docs.google.com/viewer?a=v&q=cache:YTQJ9JBiyt0J:www.spss.com/media/whitepapers/IMW14283-USEN-00lr.pdf+data+mining+techniques+in+medical+insurance+fraud&hl=en&pid=bl&srcid=ADGEESi4QOg175AQbtEi3fJHcKEbOP053CHLdNSslW5MS7BTTwc0M_CyS5S7IT1rWuAEFhnu-2OYeIUoNPmh78abJoqj6rsc6eRfLJ51_LOEavxvmyBTSbXnFTMsw4Ec6q85NyZaeJDO&sig=AHIEtbS3bpz118ncxWEo3SNFOGWEF0fIyw

[5] D. Weston, N. Adams, D. Hand, C. Whitrow, and P. Juszczak, *Plastic Card Fraud Detection using Peer Group Analysis. Sydney, Australia: Marchel Publication, 2007.*

[6] H. Chye Koh and G. Gervais. (2008). [Online]. Available: http://webcache.googleusercontent.com/search?q=cache:x1l_zxwLIXIJ:bai-conference.org/files/BAI2010%2520Proceeding/Papers/8.Others/8090.doc+data+mining+techniques+in+medical+insurance+fraud&cd=5&hl=en&ct=clnk

[7] A. Abelovszky, *Plastic Card Fraud and Safety Measure*. London, England: National Press, 2008.

[8]M. T. Biegelman, *Identity Theft: Data Mining Detection, Prevention and Security*. Toronto, Canada: Wiley, 2008.

[9] Identity Theft in Riyadh. (1999). [Article]. Available: http://www.alriyadh.com/2006/11/20/section.econ.html

[10] R. Nisbet, J. Elder, J. F. Elder, G. Miner, *Hnadbook of Statistical Analysis and Data Mining Applications*. London: Academic Press, 2009.

[11] W. S. Albrecht, C.C. Albercht, C. O. Albrecht, and M. Zimbelman, *Fraud Examination*, 3rd ed. . Mason, USA: South-Western Cengage Learning, 2009.

[12] T. Lappas, and K. Pelechrinis, *Data Mining Techniques for (Network) Intrusion Detection Systems.* Department of Computer Science and Engineering.

[13] *Results of Worldwide Telecom Fraud Survey.* NJ: Communication Fraud Control Association (CFCA), 2009.

[14] G. M. Weiss, *Data Mining in the Telecommunications Industry*, IGI Global, pp. 486-491, 2009.

[15] P. G. Ferreira, R. Alves, O. Belo, and J. Ribeiro, *Detecting Telecommunications Fraud Based on Signature Clustering. Business Intelligence Workshop of 13th Portugese Conference on Artificial Intelligence, EPIA '07.* Braga: University of Minho, Department of Informatics, Campus of Gualtar, 2007.

[16] C. Cortes, and D. Pregibon, *Signature-Based Methods for Data Streams, pp. 167-182, 2001*.

[17] C. Phua, V. Lee, K. Smith-Miles, and R. Gayler, *A Comprehensive of Data Mining-based Fraud Detection Research.* Australia: Clayton School of Information Technology, Monash, 2005.

[18] P. Perner, *Advances in Data Mining: Applications in Medicine, Web Mining, Marketing, Image and Signal Mining, 6th ed.* . Leipzig, Germany: Springer, 2006.

[19] Fawcett, T. and F. Provost (1997). Adaptive fraud detection. *Data Mining and Knowledge Discovery 1* (3), 291-316.

[20]B. Kuşaksızoğlu, *Fraud Detection in Mobile Communication Networks using Data Mining.* The University of Bahcesehir, 2006.

[21] P. Ferreira, R. Alves, O. Belo, and L. Cortesao, *Establishing Fraud Detection Patterns Based on Signatures*, pp.526-538. Leipzig, Germany: University of Minho, 2006.

[22] W. Lee, S. J. Stolfo, and K. W. Mok, *A Data Mining Framework for Building Intrusion Detection Models. IEEE Symposium on Security and Privacy*, pp.120-132. New York: IEEE Symposium on Security and Privacy, 1999.

[23] K. Julisch, *Data Mining for Intrusion Detection: A Critical Review*. Zurich: IBM Research, Zurich Research Laboratory, 2007.

[24] W. Lee, and S. J. Stolfo, *Adaptive Intrusion Detection: A Data Mining Approach. Artificial Intelligence Review.* New York: Kluwer Academic Publishers, 2000.

[25] R. G. Bace, *Intrusion Detection.* Indianapolis: Macmillan Technical Publishing, 2000.

[26] J. Boltan, and J. Hand, *Profiling Methods for Fraud Detection.* Imperial London College, 2009.

[27] C. C. Phua, *Investigative Data Mining in Fraud Detection.* Monash University, 2003.

[28] W. Lee, and S. J. Stolfo, *Data Mining Approaches for Intrusion Detection. New York: Computer Science Department, Columbia University.*

[29] P. Barson, and R. Frank, *Fraud Auditing and Forensic Accounting, 2ed.* . John Wiley & Sons, 1998

[30] Bolton, R. and D. Hand, *Statistical fraud detection: A review*. *Statistical Science 17 (3)*,pp. 235-255, 2002.

[31] Cahill, M., D. Lambert, J. Pinheiro, and D. Sun (2000). Detecting fraud in the real world. Cortes, C., D. Pregibon, and C. Volinsky (2002). Communities of interest. *Intelligent Data Analysis 6*, 211-219.

[32] Cox, K., S. Eick, and G. Wills (1997). Visual data mining: Recognizing telephone calling fraud. *Data Mining and Knowledge Discovery 1*, 225-231.

[33] C. Held, and C. Perez (2006). Subscription fraud prevention in telecommunications using fuzzy rules and neural networks. *Expert Systems with Applications 31*, 337-344.

[34] Fanning, K. and K. Cogger (1998). Neural network detection of management fraud using published financial data. *International Journal of Intelligent Systems in Accounting, Finance & Management 7*, 21-41.

[35] Fawcett, T. and F. Provost (1999). Activity monitoring: Noticing interesting changes in behavior. In Chaudhuri and Madigan (Eds.),

Proceedings on the Fifth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Diego, CA, pp. 53-62.

[36] Green, B. and J. Choi (1997, Spring). Assessing the risk of management fraud through neural network technology. *Auditing 16* (1).

[37] A. Berson, S. Smith, and K. Thearling. An Overview of Data Mining Techniques. [Online].

http://www.thearling.com/text/dmtechniques/dmtechniques.htm

[38] Abidogun, Olusola A. "Data Mining, Fraud Detection and Mobile Telecommunications: Call Pattern Analysis with Unsupervised Neural Networks." 2005.