A Survey on Financial Fraud Detection Methodologies

Pankaj Richhariya
BITS, Bhopal

Prashant K Singh
ISC Softwares

ABSTRACT
Owing to levitate and rapid escalation of E-Commerce, cases of financial fraud allied with it are also intensifying and which results in trouncing of billions of dollars worldwide each year. Fraud detection involves scrutinizing the behavior of populations of users in order to ballpark figure, detect, or steer clear of objectionable behavior: Undesirable behavior is a extensive term including delinquency: swindle, infringement, and account evasion. Factually, swindle transactions are speckled with genuine transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately. In this survey we, will focuses on classifying fraudulent behaviors, identifying the major sources and characteristics of the data based on which fraud detection has been conducted. This paper provide a comprehensive survey and review of different techniques to detect the financial fraud detection used in various fraud like credit card fraud detection, online auction fraud, telecommunication fraud detection, and computer intrusion detection.

General Terms
Financial fraud, financial transaction, Fraudster

Keywords
Fraud detection, Data mining, Neural network

1. INTRODUCTION
The Association of Certified Fraud Examiners (ACFE) defined fraud as "the use of one's occupation for personal enrichment through the deliberate misuse or application of the employing organization's resources or assets" [1]. Swindle activities are unfavorably affecting businesses. As a effect of which it has turn out be a stuff of immense fretful & obligatory to be explored. The assorted methods which are presently being worned for swindle detection are Statistics, Data Mining, and Neural Network & Artificial Intelligence. Issues in the development of new methods of fraud detection: Limitation of exchange of ideas, unavailability of data sets & hidden results of exploration. Swindle is revealed by sieving the anomalies in data & patterns. Employing accounting, auditing & investigative skills along with mathematical, statistical & data mining models discover frauds [2].

Financial Fraud: Asset misappropriation, kick backs etc. are included in Internal Financial Fraud. External Financial Fraud includes misrepresentation of company's financial position to stake holders. As per the literature published so far it can be said that most of research is done on detection of External Financial Fraud. Unfortunately very little work is done on internal financial fraud. Methods like Artificial Neural Network, Genetic Algorithm, Rough & Fuzzy set, Rule Discovery, Cluster Analysis & logistic regression are reviewed for discovering frauds. Knowledge Driven Internal Fraud Detection (KDIFD) framework is proposed for discovering internal financial fraud in paper [3]. This framework helps the auditors in finally confirming whether possibility of fraud is or not.

Financial fraud detection (FFD) is vital for the prevention of the often devastating consequences of financial fraud. FFD involves distinguishing fraudulent financial data from authentic data, thereby disclosing fraudulent behavior or activities and enabling decision makers to develop appropriate strategies to decrease the impact of fraud.

In general, the objective of fraud detection is to maximize correct predictions and maintain incorrect predictions at an acceptable level [4]. A high correct diagnostic probability can be implied by minimizing probability of undetected fraud and false alarms. Some technical terms are described as follows. False alarm rate (or false positive rate) is the percentage of legitimate transactions that are incorrectly identified as fraudulent. Fraud catching rate (or true positive rate or detection accuracy rate) is the percentage of fraudulent transactions that are correctly identified as fraudulent.

The objectives of this paper is to provide a comprehensive review of different techniques to detect financial frauds and defined existing challenges in this domain for the different types of large dataset and streams. It categories, compare and summarizes relevant financial fraud detection methods and techniques in published academic and industrial research. Second, to highlight promising new directions from related adversarial financial fields such as epidemic and outbreak detection, insider trading, intrusion detection, money laundering, spam detection and terrorist detection. Knowledge and experience from these adversarial domains can be interchangeable can be interchangeable and will help prevent repetitions of common mistakes and reinventions of the wheel'.

2. LITERATURE REVIEW
As a result of diverse perception, several groups of researchers have devoted a momentous amount of effort in studying financial fraud exposure for which various data mining algorithm has been espoused. For instance, no-fraud firms have boards with radically higher percentages of outside members than swindle firms, found by using Logit regression analysis Beasley [5]. Prediction of management fraud based on a set of data developed by an international public secretarial firm was done by a powerful sweeping qualitative response model by Hansen et al. [6]. A research was demeanor to examine the use of expert systems to enhance the performance of auditors [7]. A neural network fraud classification model employing endogenous financial data was presented by Green and Choi [8].The learned behavior pattern then created a classification model which applied to test sample. For prediction of management fraud Fanning and Cogger [9] used an artificial neural network. They found a model of eight variables with a high probability of detection using publicly available predictors of fraudulent financial

statements. The incentives and the penalties are investigated allied to earnings overstatements above all in firms that are subject to accounting enforcement actions by the Securities and Exchange Commission by Beneish [10]. Abbott et al. [11] scrutinized and deliberated the audit committee autonomy and activity in extenuating the likelihood of fraud. A number of researchers have endeavored to synthesize the literature. As, Phua et al. [12] sorted, contrasted, abridged and recapitulated from approximately all published technical and review articles in automated swindle detection of the last 10 years. Nevertheless, the research focused on general exposure like financial crime and terrorist detection, spam and intrusion detection. In this study, we comprehensively examine publicly presented papers about data mining and accounting for detecting FSF specially. We exercised recent references (from years 1995 to 2011) on financial fraud detection methods. We also exercised on references about the liaison of fraud, auditor & governance as the basis for our review and scrutiny.

Analyzing the so far published literature it is pragmatic that most of the articles focus on detection of external financial fraud. For detecting external fraud for instance financial statement frauds advanced analytical techniques have been proposed. The work done in the area of internal financial fraud is meager. An analysis of advanced statistical methods such as logistic regression, cluster analysis, rule discovery, fuzzy set, genetic algorithm and artificial neural networks for discovering fraud [13, 14]

3. FINANCIAL FRAUD

Financial institutions have now recognized that the application of isolated security mechanisms on individual delivery channels simply no longer enforces the necessary levels of protection against unauthorized account activity [15] and [16]. Financial IT platforms are often easy fraud targets due to their potential for large scale monetary theft through the numerous authentication flaws and loopholes within deployed service platform security models. Weak authentication provided by signature, PIN, password and Card Security Code (CSC) mechanisms therefore continue to facilitate illegitimate financial transactions through development of innovative system attacks and methodologies by malicious third parties.

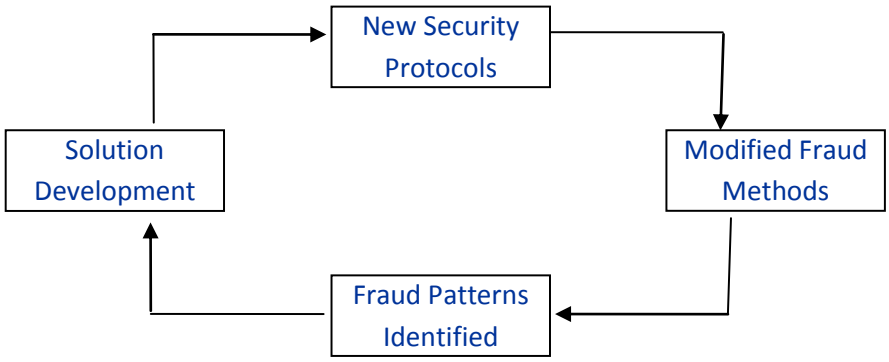

Fig 1: Threat Cycle of Fraud

4. FRAUD MANAGEMENT

Financial Banks have great concern in the swift swindle detection because of its strong influence on bottom line operating expenditure, service delivery and its reputation. Therefore several institutions are merging typical channelized security rules with a surplus security layer called as 'Swindle Management' to recompense for the various deficiencies which fraudsters suffer within channelized authentication mechanisms. Swindle management technologies simplify the active vetting of account activity data to cultivate all-inclusive swindle control framework with multi-level assimilated security about all service conveyance networks.

Financial organizations endure to multiply the convenience of financial amenities by deploying modern service techniques comprising plastic credit/debit cards, Automated Teller Machines (ATM), internet banking services and even mobile banking applications. Received requests are directed by allied network level servers for application layer management of financial services within fundamental business and data logic system layers. Network level security rules & techniques are imposed for authentication of honest customers using techniques based predominantly on the "what the user knows" and "what the user has" security standards. So, introducing users essentially put forward the obligatory security information like Personal Details, Personal Identification Number, and Passwords etc. or retain the necessary security device such as smart card, hard security token etc. to confirm themselves as an honest account possessor to and accomplish the asked financial service.

In Reactive Fraud Management, knowledge discovery techniques such as data mining [6] are applied to achieve algorithmic processing and complex calculations on stowed transactional data. Fraudulent cases are recognized either compared to pre-identified fraud patterns or as unusual behavior against the reported previous behavioral history. In spite of this the execution of a 'store now, query later' method ominously raises swindle detection latency due to the need of transactional data within the evaluated data store prior to application of employed data analysis techniques. Therefore

eliciting of a preventive reply may only be undertaken following transaction accomplishment and advancement of the allied fiscal value.

Shortcoming of Reactive fraud management solutions is dependence on labeled priming data sets for complying required behavioral models against which estimate new data occurrences, also as new data occurrences essentially be labeled and models continually retrained for detection of the newest fraud threats from unlabelled incoming transaction requests. So, substantial delay is experienced as an adequate number of labeled swindle cases are recognized and labeled suitably for contribution to the training data set, during which fraud cases will go undetected and add to a significant financial loss.

5. METHODS & TECHNIQUES

In this section we study four commonly used major methods, and their equivalent algorithms and techniques.

Overview: A fascinating concept borrowed from spam [16] is to know the terrestrial nature of fraud in the "black lists" by chasing the frequency of terms and category of terms i.e. fraudsters' tactics in the attributes of eventual fraudulent illustrations. Here is delineating for the convoluted nature of data used for fraud detection in common [19]:

- Class distributions (proportion of dishonest examples to honest examples) will eventually change as a consequence of independent fluctuation in volume of illegitimate & legitimate classes.
- Numerous mode of fraud can occur together. Every style can have a usual, irregular, recurrent, or once off terrestrial characteristic.
- Legitimate characteristics/conduct can change in due course.
- The same swindlers continue to bring contemporary or customized ways of fraud until the detection system commence false negatives again within short span of time after revealing the current modus operandi of trained swindlers.

5.1 Supervised algorithms

Predictive supervised algorithms study all known labeled transactions to mathematically uncover how a typical deceptive transaction looks like by assigning the risk score [16].

SVMs (Support Vector Machines) and admired Neural networks have been applied. A three layer, feed-forward Radial Basis Function (RBF) neural network for new credit card transactions used by Ghosh and Reilly [17] through only two priming passes required to churn out a fraud score in every two hours.

Barse et al [18] bring into play a multi-layer neural network companying exponential trace memory to manage chronological enslavement in synthetic Video-on-Demand log data.

Syeda et al [19] offer fuzzy neural networks on parallel machines to accelerate rule production for customer specific credit card swindle detection.

For credit transactional fraud detection comparative study of neural network and Bayesian network [20] works on the STAGE algorithm for Bayesian networks and back propagation algorithm for neural networks. Proportional outcomes prove that Bayesian networks were more correct and rapid to train, but cannot pace when applied to novel instances.

Supplementary techniques comprise of association rules, genetic programming and expert systems. Insurance fraud detection mainly used Expert systems.

Chiu and Tsai [21] bring in a Fraud Patterns Mining (FPM) algorithm, customized from Apriori, to extract a common format for fraud-only credit card data.

Kim et al [22] recommend SVM ensembles with either snaring or making the things better by telecommunications subscription fraud methods aggregation.

Ezawa and Norton [23] expound Bayesian network models with two parameters in four stages. They claim neural networks, nearest-neighbor, and regression to be too slow & also decision trees have some stumbling block with certain discrete variables. The model give performed outstanding for their telecommunications uncollectible debt data with nearly all variables and with a few dependencies.

Bentley [24] created rules for classifying data tested on real home insurance claims and credit card data used fuzzy logic with genetic programming.

Major and Riedinger [25] have put into action five-layer expert system, integrated expert knowledge with statistical information estimation to discover medical insurance fraud.

Pathak et al [26], Stefano and Gisella [27] and Von Altrock [28] have conducted experiments on fuzzy expert systems.

Deshmukh and Talluru [29] implemented an expert system to management fraud transaction data [24].

None of these papers on expert systems, association rules, and genetic programming provide any direct comparisons with the many other available methods and techniques. Supervised algorithms discussed so far are conformist learning techniques which can only process structured data from one to one data tables. Foster research by means of labeled data in fraud detection can benefit by applying relational learning approaches like Inductive Logic Programming (ILP) and simple homophily-based classifiers [30] on relational databases. Perlich and Provost [30] as well gave new target-dependent aggregation methods for conversion of the relation learning problem into conventional.

5.2 Hybrid Algorithms

5.2.1 Supervised Hybrid

Pervasive supervised algorithms such as Neural networks, Bayesian networks, and decision trees have been pooled or applied adequately to get better results.

Chan et al [31] uses naive Bayes, C4.5, CART, and RIPPER as foundation classifiers and amass to combine them. They also studied bridging irreconcilable data sets from various companies and the abridging of base classifiers. The outcome is lofty cost savings and enhanced efficiency on credit card transactions.

Phua et al [33] proposes back propagation neural networks, naive Bayes, and C4.5 as base classifiers on data partitions derived from minority oversampling with replacement. Its originality lies in the use of a single meta-classifier (stacking) to choose the best base classifiers, and then combine these base classifiers' predictions (bagging) to produce the best cost savings on automobile insurance claims.

5.2.2 Supervised/ Unsupervised Hybrid

For telecommunications fraud detection massive work is done on labeled data using both supervised and unsupervised algorithms.

Cortes and Pregibon [34] recommend signatures (summaries of telecommunication account) which are restructured every day. Fake signatures are added to the priming set and handled by supervised algorithms such as a model-averaged regression, tree, and slipper. They observed that fake toll-free numbers lean to have generally late night commotion and stretched call durations. Cortes and Pregibon [34] use signatures supposed to be genuine to know important fluctuations in calling behavior. Remarkable country combinations and temporal information from the previous month are discovered using Association Rules. Visual detection fraudulent international call accounts can be done by a graph-theoretic method [39].

Cahill et al [35] consign an averaged inkling score to all the calls (event-driven) based on its similitude to fraudulent signatures and dissimilitude to its account's normal signature. Current calls are heavily weighted than earlier ones and low scores calls are used to update the signature.

Results are better with supervised approaches as compared to unsupervised ones as proved by two investigations on telecommunication data using AUC as the performance measure.

According to Moreau et al [36] rule induction algorithms and supervised neural network are more efficient than two forms of unsupervised neural networks in differential identification between short-term and long-term statistical account behavior profiles. Hybrid model, combination of four techniques using logistic regression is superlative. Using true positive rate with no false positives as the performance measure,

Taniguchi et al [37] also claim the outperformance of supervised neural networks and Bayesian networks on labeled data than unsupervised techniques like Gaussian mixture models on all non-fraud users to detect anomalous phone calls.

Insurance data is segmented into clusters for supervised approaches using unsupervised approaches. A three step process: (a) k-means for cluster detection (b) C4.5 for decision tree rule induction (c) domain knowledge, statistical summaries and visualization tools is applied by Williams and Huang [38] for rule evaluation. Instead of C4.5 they also used a genetic algorithm, to make rules and to permit the domain user, like a fraud specialist, to look at the rules and to permit them to consequently develop on medical insurance claims.

Brockett et al [39] gave a similar method using the Self Organizing Maps (SOM) for detecting clusters in automobile injury claims before back propagation neural networks.

Cox [40] to monitor medical providers' claims utilized an unsupervised neural network pursued by a neuro-fuzzy classification system.

5.2.3 Semi-Supervised Algorithm with only legal non fraud data

Kim et al [41] created a new five steps fraud detection method: (a) Using association rules algorithm Apriori and increase diversity by a calendar schema to make rules randomly; (b) apply rules on known legitimate transaction database, remove any rule which matches this data; (c) use remaining rules to monitor actual system, reject any rule which detects no abnormality; (d) repeat any rule which identify abnormality by adding tiny random mutations; (e) preserve & maintain the successful rules. Even previously and currently this system is being tested for internal fraud by employees within the retail transactions processing system.

Murad and Pinkas [42] utilize the details from each telecommunications account such as silhouette at call, study of all levels of normal behavior. By a clustering algorithm with cumulative distribution distance function the common daily silhouettes are wringed. A signal is raised if the daily silhouette's call destination, duration, quantity surpass the threshold and standard deviation of the inclusive silhouette.

Aleskerov et al [43] studied on each credit card account's legal transactions with auto-associative neural networks (one hidden layer and the same number of input and output neurons).

Kokkinaki [44] proposes similarity trees (decision trees with Boolean logic functions) to profile each legitimate customer's behavior to detect deviations from the norm and cluster analysis to segregate each legitimate customer's credit card transactions.

5.3 Unsupervised Algorithm

Ardent research techniques in antiterrorism, law enforcement, and other security areas are Link analysis & Graph mining, but these look to be relatively under-valued in fraud detection research. White paper [45] explanation for the emergent group algorithm utilization in making clusters of cozily connected data and how it led to ensnare of an actual enigmatic fraudster by visually scrutinizing one year worth of insurance claims. An application is developed to flexibly encode data using color, position, size and other visual characteristics with multiple different views and levels for visual telecommunications fraud detection system [40]. The idea is to merge machine computation and human detection.

Cortes et al [34] study sequential development of hefty dynamic graphs' for detecting telecommunications fraud. Each graph is collection of sub graphs called Communities of Interest (COI). The authors used the exponential weighted average method to renovate sub graphs daily to trounce the flux of using just the current graph, and storage and weight-age problems of using all graphs at each time step.

By linking mobile phone accounts using call quantity and durations to form COIs, the authors confirm two distinctive characteristics of fraudsters. First, fraudulent phone accounts are linked - fraudsters call each other or the same phone numbers. Second, fraudulent call behavior from flagged frauds are reflected in some new phone accounts - fraudsters retaliate with application fraud/identity crime after being detected. Cortes et al [34] states their contribution to dynamic graph research in the areas of scale, speed, dynamic updating, condensed representation of the graph, and measure direct interaction between nodes.

Bolton and Hand [46] acclaim Peer Group Analysis to keep an eye on inter account behavior over time. Target account collective weekly amount is compared with other accounts (peer group) at ensuing time points. The distance metric/suspicion score is a t-statistic which determines the standardized distance from the center of the peer group. The time window to calculate peer group is ninety-one day time window is used to calculate the peer group and twenty-eight future time window on credit card accounts. They also recommend Break Point Analysis to keep an eye on intra account behavior over time. It senses hasty spending or

sudden surges in weekly spending in single account. Accounts are tiered by the t-test. Twenty-four transactions are present in a fixed-length moving transaction window: first twenty for training and next four for assessment on credit card accounts.

6. FRAUD DETECTION CASES

6.1 Credit Card fraud detection

Unsupervised learning is adopted in this model. Without the knowledge of fraudulent & non-fraudulent transactions in advance variations in behavior or unusual transactions are detected by this model. These techniques form a baseline for the typical behavior depiction pursued by the detection of observations showing maximum departure from this base line. Unsupervised method is used to detect previously undiscovered types of fraud however the detection is done by substandard observations. In outlier detection technique with supervised learning approach is useful only for the circumstances where previously occurred swindles are to be detected & also exact identification of fraudulent transactions is required. The main shortcoming of this technique is that it can detect only previously revealed fraud. The Abnormal spending behavior & frequency of transactions identified as outliers.

6.2 Telecommunication Fraud Detection

Accustoming sophisticatedly to the behavior of the various users. Network computers user profiles autonomously. Thus it has been widely used in detecting fraud. Neural Networks are entitled to considerably cut the operation costs. ASPECT, European Commission project, using together the supervised & unsupervised approach examined the practicability of the instigation with neural & rule based approach on toll tickets data [47]. In [37] three concepts were presented based on toll tickets (billing purpose call records). First, a supervised feed-forward neural network, which classify subscribers using digest statistics by studying non-linear discriminative function. Second, the Gaussian mixture model density estimation detecting any abnormalities from the past behavior by applying it to sculpt the previous behavior of all subscribers. Third, Bayesian networks are worned to characterize probabilistic models specified the subscribers' behavior.

6.3 Online auction fraud detection

Online Auction put on mammoth popularity by creating an accessible environment for exchanging goods at rational prices. Even though the number of sellers and buyers fascinated by online auctions is growing swiftly, this modern business medium defy an imperative challenge – auction fraud. Both sellers and buyers can partake in auction fraud for their own profit.

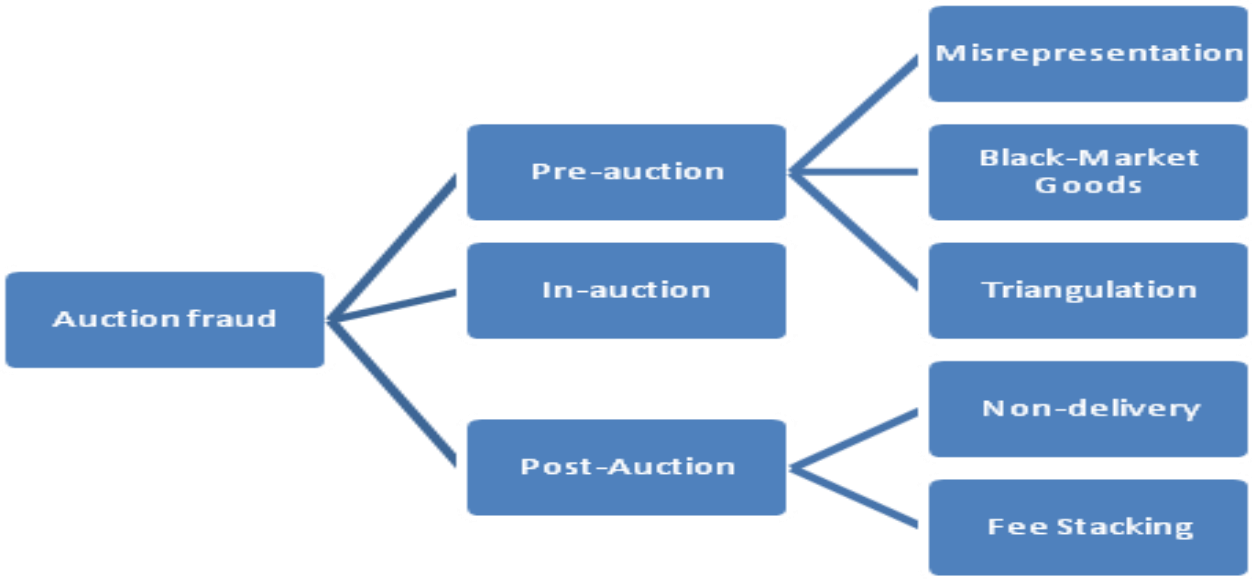

Fig 2: Classification of Online auction fraud

Pre-auction and post-auction frauds does not depend much on online prevention & detection mechanism because it comprise offline behavior so their investigation depends more on real-world evidence. On the other hand, in-auction fraud ensue when transactions are proceeded, thus it may happen devoid of direct physical proof, and nastiest of all is that it may not even be perceived by the sufferers. Due to the complication in detection of in-auction fraud has fascinated much less attention whereas pre-auction & post-auction frauds have previously fascinated policy makers' & researchers' [48, 49].

6.4 Computer Intrusion Detection

Analysis of audit data generated by operating system becomes pedestal for operations of many intrusions detection system. Record of the chronologically arranged activities on a system logged into a file is known to be an audit trial. By maintaining cumulative audit trial statistics to automate and execute system monitoring intrusion detection system is required. Misuse Detection & Anomaly Detection: categorical classification based on the model for Intrusion detection approach.

Misuse detection endeavor to identify the damage of previously observed intrusions in pattern or signature such as frequent changes of directory or attempts to read a password file and directly monitor for the occurrence of these patterns [50], [51]. Misuse loom comprise and keystroke dynamics monitoring, expert systems, state transition analysis, model-based reasoning [52]. Previous attacks can be detected very consistently with a low FAR, since specific attack sequences are encoded into misuse detection system. Anomaly detection is bit difficult in comparison to Misuse detection. But misuse detection is not able to predict all the different attacks because it looks only known abused patterns.

In Anomaly detection initially a historical normal profile for each user is established after that suitably large deviation from the profile is used to point possible intrusions [51], [17]. Neural networks, predictive pattern generation and statistical approaches are taken in Anomaly detection approach. The benefit of anomaly detection is it probable to detect unusual attacks on the systems, because following the statistical model it compares current activities for past behavior, without relying known patterns. However, there are some of the weaknesses of this approach. The drawbacks of Anomaly detection approach are high FAR, unusual but justified use may sometimes be considered anomalous. Systems can be skilled over a period of time by intruders because statistical measures of user profile can be gradually prepared.

7. CONCLUSION

This paper provides a comprehensive survey in financial fraud detection methodologies. And defines the adversary, the types and subtypes of fraud, performance metrics, the nature of technical data, and the methods and techniques. After identifying the limitations in techniques and methods of fraud detection it is shown that this paper can benefit from other related fields.

There are only few approaches for credit card detection that are available in public because of the security issues. Among them, neural networks approach is a very popular tool. Due to lack of availability of data set it is difficult to implement. For intrusion detection, some techniques have been applied to the real application. However, it is difficult to test existing intrusion detection systems, simulate potential attack scenarios, and duplicate known attacks. Moreover, intrusion detection system has poor portability because the system and its rule set must be specific to the environment being monitored. Most telecommunication fraud detection techniques explore data set of toll tickets and detect fraud from call patterns. These systems are effective against several kinds of frauds, but still have some main problems: Firstly, they cannot support fraud incidences that not follow the profiles. Secondly, these systems require upgrading to keep them up to date with current frauds methods. Upgrade and maintenance costs are high and mean continual dependence on system vendors. Thirdly, they require very accurate definitions of thresholds and parameters.

8. ACKNOWLEDGMENTS

I would like to thank my colleagues for providing a stimulating and fun environment in which to learn and grow.

9. REFERENCES

[1] Investigating Fraudulent Acts, 2000 UNIVERSITY OF HOUSTON SYSTEM ADMINISTRATIVE MEMORANDUM, http://www.uhsa.uh.edu/sam/AM/01C04.htm

[2] Bologna, Jack & Robert J. Lindquist, 1987. Fraud Auditing & Forensic Accounting, New York: John Wiley & Sons.

[3] Prabin K Panigrahi,2011. “A Framework for Discovering Internal Financial Fraud Using Analytics” in Communication Systems and Network Technologies (CSNT), IEEE 2011 International Conference , pp. 323 - 327

[4] Stream Base, 2008 Entrust www.entrust.com

[5] M. S. Beasley,1996. “An empirical analysis of the relation between the board of director composition and financial statement fraud,” The Accounting Review, vol. 71, no. 4, pp. 443-465.

[6] J. V. Hansen, J. B. McDonald, and W. F. Messier, 1997. “A generalized qualitative-response model and the analysis of management fraud”, Management Science, vol. 42, pp. 1022-1032.

[7] M. M. Eining, DS. R. Jones, and J. K. Loebbecke, 1997. “Reliance on decision aids: an examination of auditors’ assessment of management fraud,” Auditing: A Journal of Practice and Theory, vol. 16, pp. 1-19.

[8] B. P. Green, and J. H. Choi, 1997. “Assessing the risk of management fraud through neural network technology,” Auditing, vol. 16, pp. 14-28.

[9] K. Fanning and K. Cogger, 1998. “Neural network detection of management fraud using published financial data,” International Journal of Intelligent Systems in Accounting, Finance & Management, vol. 7, no. 1, pp. 21-24.

[10] M. D. Beneish, 1999. “Incentives and penalities related to earnings overstatements that violate GAAP,” Accounting Review, vol. 4, pp. 425-457.

[11] L. J. Abbott, S. Parker, and G. F. Peters, 2001. “Audit committee characteristics and financial misstatement: A study of the efficacy of certain blue ribbon committee recommendation,” Proceedings of the Auditing Section of the AAA Meeting.

[12] K. Fanning, K., Cogger, and R. Srivastava, 1995. “Detection of management fraud: a neural network approach”, International Journal of Intelligent Systems in Accounting, Finance & Management, vol. 4(2), pp. 113-126.

[13] Agyemang, M., Barker, K., & Alhajj, 2006. “A comprehensive survey of numeric and symbolic outlier mining techniques”, Intelligent Data Analysis, vol.10, pp.521-538.

[14] Kou, Y., Lu, C., & Sirwongwattana, 2004. “Survey of Fraud Detection Techniques”, In International Conference on Networking, Sensing, and Control, pp.749-754.

[15] Massey, K. Massey, 2005. “Combating eFraud – a next generation approach”, Financial Insights White Paper.

[16] Fair Isaac, 2005 “The evolving threat of card skimming”, Fair Isaac White Paper.

[17] Ghosh, S. & Reilly, 2004. “Credit Card Fraud Detection with a Neural Network” In Proc. of 27th Hawaii

International Conference on Systems Science vol.3, pp.621-630.

[18] Barse, E., Kvarnstrom, H. & Jonson, 2003. "Synthesizing Test Data for Fraud Detection Systems" In Proc. of the 19th Annual Computer Security Applications Conference, pp.384-395.

[19] Syeda, M., Zhang, Y. & Pan, 2002. "Parallel Granular Neural Networks for Fast Credit Card Fraud Detection" In Proc. of the 2002 IEEE International Conference on Fuzzy Systems. 2002. Newsweek.

[20] Maes, S., Tuyls, K., Vanschoenwinkel, B. & Manderick, 2002. "Credit Card Fraud Detection using Bayesian and Neural Networks" In Proc. of the 1st International NAISO Congress on Neuro Fuzzy Technologies.

[21] Chiu, C. & Tsai, 2004. "A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection" In Proc. of 2004 IEEE International Conference on e-Technology, e-Commerce and e- Service.

[22] Kim, J., Ong, A. & Overill, R, 2003. "Design of an Artificial Immune System as a Novel Anomaly Detector for Combating Financial Fraud in Retail Sector", Congress on Evolutionary Computation.

[23] Ezawa, K. & Norton, S., 1996 "Constructing Bayesian Networks to Predict Uncollectible Telecommunications Accounts", IEEE Expert pp. 45-51.

[24] Bentley, P., Kim, J., Jung., G. & Choi, J. , 2000. "Fuzzy Darwinian Detection of Credit Card Fraud." In Proc. of 14th Annual Fall Symposium of the Korean Information Processing Society.

[25] Major, J. & Riedinger, D., 2002. "EFD: A Hybrid Knowledge/ Statistical-based system for the Detection of Fraud.", Journal of Risk and Insurance vol.69 (3), pp. 309-324.

[26] Pathak, J., Vidyarthi, N. & summers, S., 2003. "A Fuzzy-base Algorithm for Auditors to Detect Element of Fraud in Settled Insurance Claims", Odette School of Business Administration.

[27] Stefano, B. & Gisella, F., 2001. "Insurance Fraud Evaluation: A Fuzzy Expert System." In Proc. Of IEEE International Fuzzy Systems Conference, pp.1491-1494.

[28] Von Altrock, C., 1997. "Fuzzy Logic and Neurofuzzy Applications in Business and Finance." pp.286-294. Prentice Hall.

[29] Deshmukh, A. & Talluru, T., 1997. "A Rule Based Fuzzy Reasoning System for Assessing the Risk of Management Fraud." Journal of Intelligent Systems in Accounting, Finance & Management vol.7 (4), pp.669-673.

[30] Perlich, C. & Provost F., 2003. "Aggregation-based Feature Invention and Relational Concept Classes." In Proc. of SIGKDD03, pp.167-176.

[31] Chan, P., Fan, W., Prodromidis, A. & Stolfo, S., 1999. "Distributed Data Mining in Credit Card Fraud Detection." IEEE Intelligent Systems vol.14, pp. 67-74.

[32] Stefano, B. & Gisella, F., 2001. "Insurance Fraud Evaluation: A Fuzzy Expert System." In Proc. of IEEE International Fuzzy Systems Conference, pp.1491-1494.

[33] Phua, C., Alahakoon, D. & Lee., 2004. "Minority Report in Fraud Detection: Classification of Skewed Data", SIGKDD Explorations vol.6(1), pp.50-59.

[34] Cortes, C. & Pregibon, D., 2001. "Signature-Based Methods for Data Streams.", In Data Mining and Knowledge Discovery vol.5, pp. 167- 182.

[35] Cahill, M., Chen, F., Lambert, D., Pinheiro, J. & Sun, D., 2002. "Detecting Fraud in the Real World", Handbook of Massive Datasets pp.911-930.

[36] Moreau, Y., Lerouge, E., Verrelst, H., Vandewalle, J., Stormann, C. & Burge, P. , 1999. "BRUTUS: A Hybrid System for Fraud Detection in Mobile Communications." In Proc. Of European Symposium on Artificial Neural Networks, pp.447-454.

[37] Taniguchi, M., Haft, M., Hollmen, J. & Tresp, 1998. "Fraud Detection in Communication Networks using Neural and Probabilistic Methods." In Proc. of 1998 IEEE International Conference in Acoustics, Speech and Signal Processing, pp.1241- 1244.

[38] Williams, G., 1999. "Evolutionary Hot Spots Data Mining: An Architecture for Exploring for Interesting Discoveries." In Proc. of PAKDD99.

[39] Murad, U. & Pinkas, G., 1999. "Unsupervised Profiling for Identifying Superimposed Fraud." In Proc. of PKDD99.

[40] Cox, E., 1995. "A Fuzzy System for Detecting Anomalous Behaviors in Healthcare Provider Claims." In Goonatilake, S. & Treleaven, P. (eds.) Intelligent Systems for Finance and Business, pp.111-134. John Wiley and Sons Ltd.

[41] Kim, H., Pang, S., Je, H., Kim, D. & Bang, S., 2003. "Constructing Support Vector Machine Ensemble." In Pattern Recognition vol.36, pp. 2757-2767.

[42] Murad, U. & Pinkas, G.,1999. "Unsupervised Profiling for Identifying Superimposed Fraud.", In Proc. of PKDD99.

[43] Aleskerov, E., Freisleben, B. & Rao, B. , 1997 "CARDWATCH: A Neural Network-Based Database Mining System for Credit Card Fraud Detection." In Proc. of the IEEE/IAFE on Computational Intelligence for Financial Engineering, pp.220-226.

[44] Kokkinaki, A., 1997. "On Atypical Database Transactions: Identification of Probable Frauds using Machine Learning for User Profiling." In Proc. of IEEE Knowledge and Data Engineering Exchange Workshop, pp.107-113.

[45] Netmap. Fraud and Crime Example Brochure. 2004.

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

[47] Y. Moreau, B. Preneel, P. Burge, J. Shawe-Taylor, C. Stoermann, and C. Cooke., 1997. "Novel techniques for fraud detection in mobile telecommunication networks." In ACTS Mobile Summit, Grenada, Spain.

[48] B. Gavish and C.L. Tucci, 2008. "Reducing Internet Auction Fraud," Communications of the ACM (CACM), vol.51 (5), pp. 89-97.

[49] S. Ba and P. Pavlou, 2002. "Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior," MIS Quarterly, vol.26 (3), pp.243-268.

[50] T. D. Garvey and T. F. Lunt., 1991. "Model based intrusion detection." In Proceedings of the 14th National Computer Security Conference.

[51] A. K. Ghosh and A. Schwartzbard. , 1999. "A study in using neural networks for anomaly and misuse detection." In Proceedings of the 8th USENIX Security Symposium, D.C.

[52] S. E. Smaha and J.Winslow., 1994. "Misuse detection tools." In Computer Security Journal vol.10 (1), pp. 39 – 49, Spring.