AN UPDATE RESEARCH ON CREDIT CARD ON-LINE TRANSACTIONS

Falaki S. O.
Alese B. K.
Department of Computer Science,
Federal University of Technology, Akure, Ondo State, Nigeria.

Ismaila W. O.
Department of Computer Science and Engineering
Ladoke Akintola University of Technology, Ogbomoso.
E-mail: ade_732001@yahoo.com

ABSTRACT

This paper aimed at comparing published technical and review articles on automated credit card and fraud detection within the last twenty-five years and its effect on the global economy. It formalised the types of credit card fraud and discussed extensively the issues of credit card online transactions. As a study that depended on secondary source of data collection, methodologies and techniques employed in credit card fraud and their performance evaluations were analysed using frequency count. However, unsupervised approaches from counter terrorism work, actual monitoring systems and spam detection communities can contribute to future fraud detection in credit card online transactions.
Keywords: *Data mining, Fraud detection, Machine learning, e-commerce, Credit cards.*

INTRODUCTION

E-commerce is not an entirely new type of commerce. It first emerged in the 1960's on private networks, as typically large organizations developed electronic data interchange (EDI) installations and banks implemented electronic funds transfer (EFT). The increasing use of Internet has seen the growth of e-payment for electronic funds transfers and transaction processing in e-commerce conducted between geographically distant parties (that is, consumers and merchants). This may take place when credit card is present at an Automated Teller Machine (ATM) or Point of Sales (POS), or when the card is not present, which covers cards used for mail order, telephone order and internet purchases.

Credit card is a system named after the small card issued to users of the system. A user is issued credit after an account has been approved by the credit provider, and is given, with which the user will be able to make purchase from merchants that are accepting that card up to a pre-established credit limit. Credit card transactions are processed through a chain of connected parties. The five primary parties involved in processing a credit card transaction are: cardholder, card issuer

(the bank that issues the credit card to the cardholder), merchant, acquirer (often a bank, processes transactions on behalf of the merchant), and card association (another term used to describe Visa and Master Card). A fraud is a deception made for personal gain or to damage another individual. The terms normal, non-fraud or legal and anomalous, fraud or illegal can be used interchangeably in this work. Some of the various kinds of frauds are; computer fraud, insurance fraud, internet auction fraud, investment scheme fraud, money laundering, medical fraud, telecommunication fraud, and credit card fraud. Credit card fraud is the act of making a purchase using someone else's credit card information. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. This can be perpetrated by individuals, merchants and also lack of security that can lead to the compromise of credit card numbers stored in online databases (computer intrusion).

Merchant fraud takes three basic forms: non delivery, overcharging, and charges for unwanted goods or services. Individual fraud include: (i) Lost and stolen card fraud: a card is physically stolen from your wallet or home, or it is lost, and is then used by a criminal, posing as you, to obtain goods and services. (ii) Counterfeit card fraud (counterfeit, cloned or skimmed card) is one that has been printed, embossed or encoded without permission from the card company, or one that has been validly issued and then altered or recoded. (iii) Card-not-present (CNP) fraud includes fraud conducted over the Internet, by telephone, fax and mail order. (iv) Application fraud is stolen or false documents used to open an account in one's name. (v) Account take-over is by obtaining key personal information, criminals are able to take over the running of one's account. The extent of credit card fraud is difficult to quantify, partly because companies are often loath to release fraud figures in case they frighten the spending public and partly because the figures change (probably grow) over time. The update statistics on the number of credit cards deployed across the world and their fraudulent levels as at 2008 was announced by APAC in March, 2009.

Anomaly detection has been the topic of a number of surveys and review articles, as well as books. For instance, Richard & Hand (2002) , Hodge and Austin [2004], Clifton et al (2004), Agyemang et al. (2006), Patcha and Park (2007) and Varun et al (2009) provided an extensive survey of anomaly detection techniques developed in research domains. However, Markou and Singh (2003a, b) and Varun et al (2009) emphasized more on intrusion detection. Clarke, M. (1990), Kou et al (2006) and Phua et al (2005) gave a detailed survey on fraud detection in insurance application domain. Gary M. in 2009 discussed on data mining in the telecommunications industry where he reviewed telecommunication fraud detections.

Thus, the main focus of this paper is to give a comprehensive up-to-date information on credit card online transactions which has been eluding the attention of many researchers, since its adverse effect on the people and the global economy has been on the increase day after days. Thus, this study attempts to provide a structured and a broad overview of extensive research on credit card fraud detection methods and techniques spanning multiple research areas.

Table 1 details the application areas where fraud occurs viz: insurance, management, credit card, and telecommunications, computer intrusion and financial crime; and the number of published articles on each area that are referenced by us and two previous researchers.

Table 1: Fraud types from 164 unique academic and published fraud detection papers.

Fraud Types	1	2	3	4
Management	12	4	7	-
Insurance	21	6	14	12
Credit transactions	28	9	17	6
Telecommunication	22	12	13	8
Computer Intrusion	69	12	18	58
Financial Crime	12	10	6	-

Note: Most of our reviewed literatures were referenced in the references in related work.

Source: 1- Our review, 2- Richard & Hand(2002), 3- Clifton , et al (2004), 4- Varun et al (2009)

However, because computer intrusion and credit transactional fraud detection has received the most attention from researchers couple with the fact that computer intrusion many a time leads to credit card fraud and the importance of credit cards in global business, this prompted us to focus and collate all the works that have been done only on credit card issues. Table 2 below revealed the published academic papers on credit card fraud detection for the past twenty-five years.

List of reviewed academic published articles on credit card fraud detections are stated as follows: Dheepa and Dhanapal, (2009), Whitrow, et al, (2009), Panigrahi and Sural (2009), Alonso Gadi, et al (2008), David (2007), Manoel et al (2007), Niall M. et al (2007), Vladimir and Strizhak (2006); Kundu Amlan et al (2006), Vatsa et al (2005) Jing He, et al, (2004), Peter, et al, (2000), Clifton et al, (2004), Richard and Hand, (2002) and Varun et al (2009). Most of the existing surveys on anomaly detection either focus on a particular application domain or on a single research area.

DATA PROCESSING IN CREDIT CARD

This section identifies and discusses the different issues that are relevant to the processing of credit card information in order to detect fraud. These issues includes factors such as the nature of the input data, the availability (or unavailability) of labels, the output reported by the detection systems.

Nature of Input Data: A key aspect of any anomaly detection technique is the nature of the input data. Input is generally a collection of data instances (also referred as object, record, point, vector, pattern, event, case, sample, observation, entity) (Tan et al. 2005). Each data instance can be described using a set of attributes (also referred to as variable, characteristic, feature, field, and dimension). The attributes can be of different types such as binary, categorical (nominal or ordinal scales e.g merchant code) or continuous (interval or ratio scales). Each data instance might consist of only one attribute (univariate) or multiple attributes (multivariate). In the

case of multivariate data instances, all attributes might be of same type or might be a mixture of different data types. Specific attributes in credit transaction data are often not revealed but they should comprise of date/time stamps, current transaction (amount, geographical location, merchant industry code and validity code), transactional history, payment history, and other account information. (Ghosh and Reilly, 1994)

Data Labels: The labels associated with a data instance denote if that instance is normal or anomalous, fraud or non-fraud, legal or illegal. It should be noted that obtaining labeled data which is accurate as well as representative of all types of behaviors, is often prohibitively expensive. Labeling is often done manually by a human expert and hence requires substantial effort to obtain the labeled training data set. Typically, getting a labeled set of anomalous data instances which cover all possible type of anomalous behavior is more difficult than getting labels for normal behavior. Moreover, the anomalous behavior is often dynamic in nature, e.g., new types of anomalies might arise, for which there is no labeled training data.

Output: An important aspect for any fraud detection technique is the manner in which the anomalies are reported. Typically, the outputs produced by fraud detection techniques are one of the following two types: (i) Scores: Scoring techniques assign a fraud score to each instance in the test data depending on the degree to which that instance is considered an anomaly. Thus the output of such techniques is a ranked list of anomalies. An analyst may choose to either analyze top few anomalies or use a cut-off threshold to select the anomalies. (ii) Labels: Techniques in this category assign a label (fraud or non-fraud) to each test instance. Scoring based fraud detection techniques allow the analyst to use a domain specific threshold to select the most relevant anomalies. Techniques that provide binary labels to the test instances do not directly allow the analysts to make such a choice, though this can be controlled indirectly through parameter choices within each technique.

There are two prominent methods of combating credit card fraud namely; prevention and detection. Fraud prevention describes measures to stop fraud from occurring in the first place. Fraud detection involves identifying fraud as quickly as possible once it has been perpetrated. Fraud detection comes into play once fraud prevention has failed. The two methods are discussed in details below:

CREDIT CARD FRAUD PREVENTION

Credit card processing on-line or card-not-present (keyed) merchants must take more precautions than merchants that process credit cards face-to-face, since they do not have the luxury of seeing the actual card or cardholder. With internet merchant account transactions, there are a number of potential fraud flags to look out for:

Unusual orders: Merchants have to be very vigilant in attending to some orders, for instance multiple orders placed on the same card in a short time period, "Next day" shipping or "Rush" orders, transactions placed on multiple cards but shipped to the

same address, shipping address differs from billing address, multiple orders with multiple cards for a single internet protocol address etc.

First time shopper: scammers are always looking for new sites that are "card able" and don't take fraud seriously.

Confirm bank details: If you are unsure of an order, call the credit card issuer and ask that they call their customer to confirm that it is an authorized use of the credit card.

Suspect shipping address: Orders from Ukraine, Indonesia, Yugoslavia, Lithuania, Egypt, Romania, Bulgaria, Nigeria, Turkey, Russia and Pakistan have a very high incidence of fraud, and often have unverifiable addresses.

Untraceable email address: In many fraudulent orders, the customer's email address is often at one of the free email services, like hotmail.com and yahoo.com, which are relatively untraceable.

Request Signature on Delivery: Not always possible, depending on what sort of business you are in.

Record Confirmed Fraudulent Orders: Fraudsters are notoriously persistent trying to place orders at the same sites, just because they didn't get through the first time certainly would not stop them trying their luck again and again. Ideally, your website will store the details of orders you have previously identified as fraudulent so that if someone tries to place another order with the same internet protocol address, credit card number, name or delivery address your website will automatically identify them.

Multiple items: It can be a bad sign, for example, if someone orders two Laptop computers or six DVD players at once, especially where the items have a high resale value.

STEPS TO REDUCE THE POTENTIAL FOR FRAUDULENT TRANSACTIONS

Here are some steps merchants can take to reduce the potential for fraudulent transactions:

(i) Always obtain an authorization code.

(ii) Verify additional information on the card such as the expiration date, Card Verification Value 2 (CVV2), and address verification service (AVS). If the cardholder is unable to provide this additional information or it does not match up, it may mean they do not actually have the card on their person.

(iii) Look for general warning signs (listed above).

(iv) If you suspect fraud (but still obtained an authorization code), ask for additional information (the name of the financial institution that issued the card), contact the cardholder directly, confirm the order by sending a note to the customers billing address first (if shipping address is different), and have the cardholder fax or email you a copy of their identification card and credit card.

METHODS OF FRAUD DETECTION

There are two prominent methods of fraud in credit card transactions, viz; data mining and machine learning. Data mining can be defined as the science and technology of exploring data in order to discover previously unknown patterns. Data mining is a confluence of multiple disciplines, among which are information science, database technology, statistics, visualization and machine learning. The most used method is machine learning which is concerned with the design and development of algorithms that allow computers to evolve behaviors based on empirical data, such as from sensor data or databases. The categorization of methods employed in fraud detection are analysed below:

Supervised Fraud Detection: Techniques that operate in supervised mode assume the availability of a training data set which has labeled instances for normal as well as fraud classes. Typical approach in such cases is to build a predictive model for fraud vs. non-fraud classes. Predictive supervised algorithms examine all previous labeled transactions to mathematically determine how a standard fraudulent transaction looks like by assigning a risk score. Any unseen data instance is compared against the model to determine which class it belongs to. Some supervised models have been implemented like in Ghosh and Reilly (1994), Syeda et al (2002), and Chiu and Tsai (2004). There are two major issues that arise in supervised fraud detection. First, the anomalous instances are far fewer compared to the normal instances in the training data. Issues that arise due to imbalanced class distributions have been addressed in the data mining and machine learning literature (Joshi et al. 2001; Phua et al. 2004). Second, obtaining accurate and representative labels, especially for the anomaly class is usually challenging.

Semi-Supervised Fraud Detection: Techniques that operate in a semi-supervised mode, assume that the training data has labeled instances for only the normal class. Since they do not require labels for the anomaly class, they are more widely applicable than supervised techniques. The typical approach used in such techniques is to build a model for the class corresponding to normal behavior, and use the model to identify anomalies in the test data. A limited set of anomaly detection techniques exist that assumes availability of only the anomaly instances for training. Aleskerov et al (1997), Kokkinaki (1997).

Unsupervised Fraud Detection: Techniques that operate in unsupervised mode do not require training data, and thus are most widely applicable. The techniques in this category make the implicit assumption that normal instances are far more frequent than anomalies in the test data. If this assumption is not true then such techniques suffer from high false alarm rate. Many semi-supervised techniques can be adapted to operate in an unsupervised mode by using a sample of the unlabeled data set as training data. Such adaptation assumes that the test data contains very few anomalies and the model learnt during training is robust to these few anomalies. Very few work has been done in this area like Dorronsoro et al (1997); Bolton and Hand, (2001) and Vladimir and Strizhak (2006).

Meta-Classifier Techniques: Stolfo et al. (1997) outlined a meta-classifier system for detecting credit card fraud that is based on the idea of using different local fraud detection tools within each different corporate environment and merging the results to yield a more accurate global tool. These fraud detection tools encompass the combinations of supervised models only, supervised and unsupervised models only. Each fraud detection tool has its unique strengths, so that it may perform better on particular data instances than the rest. Related work can be found in Burge, et al (1997), Chan et al (1999), Manoel F., et al (2007), Kim and Kim (2002), Wei Fan (1999), etc.

Anomaly Detection Techniques: The challenge associated with detecting unauthorized credit card usage is that it requires online detection of fraud as soon as the fraudulent transaction takes place. Anomaly detection techniques have been applied in two different ways to address this problem. The first one is known as by-owner in which each credit card user is profiled based on his/her credit card usage history. Any new transaction is compared to the user's profile and tagged as an anomaly if it does not match the profile. Another approach known as by-operation detects anomalies from among transactions taking place at a specific geographic location. Some of the anomaly techniques that are applicable to credit card fraud detection are discussed below.

Classification Based Techniques: Classification is used to learn a model (classifier) from a set of labeled data instances (training) and then, classify a test instance into one of the classes using the learnt model (testing). Classification based anomaly detection techniques operate under the following general assumption: "A classifier that can distinguish between normal and anomalous classes can be learnt in the given feature space". Classification based anomaly detection techniques operate in a similar two-phase fashion. The training phase learns a classifier using the available labeled training data. The testing phase classifies a test instance as normal or anomalous using the classifier. Based on the labels available for training phase, classification based anomaly detection techniques can be grouped into two broad categories: multi-class and one-class anomaly detection techniques.

Multi-class classification based anomaly detection techniques assume that the training data contains labeled instances belonging to multiple normal classes. Such anomaly detection techniques learn a classifier to distinguish between each normal class against the rest of the classes. One-class classification based anomaly detection techniques assume that all training instances have only one class label. Such techniques learn a discriminative boundary around the normal instances using a one-class classification algorithm. Neural Networks Based techniques are multi-layer feed forward, back-propagation; Bayesian Networks Based (linear and logistic discrimination), Rule Based such as BAYES, FOIL and RIPPER; Tree-based algorithms such as classification and regression tree (CART) and C4.5.

The classification based techniques employ powerful algorithms that can distinguish between instances belonging to different classes. But they assign a label

to each test instance, which can also become a disadvantage when a meaningful anomaly score is desired for the test instances.

Nearest Neighbour Based Techniques: A basic nearest neighbour anomaly detection technique is based on the following definition: "The anomaly score of a data instance is defined as its distance to its k nearest neighbour in a given data set". These techniques are based on the following key assumption: "Normal data instances occur in dense neighborhoods, while anomalies occur far from their closest neighbors". Nearest neighbour based anomaly detection techniques require a distance or similarity measure defined between two data instances. Distance (or similarity) between two data instances can be computed in different ways.

For continuous attributes, Euclidean distance is a popular choice but other measures can be used. A basic nearest neighbour anomaly detection technique is based on the following definition: The anomaly score of a data instance is defined as its distance to its k nearest neighbour in a given data set. Nearest neighbour based anomaly detection techniques can be broadly grouped into two categories: (i) Techniques that use the distance of a data instance to its k nearest neighbour as the anomaly score. (ii) Techniques that compute the relative density of each data instance to compute its anomaly score. The nearest neighbour based techniques are unsupervised in nature. However, if the data has normal instances that do not have enough close neighbours or if the data has anomalies that have enough close neighbours, the technique fails to label them correctly, resulting in missed anomalies.

Clustering Based Techniques: Clustering is used to group similar data instances into clusters. Clustering is primarily an unsupervised technique though semi-supervised clustering has also been explored lately. Even though clustering and anomaly detection appear to be fundamentally different from each other, several clustering based anomaly detection techniques have been developed. Clustering based anomaly detection techniques can be grouped into two categories.

First category of clustering based techniques rely on the following assumption: "Normal data instances belong to a cluster in the data, while anomalies either do not belong to any cluster". Techniques based on the above assumption apply a known clustering based algorithm to the data set and declare any data instance that does not belong to any cluster as anomalous.

Second category of clustering based techniques rely on the following assumption: "Normal data instances lie close to their closest cluster centroid, while anomalies are far away from their closest cluster centroid". Techniques based on the above assumption consist of two steps. In the first step, the data is clustered using a clustering algorithm. In the second step, for each data instance, its distance to its closest cluster centroid is calculated as its anomaly score. Techniques based on the second assumption can also operate in semi-supervised mode. Clustering based techniques performance is highly dependent on the effectiveness of clustering algorithm in capturing the cluster structure of normal instances.

Performance Metrics: Most credit card fraud detection techniques place monetary

value on predictions to maximize cost savings/profit. They can either define explicit cost (Chan et al, 1999; Fawcett and Provost, 1997), confidence metric (Brause et al, 1999), or misclassification costs (false positive and false negative, FP-FN) (Chen et al, 2004). Fawcett and Provost (1999) recommended Activity Monitoring Operating Characteristic (average score versus false alarm rate) suited for timely credit transactional fraud detection.

CONCLUDING REMARK

This extract has explored almost all published credit card fraud detection studies in comparison with three former reviewed papers. The papers reviewed showed that there has been great increase in the number of published papers especially on credit transactions and computer intrusion. We discussed credit card fraud and it the types, the technicality of credit card data, the methods and techniques of credit card fraud detection. However, unsupervised approaches from counter terrorism work, actual monitoring systems and spam detection communities can contribute to future fraud detection research in credit card online transactions.

REFERENCES

Aleskerov, E., B. Freisleben, B. Rao (1997). CARDWATCH: A neural network based database mining system for credit card fraud detection. In Proceedings of the IEEE/IAFE 1997 Conference on Computational Intelligence for Financial Engineering (CIFEr) pp. 220-226. IEEE Press.

Agyemang M., Barker K. and **Alhajj R.** (2006). A comprehensive survey of numeric and symbolic outlier mining techniques. *Intelligent Data Analysis* 10, 6, 521-538.

Alonso G., Manoel F., Xidi W. and **Alair P.** (2008). Comparison with Parametric Optimization in Credit Card Fraud Detection, Seventh International Conference .

APACS (2009). 2008 fraud figures, *http://www.apacs.org.uk/*09_03_1 9.htm.

Brause R., Langsdorf T. and **Hepp M.** (1999). Neural data mining for credit card fraud detection. In Proceedings of IEEE International Conference on Tools with Artificial Intelligence. 103-106.

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

Burge, P. and **J. Shawe-Taylor** (1997). Detecting cellular fraud using adaptive prototypes. In Proceedings of AAAI-97 Workshop on AI Approaches to Fraud Detection & Risk Management, pp. 9-13. AAAI Press.

Chan, P., Fan, W., Prodromidis, A. and **Stolfo, S.** (1999). Distributed Data Mining in Credit Card Fraud Detection. *IEEE Intelligent Systems* 14, 67-74.

Chen, R., Chiu, M., Huang, Y. and **Chen, L.** (2004). Detecting Credit Card Fraud by Using Questionnaire-Responded Transaction Model Based on Support Vector Machines. Proceedings of IDEAL2004, 800-806.

Chiu, C. and Tsai, C. (2004). A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection. Proc. of 2004 IEEE International Conference on e-Technology, e-Commerce and eService.

Clarke, M. (1990). The Control of Insurance Fraud: A Comparative View. *British Journal of Criminology,* 30, 1-23.

Clifton P., Vincent L., Kate S. & Ross G. (2003). A Comprehensive Survey of Data Mining-based Fraud Detection Research, Australia.

Dheepa V. and **Dhanapal R.** (2009). Analysis of Credit Card Fraud Detection Methods, International *Journal of Recent Trends in Engineering,* 2, 3.

David, J. H. (2007) Statistical techniques for fraud detection, prevention, and evaluation. London: Imperial College.

Dorronsoro J., Ginel F., Sánchez and **Cruz S.** (1997). Neural fraud detection in credit card operations. *IEEE Transactions on Neural Networks* 8 (4), 827-834.

Fawcett, T. and **Provost, F.** (1997). Adaptive fraud detection. *Journal of Data Mining and Knowledge*

Discovery 1 (3), 291-316.

Gary, M. W. (2009). *Data Mining in the Telecommunications Industry.* Fordham University, USA, IGI Global. 486-491

Ghosh, S. and **D. L. Reilly** (1994). Credit card fraud detection with a neural network. In Proc. of the Twenty-Seventh Hawaii Int. Conference on System Sciences, pp. 621-630. IEEE Computer Society Press.

Hodge, V. and **Austin, J.** (2004). A survey of outlier detection methodologies. *Artificial Intelligence Review,* 22, (2) 85-126.

Jing H., Xiantao L., Yong S., Weixuan X. and **Nian Y.** (2004). Classifications of Credit Cardholder Behavior by using Fuzzy Linear Programming. *International Journal of Information Technology & Decision Making,* 3, 633-650.

Kim, M. and **Kim, T.** (2002). A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection. *Proceedings of IDEAL,* 378-383.

Kokkinaki, A. (1997). On Atypical Database Transactions: Identification of Probable Frauds using Machine Learning for User Profiling. Proc. of IEEE Knowledge and Data Engineering Exchange Workshop, 107-113.

Kou, Y., C. Lu, S. Sirwongwattana and **Y. Huang** (2004). Survey of fraud detection Techniques. Proceeding of the 2004 International Conference on Networking, Sensing, and Control, pp. 749-754.

Kundu A., Sural S. and **Majumdar A.** (2006). Two-stage credit card fraud detection using sequence alignment, Lecture notes in computer science, Springer, Berlin, ISSN 0302-9743.

Markou, M. and **Singh, S.** (2003a). Novelty detection: a review-part 1: *Statistical Approaches. Signal Processing* 83, 12, 2481-2497.

Markou, M. and **Singh, S.** (2003b). Novelty detection: a review-part 2: Neural Network based Approaches. *Signal Processing* 83, 12, 2499-2521.

Manoel F., Alonso G., Xidi W. and **Alair P.** (2007). Credit Card Fraud Detection with Artificial Immune System, ICARISO.

Moreau Y., Preenel B., Burge P., Shawe-Taylor J., Störmann C. and Cooke C. (1996). Novel techniques for fraud detection in mobile telecommunication networks. In Proceedings of ACTS Mobile Telecommunications Summit, Granada, Spain.

Niall M. A., Christopher W. and David J. (2007) Plastic Card Fraud Detection using Peer Group Analysis.

Nigrini, M. J. (1999). I've got your number. *Journal of Accountancy* May 79-83.

Peter J. B., Jungwon K., Gil-Ho J. and **Jong-Uk C.** (2000) Fuzzy Darwinian Detection of Credit Card Fraud. (Retrieved on-line)

Phua C., Lee V., Smith K. and **Gayler R.** (2005). A Comprehensive Survey of Data Mining-based Fraud Detection Research. *Artificial Intelligence Review.*

Patcha, A. and **Park, J.** (2004). A Game Theoretic Approach to Modeling Intrusion Detection in Mobile Ad Hoc Networks. Proceedings of 2004 IEEE Workshop on Information Assurance and Security, 30-34.

Richard J. B. and **David J. H.** (2002). Statistical Fraud Detection: A Review. *Statistical Science,* 17, (3), 235-255.

Stolfo S. J., Fan D. W., Lee W. and **Prodromidis A. L.** (1997). Credit card fraud detection using meta-learning: Issues and initial results. In Proceedings of AAAI-97 Workshop on AI Approaches to Fraud Detection & Risk Management, pp. 83-90. AAAI Press.

Syeda, M., Zhang, Y. and **Pan, Y.** (2002). Parallel Granular Neural Networks for Fast Credit Card Fraud Detection. Proc. of the 2002 IEEE International Conference on Fuzzy Systems.

Tan P., Steinbach M. and **Kumar V.** (2005). *Introduction to Data Mining.* Addison-Wesley.

Varun C., Arindam B. and **Vipin K.** (2009). *Anomaly Detection: A Survey.* ACM Computing Surveys.

Vatsa V., Sural S. and **Majumdar A.** (2005). A game-Theoretical approach to Credit Card Fraud Detection. *ICISS,* 3803, 263-276.

Vladimir, Z. and **Strizhak, A.** (2006). Credit Card Fraud Detection Using Self-Organizing Maps. *Information & Security. An International Journal,* 18, 48-63.

Wei F., Prodromidis A. L. and **Stolfo S. J.** (1999). Distributed Data Mining in Credit Card Fraud detection Intelligent Systems and Their Applications, IEEE in Intelligent Systems and Their Applications, *IEEE,* 14 (6), 67-74.

Whitrow C., Hand D., Juszczak P., Weston D. and **Adams N.** (2009). Transaction Aggregation as a Strategy for Credit Card Fraud Detection. *Data Min Knowl Disc,* 18, 30-55.

Wheeler, R. and **Aitken, S.** (2000). Multiple Algorithms for Fraud Detection. *Knowledge-Based Systems,* 13 (3), 93-99.