Data Mining Tools To Detect Financial Fraud

Renu Chaudhary
Punjab Technical University,
Department of Computer Science, Chandigarh Engineering College,
Landran 140307, Chandigarh, Punjab , India

Abstract

Every day, news of financial statement fraud is adversely affecting the economy worldwide. Considering the influence of the loss incurred due to fraud, effective measures and methods should be employed for prevention and detection of financial statement fraud**.** I synthesize academic literature related to fraudulent financial reporting with dual purposes: (1) to better understand the nature and extent of the existing literature on financial reporting fraud, and (2) to highlight areas where there is need for future research. I review publications in accounting and related disciplines including criminology, ethics, finance, organizational behavior accepted for publication. Data mining techniques has been proved the most commonly used techniques for prevention and detection of financial frauds. The implementation of data mining techniques for fraud detection follows the traditional information flow of data mining, which begins with feature selection followed by representation, data collection and management, pre - processing, data mining, post-processing, and performance evaluation.

Keywords: Fraud, auditing, literature review, fraud deterrence, fraud prevention and detection.

1. Introduction

With the advent of fast moving information technology everybody wishes to keep his information in the public domain i.e. either on internet or on intranet. We usually ignore the security threats and important network safety concerns with the informative data transmitted through the web. In the last two years many cases of credit card thefts have been reported to the cyber security department in London. A business consulting firm KPMG in its recent survey on cyber crime reported that FTSE 350 companies pose a huge risk of getting their databases hacked from unethical hackers .We all use internet banking and credit card for online shopping. It is possible for someone standing a meter away to note your password without your knowledge. There are several solutions available in the market to ensure your cyber safety. An internet user must be cautious about his private security from any cyber offense, scam and personal identity theft. We should be cautious of any small transaction done through our card. On a daily basis insurance providers mine through vast repositories of data to validate and process thousands of claims.

Yet, billions of dollars are lost annually because of fraudulent insurance claims. In order to provide quality services to their customers, providers need to recover this lost money. Preventing fraud requires mining and analyzing massive volumes of data to gain better insights and, in turn, improve decision-making ability.

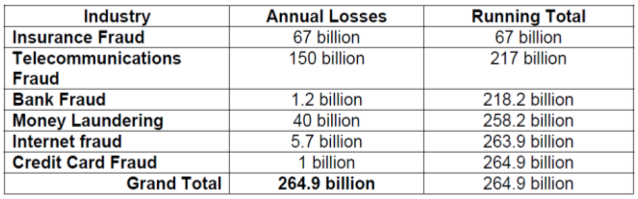
According to a recent survey by FICO and Property Casualty Insurers Association of America (PCI), 45 percent of insurers estimated that insurance fraud costs represent 5 to 10 percent of their claims volume, while 32 percent said the ratio is as high as 20 percent. More than half (54 percent) of insurers expect to see an increase in the cost of fraud.

Now let’s evaluate some of the challenges that persist and the changing insurance landscape that is driving innovative solutions and approaches.

Challenges include:

- Information overload and the rise in the number of security threats and frauds.
- Technological limitations that make it challenging to process and analyze data in a timely manner.
- Information silos, disparate systems and departmental processes that create information leakages.
- Evolving demand to keep up with changing compliance and regulations requirements.
- Lack of skilled resources to investigate and address fraudulent activities.

Below is the table showing the estimate of the cross industry loses annually :



Industry	Annual Losses	Running Total
Insurance Fraud	67 billion	67 billion
Telecommunications Fraud	150 billion	217 billion
Bank Fraud	1.2 billion	218.2 billion
Money Laundering	40 billion	258.2 billion
Internet fraud	5.7 billion	263.9 billion
Credit Card Fraud	1 billion	264.9 billion
Grand Total	**264.9 billion**	264.9 billion

Fig. 1 Cross Industry Fraud Losses estimates.

An example of fraud as economic externality involves an Internet travel agent in September 2011. It seemed that their web site was being used fraudulently to book air travel. Their chief legal officer indicated that it was not their place to fix society's problems; they just needed to reduce their losses to a tolerable "cost of doing business." This same company utilized a processing system that displayed their customers' travel and payment information in such a way that employees could access it and use it to facilitate illegal activity. However, since the losses resulting from this activity were external to the travel company and it was deemed "not worth our investment" to remedy the situation according to Wesley Kenneth Wilhelm **(**Spring 2004**).**

In fact, many companies subscribe to the philosophy of fraud prevention as a "competitive advantage" where they gauge part of their success by how much fraud they can push off on their competitors. This can be described as a "not in my backyard" approach. These companies typically are unwilling to discuss or share their fraud management methods with their competitors. Fast action can make fraudsters go elsewhere. This forced migration is a core component for those companies which treat fraud management as a competitive advantage. Their focus is one of implementing strategies before their competitors, so the fraudsters will go to their competitors to commit the fraud.

2. Data Mining: A Proven Way to Increase Fraud Detection

It's difficult to detect and prevent fraud. Fraudsters develop new schemes all the time, and those schemes grow more and more sophisticated to elude easy detection. According to The Association of Certified Fraud Examiners' "2010 Report to the Nations on Occupational Fraud and Abuse," the top two methods of fraud detection are tips (40.2 percent) and management review (15.4 percent). If 15.4 percent seems low, it is; many organizations simply don't conduct the appropriate testing to proactively detect fraudulent activity. By employing data mining techniques, however, organizations can significantly increase their detection of fraud and, as a result, deter fraudsters.

2.1 Why Data Mining?

Data mining is the process of extracting patterns from data. It uses sophisticated data search capabilities and statistical algorithms to unearth patterns and correlations and can be useful in a variety of applications, including fraud detection. Data mining can help your organization find anomalies and spot internal control weaknesses, including inconsistent data, unusual transactions, duplicate payments, missing invoices, deviant transactions/vendors, and procurement and disbursement frauds.

2.2 What Does It Entail?

It depends upon the organization. Companies in the manufacturing industry will employ a series of tests different from those in the service industry. In fact, even companies within one particular industry will likely not use the same tests, as different organizations have distinct risk areas. What data mining does afford all organizations is the ability to test all data within specified parameters simultaneously. Traditionally, testing for anomalies is done via sample; this only affords a partial picture of potential fraudulent activity. Data mining includes all data—and, therefore, paints a more complete picture of an organization.

2.3 Here Are Some Examples?

Following are a few examples of tests organizations can conduct to gauge fraudulent activity. Keep in mind, however, that there are multiple tests from which to choose, depending upon an organization's high risk areas.

Cash Receipts: Review customers with credit balances. While these may be legitimate — returns, honest oversights — they could be a sign that something's amiss. How old are the receipts? Who's attending to them? Are the "customers" associated with the credits valid?

Cash Disbursements: Review payments made on non-business (i.e., vacation) days. If the accounts payable clerk is supposed to be on vacation on a Monday, yet it appears transactions occurred that only they handle, it's a serious red flag that fraud may be occurring.

Vendor Testing: Look for duplicate invoice numbers by vendor. If a vendor exists with a duplicate invoice number, that invoice has likely already been paid. Keep in mind that fraudsters often try to work around this problem by slightly modifying the vendor number (instead of using MS001, they might use MS001. or MS001a). This is easy to track and discover.

Payroll: Take a close look at employees with matching information (addresses, direct deposit accounts, etc.). Usually, the only time this should occur is if a married couple or relatives are employed at the organization. Be sure to verify that no two employees have matching social security numbers as well. Improved fraud detection thus has become essential to maintain the viability of the US payment system. Banks have used early fraud warning systems for some years. Large scale data-mining techniques can improve the state of the art in commercial practice. Scalable techniques to analyze massive amounts of transaction data that efficiently compute fraud detectors in a timely manner is an important problem, especially for e-commerce. Besides scalability and efficiency, the fraud-detection task exhibits technical problems that include skewed distributions of training data and non-uniform cost per error, both of which have not been widely studied in the knowledge-discovery and data mining community.

3. Detection of fraud

3.1 How Do I Get Started?

First, identify which tests are appropriate for your industry as well as your organization. For example, certain companies may want to employ the majority of tests focusing on vendors and inventory while other companies may be more inclined toward payroll tests. Certain tests can be run using Microsoft Access or Excel; others may require more complex data mining software. Once the tests are complete, the next stage is interpreting the results; it’s just as important to know how to analyze the data as it is to obtain it in the first place. Results may lead to a number of possibilities, including beginning a fraud investigation or adjusting internal controls. The good news is that once data analysis plans are established, reports can be run quickly and routinely. Care must be taken to ensure that the tests you put in place continue to address a company’s high risk areas, which will evolve as the business grows and changes.

Fraud deterrence is based on the premise that fraud is not a random occurrence; fraud occurs where the conditions are right for it to occur. Fraud deterrence attacks the root causes and enablers of fraud; this analysis could reveal potential fraud opportunities in the process, but is performed on the premise that improving organizational procedures to reduce or eliminate the causal factors of fraud is the single best defense against fraud. Fraud deterrence involves both short term (procedural) and long term (cultural) initiatives. Fraud detection involves a review of historical transactions to identify indicators of a non-conforming transaction , looking at what could happen in the future given the process definitions in place, and the people operating that process

4. Deterrence of fraud:

Deterrence involves eliminating factors that may cause fraud.

4.1 Fraud Triangle

The causal factors that should be removed to deter fraud (as described above) are best described in the “Fraud Triangle.” This idea was first coined by Donald R. Cressey. The Fraud Triangle describes three factors that are present in every situation of fraud:

1. Motive (or pressure) – the need for committing fraud (need for money, etc.);
2. Rationalization – the mindset of the fraudster that justifies them to commit fraud; and
3. Opportunity – the situation that enables fraud to occur (often when internal controls are weak or nonexistent).

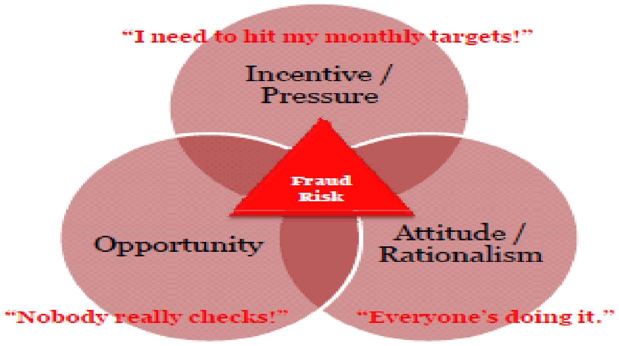


Fig. 2 Fraud Triangle

4.1.1 Breaking the Fraud Triangle

Breaking the Fraud Triangle is the key to fraud deterrence. Breaking the Fraud Triangle implies that an organization must remove one of the elements in the fraud triangle in order to reduce the likelihood of fraudulent activities. “Of the three elements, removal of Opportunity is most directly affected by the system of internal controls and generally provides the most actionable route to deterrence of fraud".

5. Fraud detection by Data Mining

Fraud is a million-dollar business and it is increasing every year. Fraud involves one or more persons who intentionally act secretly to deprive another of something of value, for their own benefit. Fraud is as old as humanity itself and can take an unlimited variety of different forms. However, in recent years, the development of new technologies has also provided further ways in which criminals may commit fraud. In addition to that, business reengineering, reorganization or downsizing may weaken or eliminate control, while new information systems may present additional opportunities to commit fraud.

❖ Credit Card Fraud is one of the biggest threats to business establishments today. Credit card transactions continue to grow in number, taking an ever-larger share of the US payment system and leading to a higher rate of stolen account numbers and subsequent losses by banks.

Goals of fraud detection:

✔High efficient technique,

✔Data are highly skewed

✔ choose Cost-based techniques

❖ **Black box fraud detection**

JAM (Java agents for Meta Learning)

❖ **Meta-Learning**

● Apply to the area of Data miming

● Combine the prediction from multiple models

✔ Reduce the cost of fraud through timely

✔ Minimize the losses by catching fraud more rapidly

✔ Minimize Costs associated with false alarms

JAM

Two Techniques with JAM are:

● Local fraud Detection agents to learn how to detect fraud

● Secure, integrated meta-detection system to view the network transaction

Experiment and Results

learning algorithms:

-C4.5
-CART
-RIPPER
-BAYES
-Mining the analog Data

Results

The neuronal network experts for analog Data. Diagnosis sequence data ideas ;

❖ First, there can be the typical fraud sequences, for instance the behavior of a thief after copying or picking the credit card.

➢ Second, there can be a typical behavior of the user which it does not correspond to the actual transaction sequence may indicate a credit card misuse.

Combining analog and symbolic Information time

Fraud y/n

➢ Combining with Sequential

➢ Ada Cost Algo

➢ Used internal heuristics based upon training accuracy

➢ Learning Algorithm to predict fraud.

➢ Employs internal metrics of misclassification cost.

5.1 Application: How is data mining applied in practice?

Many companies use data mining today, but refuse to talk about it. In direct marketing, data mining is used for targeting people who are most likely to buy certain products and services.

In **trend analysis**, it is used to determine trends in the marketplace, for example, to model the stock market.

In **fraud detection**, data mining is used to identify insurance claims, cellular phone calls and credit card purchases that are most likely to be fraudulent.

Other than these there are many other application areas.

Application areas are-

➢ Banking: loan/credit card approval:

Predict good customers based on old customers

➢ Customer relationship management:

Identify those who are likely to leave for a competitor.

➢ Targeted marketing:

Identify likely responders to promotions

➢ Telecommunications, financial transactions from an online stream of event identify fraudulent events

- Manufacturing and production:
  Automatically adjust knobs when process parameter changes
- Medicine: disease outcome, effectiveness of treatments
  Analyze patient disease history: find relationship between diseases
- Molecular/Pharmaceutical:
  Identify new drugs
- Scientific data analysis:
  Identify new galaxies by searching for sub clusters
- Web site/store design and promotion:

Fraud detection is continuously evolving discipline and requires a tool that is intelligent enough to adapt to criminal strategies and ever changing statics to commit fraud. With the relatively recent growth of the internet in the global economic force, credit card fraud has become more prevalent.

6. Detecting fraud

Research on fraud detection has been foccused on pattern matching in which abnormal patterns are identified from the normality.

Techniques used for fraud detection fall into two primary classes: **statistical techniques** and **artificial intelligence.**

Examples of **statistical data analysis techniques** are:

- Data preprocessing techniques for detection, validation, error correction, and filling up of missing or incorrect data.

- Calculation of various statistical parameters such as averages, quantiles, performance metrics, probability distributions, and so on. For example, the averages may include average length of call, average number of calls per month and average delays in bill payment.

- Models and probability distributions of various business activities either in terms of various parameters or probability distributions.

- Computing user profiles.

- Time-series analysis of time-dependent data.

- Clustering and classification to find patterns and associations among groups of data.

- Matching algorithms to detect anomalies in the behavior of transactions or users as compared to previously known models and profiles. Techniques are also needed to eliminate false alarms, estimate risks, and predict future of current transactions or users.

Fraud management is a knowledge-intensive activity. The main **AI techniques** used for fraud management include:

- Data mining to classify, cluster, and segment the data and automatically find associations and rules in the data that may signify interesting patterns, including those related to fraud.

- Expert systems to encode expertise for detecting fraud in the form of rules.

- Pattern recognition to detect approximate classes, clusters, or patterns of suspicious behavior either automatically (unsupervised) or to match given inputs.

- Machine learning techniques to automatically identify characteristics of fraud.

- Neural networks that can learn suspicious patterns from samples and used later to detect them.

Artificial Intelligence technique for credit card fraud detection:

The major functionalities of the artificial neural network (ANN) based credit card detection system designed are as follows: to facilitate real-time transaction entry, and react to a suspicious transaction that may lead to fraud. The design of the architecture is based on a neural network unsupervised method, which was applied to the transactions data to generate four clusters: the low, high, risky and high-risk clusters.
The system runs secretly beneath the banking software within banks offering credit card services where fraudulent transactions are observed. Business rules relevant to the enlisted CCF types are further applied to the four clusters to detect transactions that deviate from the norm. Deviation from the usual pattern of an entity implies the existence of a fraud. Each transaction entering the database such as withdrawal, deposit, and any card transaction is treated as a signature, suspected and prone for verification.
The similarity between a customer’s present transaction and a known fraud scenario indicates the same fraud may occur again. Suspected transactions are flagged within seconds for further investigations and subsequent decision-

making. Visualization is provided using appropriate graphical user interface (GUI).

Other techniques such as link analysis, Bayesian networks, decision theory, land sequence matching are also used for fraud detection.

Some of the Detector Constructor Framework called DC-1 proposed by Fawcett and Provost [9] for telephone call fraud detection, Instruction Detection Framework and algorithms for pattern comparison proposed by Lee et al. Doronsoro et al.[5] described the operational system for fraud detection of credit card operations based on neural classifier; Aleskerov et al. [21] presented a neural network based data mining system for credit card detection and tested it on synthetically generated data; and Chan and Stolfo [5] addressed the question of non-uniform class distributions in credit card fraud detection. Haimowitz and Schwarz [20] presented a framework for credit customer optimization based on clustering and prediction. has introduced a hierarchical off-line anomaly network intrusion detection system based on Distributed Time-Delay Artificial Neural Network.

6.1 Credit Card fraud detection

You don't need a gun to rob a bank any more. Now a bank robber's most powerful weapon is a computer and an internet connection. As internet trading increases, so does the threat of organized and automated fraud. No longer does the fraudster need to be present or make a phone call to commit a crime.

To reduce the risks, banks themselves are using more sophisticated technologies. For example: The Royal Bank of Scotland (RBS), has signed up to a peer-to-peer fraud-reduction network from Ethoca.

6.1.1 Methodology

The credit card fraud detection system developed used four clusters of low, high, risky and high risk as shown in Fig.1. Once the transaction is legitimate, it was processed but if any transaction falls into any of these clusters; it was labeled as suspicious/fraudulent. The alert goes off and the reason is given. The fraudulent transaction will not be processed but will be committed to the database.

Credit card fraud detection model mainly consists of four stages as shown in the figure below:-

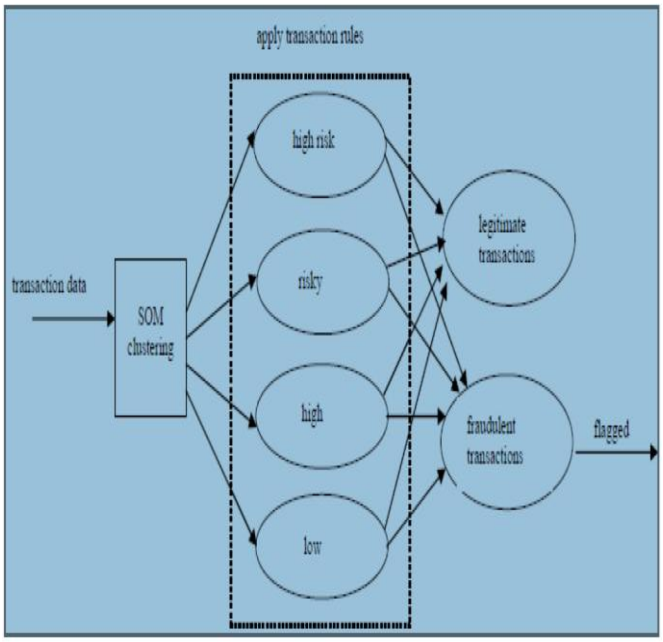


Fig. 3. A Four-Stage Credit Card Fraud Detection Model

Things to Know About Detecting Credit Card Fraud :-

Fraud can quickly be detected with a computer by tracking usage patterns and history. Let us take an example of IBM. IBM has solutions to help. Here are 5 things to know about IBM fraud detection solutions.

1. Companies get ripped off by billions of dollars each year due to fraud.

In the U.S., 32 percent of consumers reported card fraud in the past fiv e years. Some of the schemes use very complex technology, while others simply rely on the trust of the purchaser. Both consumers and banks are very interested in minimizing these losses.

2. The top 25 world banks run their businesses on mainframes.

In fact, 71% of Fortune 500 banks use mainframes. These facts are seldom publicized, but should be no surprise. IBM System z mainframes have experienced nearly 50 years of improved hardware, software, and procedures, making them reliable and quite foolproof. You don’t often (if ever) hear of someone hacking a mainframe.

3. The ideal solution avoids making fraudulent payments without slowing down legitimate payments.

Such a solution requires the adoption of a comprehensive fraud business architecture that applies advanced predictive analytics to reduce fraud, waste, and abuse, by using some techniques.

The techniques are:

- Identify vulnerabilities
- Detect transactions
- Evaluate workloads
- Conduct remediation
- Process appeals

Some fraud analysis and scoring models are supported by such familiar products as System z, the DB2 Analytics Accelerator (IDAA), DB2 for z/OS, and SPSS. New functions in DB2 for zOS and SPSS Modeler allow the solution to be run in close proximity to the vast amounts of historical data that is on System z. This allows the scoring of a payment to be made directly within DB2. Figure 4 shows the layout and flow of this solution.

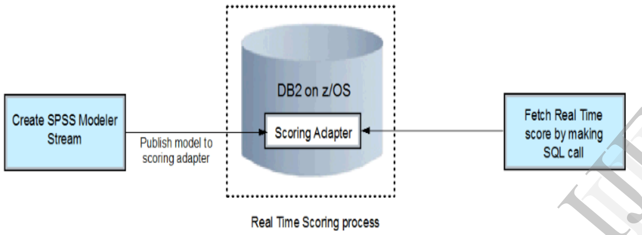

Create SPSS Modeler Stream
Publish model to scoring adapter
DB2 on z/OS
Scoring Adapter
Fetch Real Time score by making SQL call
Real Time Scoring process

Fig. 4. Real-time fraud detection solution on System x

4. SPSS scoring adapter that runs in DB2.

The scoring process uses live transaction data as the input and produces real-time results. Figure 5 shows a sample SPSS Modeler stream that gets published to the scoring adapter.

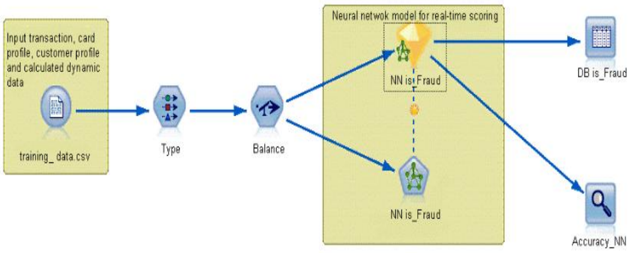

Input transaction, card profile, customer profile and calculated dynamic data
training_ data.csv
Type
Balance
Neural netwok model for real-time scoring
NN is Fraud
NN is_Fraud
DB is_Fraud
Accuracy_NN

Fig. 5. *The* SPSS scoring adapter in DB2 is the heart of the solution

The brains behind predicting scoring ratings is a user-written SPSS model**.**

For a typical transactional fraud detection business case, assume that a customer is making a credit card payment. At the time of payment, the bank analyzes the payment pattern on that particular credit card to detect the possibility of fraud. This analysis involves the history, frequency, and dollar amounts of previous transactions for that credit card from its database records. Depending on the scoring analysis, the bank authorizes the transaction, keeps it on hold, or declines it, all in real time.

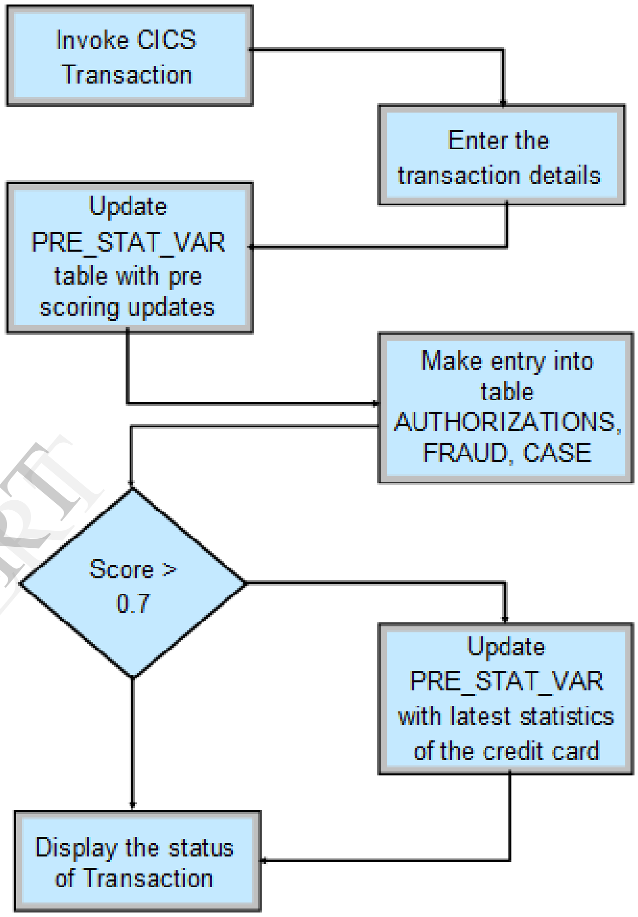

Invoke CICS Transaction
Enter the transaction details
Update PRE_STAT_VAR table with pre scoring updates
Make entry into table AUTHORIZATIONS, FRAUD, CASE
Score > 0.7
Update PRE_STAT_VAR with latest statistics of the credit card
Display the status of Transaction

Fig. 6. The SPSS model is the brains of the solution.

7. Steps for Data Mining Approach:

The data mining approach involves the following steps: The steps select an appropriate algorithm; implement the algorithm in software; test the algorithm with known data set; evaluate and refine the algorithm as it is being tested with other known data sets; and show the results.

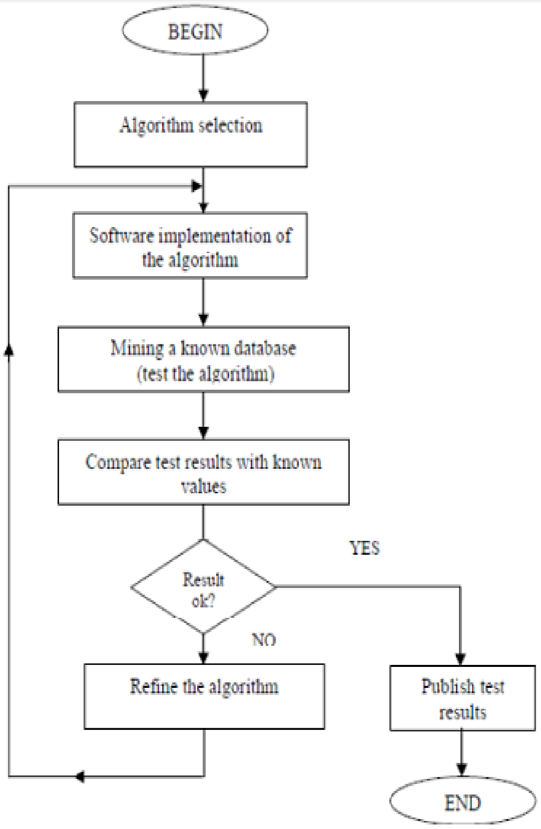

BEGIN
Algorithm selection
Software implementation of the algorithm
Mining a known database (test the algorithm)
Compare test results with known values
Result ok?
YES
NO
Refine the algorithm
Publish test results
END

Fig. 7. Steps Used in the Data Mining Approach.

Based on the algorithms selected and used, here is a table showing different algorithms implemented :

TABLE OF ALGORITHMS IMPLEMENTED:

Algorithm	IBM	ISL	SAS	TMC	Unica
Decision Trees	✓	✓	✓	✓	
Neural Networks	✓	✓	✓	✓	✓
Regression	1	✓	✓		✓
Radial Basis Functions	✓[2]				✓
Nearest Neighbor			✓	✓	✓
Nearest Mean					✓
Kohonen Self-Organizing Maps		✓	✓		
Clustering	✓	✓			✓
Association Rules	✓	✓			

The cost of occupational fraud — both financially and to an organization's reputation — can be acutely damaging. With nearly half of victim organizations unable to recover their losses, proactive measures to prevent fraud are critical. Management should continually assess the organization's specific fraud risks and evaluate its fraud prevention programs in light of those risks.

7. Conclusions

Overall this research work is helpful in understanding the existing use of data mining methods for prevention and detection of financial statement fraud, preventing financial statement fraud at the first place and detecting it in case of failure of prevention mechanism. It further helps in identifying financial variables responsible for fraud from publically available financial statements, suggesting data mining methods for prevention of fraudulent financial reporting and selecting a best data mining method for detection of fraud.

The nature and threat of occupational fraud is truly universal. Though my research noted some regional differences in the methods used to commit fraud — as well as organizational approaches to preventing and detecting it — many trends and characteristics are similar regardless of where the fraud occurred.

Providing individuals a means to report suspicious activity is a critical part of an anti-fraud program. Fraud reporting mechanisms, such as hotlines, should be set up to receive tips from both internal and external sources and should allow anonymity and confidentiality. Management should actively encourage employees to report suspicious activity, as well as enact and emphasize an anti-retaliation policy.

Targeted fraud awareness training for employees and managers is a critical component of a well-rounded program for preventing and detecting fraud. Not only are employee tips the most common way occupational fraud is detected, but my research shows organizations that have anti-fraud training programs for employees, managers and executives experience lower losses and shorter frauds than organizations without such programs in place. At a minimum, staff members should be educated regarding what actions constitute fraud, how fraud harms everyone in the organization and how to report questionable activity.

External audits should not be relied upon as an organization's primary fraud detection method. Such audits were the most commonly implemented control in our study; however, they detected only 3% of the frauds reported to us, and they ranked poorly in limiting fraud losses. While external audits serve an important purpose and can have a strong preventive effect on potential fraud, their usefulness as a means of uncovering fraud is limited.

This research continues to show that small businesses are particularly vulnerable to fraud. These organizations typically have fewer resources than their larger counterparts, which often translates to fewer and less-effective anti-fraud controls. In addition, because they have fewer resources, the losses experienced by small businesses tend to have a greater impact than they would in larger organizations. Managers and owners of small businesses should focus their anti-fraud efforts on the most cost-effective control mechanisms, such as hotlines, employee education and setting a proper ethical tone within the organization. Additionally, assessing the specific fraud schemes that pose the greatest threat to the business can help identify those areas that merit additional investment in targeted anti-fraud controls.

References

[1] Idris, J. (2009): Nigerian Auditors are Toothless Bulldogs. October 3. http://www.saharareporters.com/articles/external-contrib/3872-nigerias-bank-auditors-are-toothless-bull-dogs.html

[2] Ogwueleka, F. N.(2008). *Credit card fraud detection using data mining techniques*. Ph.D. Dissertation. Department of Computer Science. Nnamdi Azikiwe University, Awka, Nigeria.

[2] PricewaterhouseCoopers LLP (2009). "2009 Global Economic Crime Survey". Retrieved June 29, 2011. Bolton, R. & Hand, D. Statistical Fraud Detection: A Review .

[3] G.K. Palshikar, The Hidden Truth – Frauds and Their Control: A Critical Application for Business Intelligence, Intelligent Enterprise, vol. 5, no. 9, 28 May 2002, pp. 46–51.

[4] Nigrini, Mark (June, 2011). "Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations". Hoboken, NJ: John Wiley & Sons Inc. ISBN 978-0-470-89046-2.

[5] Distributed data mining in credit card fraud detection P. Chan, W. Fan, A. Prodromidis, and S. Stolfo IEEE Intelligent Systems, 14(6):67-74, 1999. JAM: Java Agents for Meta-learning over Distributed Databases
S.J. Stolfo, D. Fan, W. Lee, A. Prodromidis, P. Chan

(Cendrowski, Martin, Petro, The Handbook of Fraud Deterrence).

. http://www.twocrows.com/glossary.html

[6] Michalski, R. S., I. Bratko, and M. Kubat. Machine Learning and Data Mining – Methods and Applications. John Wiley & Sons Ltd.

[7] Green, B. & Choi, J. Assessing the Risk of Management Fraud through Neural Network Technology. Auditing 16(1): 14–28.

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

[9] Fawcett, T. AI Approaches to Fraud Detection and Risk Management: Papers from the AAAI Workshop.

[10] Feb 28, 2011 http://www.plantemoran.com

[11] Phua, C., Lee, V., Smith-Miles, K. and Gayler, R. (2005). A Comprehensive Survey of Data Mining-based Fraud Detection Research. Clayton School of Information Technology, Monash University.

[12] Cortes, C. & Pregibon, D. Signature-Based Methods for Data Streams. Data Mining and Knowledge Discovery 5: 167–182.

[13] Bolton, R. & Hand, D. (2001). Unsupervised Profiling Methods for Fraud Detection. Credit Scoring and Credit Control VII.

[14] Behaviour Mining for Fraud Detection Xu, Jianyun, Sung, Andrew H, Liu, Qingzhong, Journal of Research and Practice in Information Technology. Vol. 39, no. 1, pp. 3–18. Feb. 2007

[15] Burge, P. & Shawe-Taylor, J. An Unsupervised Neural, Network Approach to Profiling the Behaviour of Mobile Phone, Users for Use in Fraud Detection. Journal of Parallel and Distributed Computing 61: 915–925.

[16] Cox, K., Eick, S. & Wills, G. Visual Data Mining: Recognising Telephone Calling Fraud. Data Mining and Knowledge Discovery 1: 225–231.

[17] Murad U. & Pinkas, G. Unsupervised Profiling for Identifying Superimposed Fraud. Proc. of PKDD99.

[18] PricewaterhouseCoopers' Global economic crime survey 2007 finds at http://www.pwc.com/crimesurvey

[19] Marane, A., (2011) Utilizing Visual Analysis for Fraud Detection, Understanding Link Analysis, http://linkanalysisnow.com/2011/09/leveraging-visual-analytics-for.html

[20] Haimowitz, I.J.; and Schwarz, H. (1997). Clustering and prediction for credit line optimization. Proceedings of AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management, 29-33.

[21] Aleskerov, E.; Freisleben, B.; and Rao, B. (1997). CARDWATCH: A neural network-based database mining system for credit card fraud detection. Proceeding of the IEEE/IAFE on Computational Intelligence for Financial Engineering, 220-226

Author's Details:

Renu Chaudhary
Bachelor of Technology in 2011
Master of Technology in 2013 (undergoing thesis work)
A member of the IEEE Computer Society and C.S.I.

Current research interests: Integration of Data mining with Remote Sensing Technologies to advance Defence Capabilities, Neural Networks, Research in Artificial Intelligence and Robotics, Exploring new frontiers of Nano Technologies in developing Quantum Computing .