Towards Fraud Detection Methodologies

Tareq Allan
Dakota State University
Madison, South Dakota, USA
tzallan@pluto.dsu.edu

Justin Zhan
National Center for the Protection of Financial Infrastructure
Madison, South Dakota, USA
justinzzhan@gmail.com

Abstract— **Fraud and abuse have led to significant additional expense in the banking and financial system of the United States. This paper aims to provide a comprehensive survey of the statistical methods applied to banking and financial fraud detection, with focuses on classifying fraudulent behaviors, identifying the major sources and characteristics of the data based on which fraud detection has been conducted, discussing the key steps in data preprocessing, as well as summarizing, categorizing, and comparing statistical fraud detection methods.**

I. 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]." In the technological systems, fraudulent activities have occurred in many areas of daily life such as telecommunication networks, mobile communications, on-line banking, and Ecommerce. Fraud is increasing dramatically with the expansion of modern technology and global communication, resulting in substantial losses to the businesses. Consequentially, fraud detection has become an important issue to be explored.

Fraud detection involves identifying fraud as quickly as possible once it has been perpetrated. Fraud detection methods are continuously developed to defend criminals in adapting to their strategies. The development of new fraud detection methods is made more difficult due to the severe limitation of the exchange of ideas in fraud detection. Data sets are not made available and results are often not disclosed to the public. The fraud cases have to be detected from the available huge data sets such as the logged data and user behavior. At present, fraud detection has been implemented by a number of methods such as data mining, statistics, and artificial intelligence. Fraud is discovered from anomalies in data and patterns. The types of frauds in this paper include credit card frauds, telecommunication frauds, and computer intrusion.

Institutions are now moving towards increasingly proactive methods of fraud detection for real-time screening of financial data, and triggering of a preventive response prior to transaction completion in order to minimize the potential fraud deficit ([2], [3] and [4]). While implementation of proactive methods increases the potential for early fraud alerting, real-time processing significantly reduces the available window within which to perform computational analysis and produce an accurate fraud decision in response to newly arriving system events. Policies based on global thresholds have limited capabilities due to their inability to learn and adapt to observed account behavior commonly resulting in large volumes of false alerts to be resolved by a business analyst. Research has illustrated how such methods can be refined to produce account-specific thresholds; however such methods continue to rely on labeled training data and application of values to derived account segments [5]. Existing research for monitoring of individual customer account behavior therefore remains tuned to fraud detection within reactive data processing architectures through application of data mining based methods over static post-transactional data repositories [6].

In general, the objective of fraud detection is to maximize correct predictions and maintain incorrect predictions at an acceptable level [7]. 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 are two-fold: First, to provide a comprehensive review of different techniques to detect frauds and define existing challenges in this domain for the different types of large datasets and streams. It categorizes, compares, and summarizes relevant financial and banking fraud detection methods and techniques in published academic and industrial research. Second, to highlight promising new directions from related adversarial banking and 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 and will help prevent repetitions of common mistakes and 'reinventions of the wheel'.

II. BACK GROUND

1. Fraudsters:

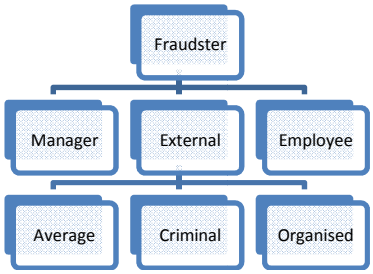

Figure 1: Hierarchy chart of fraud crime perpetrators from both firm-level and community-level perspectives.

With reference to figure 1, the profit-motivated fraudster has interactions with the affected business. Traditionally, each business is always susceptible to internal fraud or corruption from its management (high-level) and non-management employees (low-level). In addition to internal and external audits for fraud control, data mining can also be utilized as an analytical tool.

A fraudster can be an external party who can either commit fraud in the form of a prospective or existing customer (consumer) or a prospective/existing supplier (provider). The external fraudster has three basic profiles: the average offender, criminal offender, and organized crime offender. Average offenders display random and occasional dishonest behavior when there is an opportunity, sudden temptation, or when suffering from financial hardships.

In contrast, the more risky external fraudsters are individual criminal offenders and organized group crime offenders because they repeatedly disguise their true identities and evolve their modus operandi over time to approximate legal forms and to counter detection systems. It is important to account for the strategic interaction, or moves and countermoves, between a

978-1-4244-6949-9/10/$26.00 ©2010 IEEE

fraud detection system's algorithms and the professional fraudsters' modus operandi. An internal and insurance fraud is more likely to be committed by average offenders. Credit and telecommunications fraud is more vulnerable to professional fraudsters.

2. Affected Commercial Industries:

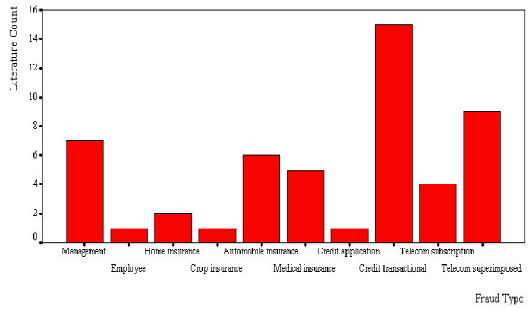

Figure 2: Bar chart of fraud types from 51 unique and published fraud detection papers.

Credit transactional fraud detection has received significant attention from researchers although it has been loosely used here to include bankruptcy prediction [8] and bad debts prediction [9]. Employee/retail [10], national crop insurance [11], and credit application [12] each has only one academic publication.

The main purpose of these detection systems is to identify general trends of suspicious/fraudulent applications and transactions. In the case of application fraud, these fraudsters apply for insurance entitlements using falsified information, and apply for credit and telecommunications products/services using non-existent identity information or someone else's identity information. In the case of transactional fraud, these fraudsters take over or add to the usage of an existing legitimate credit or telecommunications account.

There are other fraud detection domains. E-businesses and ecommerce on the Internet present a challenging data mining task because it blurs the boundaries between fraud detection systems and network intrusion detection systems. Related literature focus on video-on-demand websites [13] and IP-based telecommunication services [14]. Online sellers and online buyers can be monitored by automated systems. Fraud detection in government organizations such as tax and customs [15] has also been reported.

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 [16]and [17]. 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.

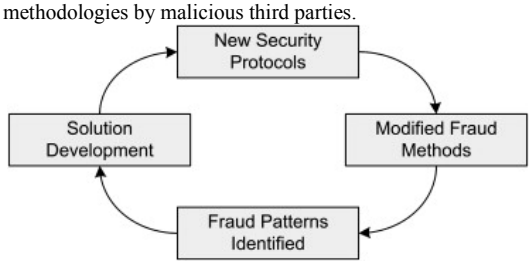

Figure 3: Fraud threat cycle.

Fraud in financial platforms can therefore be modeled as a recurring lifecycle illustrating the continual response of financial institutions to fraudster behavior (Figure 3). Emerging fraud trends are identified through data analysis and mining techniques over the institutions labeled transactional database to assist in formulation of new security policies and authentication protocols. In response, fraudsters modify their methods based upon new security deployments while identifying alternative fraud opportunities within the current service platform. New fraud patterns resulting from deployed security enhancements are then identified initiating further realignment of the organizations fraud prevention strategy through implementation of additional authentication and security procedures.

4. Fraud Management:

Banking institutions have a strong interest in the speed at which fraudulent activity can be detected due to its direct impact upon an institutions customer service delivery, bottom line operating expenditure and status as a reputable financial provider. Many institutions are therefore combining standard channel level security protocols with an additional security layer known as 'Fraud Management' to compensate for the numerous shortcomings which fraudsters continue to exploit within channel level authentication mechanisms. Fraud management technologies facilitate the active screening of account activity data to develop a holistic fraud control framework with multi-level integrated security across all service delivery channels

Financial institutions continue to expand the availability of financial services through deployment of innovative service channel provisions including Automated Teller Machines (ATM), plastic credit/debit cards, internet banking services and even mobile banking applications. Incoming requests are managed by associated channel level servers for application layer management of financial operations within underlying business and data logic system layers. Channel level security methods and protocols are enforced upon deployed service channel technologies for authentication of genuine account holders using techniques based primarily on the "*something the user knows"* and *"something the user has"* security paradigms. Accordingly, initiating users must submit the necessary security data (Personal Identification Number, Passwords, Personal Details, etc) or possess the required security device (Plastic card, hardware security token, etc) to authenticate themselves as a genuine account signatory and complete the requested financial transactions.

In *Reactive Fraud Management*, knowledge discovery techniques such as data mining [6] are implemented to perform algorithmic processing and complex calculations over stored transactional data. Fraudulent instances are identified either against pre-defined fraud pattern libraries or as anomalous behavior against the accounts previous behavioral history. Implementation of a 'store now, query later' approach however significantly increases the fraud detection latency due to the requirement of transactional data within the assessed data store prior to application of employed data analysis techniques. Triggering of a preventive response may therefore only be undertaken following transaction completion and movement of the associated monetary value.

Reactive fraud management solutions suffer due to their heavily reliance upon labeled training data sets for assembly of the required behavioral models against which to evaluate new data instances. Maintenance of reactive solutions presents further difficulties as new data instances must be labeled and models continually retrained for detection of the latest fraud threats from unlabelled incoming transaction requests. A significant delay is therefore incurred as a sufficient number of labeled fraud cases are identified and labeled appropriately for addition to the priming data set, during which fraud instances will go undetected and contribute to a substantial financial loss.

5. Neural Networks:

Neural network approaches are generally non-parametric and modelbased, they generalize well to unseen patterns and are capable of learning complex class boundaries. After training the neural network forms a classifier. However, the entire data set has to be traversed numerous times to allow the

network to settle and model the data correctly. They also require both training and testing to fine tune the network and determine threshold settings before they are ready for the classification of new data. Many neural networks are susceptible to the curse of dimensionality though less so than the statistical techniques. The neural networks attempt to fit a surface over the data and there must be sufficient data density to discern the surface. Most neural networks automatically reduce the input features to focus on the key attributes. But nevertheless, they still benefit from feature selection or lower dimensionality data projections.

III. METHODS AND TICHNEQUES

This section examines four major methods commonly used, and their corresponding techniques and algorithms.

Overview:

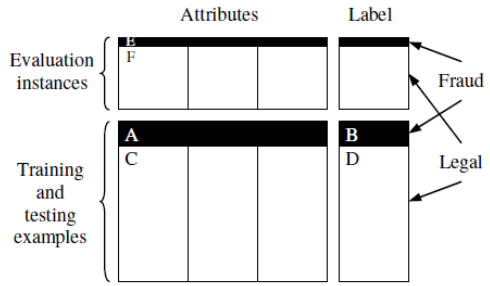

Figure 4: Structured diagram of the possible data for analysis. Data mining approaches can utilize training/testing data with labels, only legal examples, and no labels to predict/describe the evaluation data.

Figure 4 shows that many existing fraud detection systems typically operate by adding fraudulent claims/applications/ transactions/accounts/sequences (A) to "black lists" to match for likely frauds in the new instances (E). Some use hard-coded rules which each transaction should meet such as matching addresses and phone numbers, and price and amount limits [18].

An interesting idea borrowed from spam [19] is to understand the temporal nature of fraud in the "black lists" by tracking the frequency of terms and category of terms (style or strategy of fraudster) found in the attributes of fraudulent examples over time. Below outlines the complex nature of data used for fraud detection in general [19]:

- Volume of both fraud and legal classes will fluctuate independently of each other; therefore class distributions (proportion of illegitimate examples to legitimate examples) will change over time.
- Multiple styles of fraud can happen at around the same time. Each style can have a regular, occasional, seasonal, or onceoff temporal characteristic.
- Legal characteristics/behavior can change over time.
- Within the near future after uncovering the current *modus operandi* of professional fraudsters, these same fraudsters will continually supply new or modified styles of fraud until the detection systems start generating false negatives again.

With reference to Figure 4, the common data mining approaches to determine the most suspicious examples from the incoming data stream (evaluation data) are:

1. Labeled training data (A + B + C + D) can be processed by single *supervised* algorithms A better suggestion is to employ hybrids such as multiple supervised algorithms, or both supervised and unsupervised algorithms to output suspicion scores, rules and/or visual anomalies on evaluation data.
2. All known legal claims/ applications/ transactions/ accounts/ sequences (C) should be used processed by *semi-supervised* algorithms to detect significant anomalies from consistent normal behavior.
3. Combine training data with evaluation data (A + C + E + F). These should be processed by single or multiple *unsupervised* algorithms to output suspicion scores, rules and/or visual anomalies on evaluation data.

1. Supervised Algorithm (A + B + C + D):

Predictive supervised algorithms examine all previous labeled transactions to mathematically determine how a standard fraudulent transaction looks like by assigning a risk score [17]. Neural networks are popular and support vector machines (SVMs) have been applied. Ghosh and Reilly [20] used a three-layer, feed-forward Radial Basis Function (RBF) neural network with only two training passes needed to produce a fraud score in every two hours for new credit card transactions. Barse *et al* [21] used a multi-layer neural network with exponential trace memory to handle temporal dependencies in synthetic Video-on-Demand log data. Syeda *et al* [22] propose fuzzy neural networks on parallel machines to speed up rule production for customer-specific credit card fraud detection. Kim *et al* [23] proposes SVM ensembles with either bagging and boosting with aggregation methods for telecommunications subscription fraud.

The neural network and Bayesian network comparison study [24] uses the STAGE algorithm for Bayesian networks and backpropagation algorithm for neural networks in credit transactional fraud detection. Comparative results show that Bayesian networks were more accurate and much faster to train, but Bayesian networks are slower when applied to new instances.

Ezawa and Norton [25] developed Bayesian network models in four stages with two parameters. They argue that regression, nearest-neighbor, and neural networks are too slow and decision trees have difficulties with certain discrete variables. The model with most variables and with some dependencies performed best for their telecommunications uncollectible debt data.

Viaene *et al* [26] applies the weight of evidence formulation of AdaBoosted naive Bayes (boosted fully independent Bayesian network) scoring. This allows the computing of the relative importance (weight) for individual components of suspicion and displaying the aggregation of evidence pro and contra fraud as a balance of evidence which is governed by a simple additivity principle. Compared to unboosted and boosted naive Bayes, the framework showed slightly better accuracy and AUC but clearly improved on the cross entropy and Brier scores. It is also readily accessible and naturally interpretable decision support and allows for flexible human expert interaction and tuning on an automobile insurance dataset.

Belhadji *et al* [27] chooses the best indicators (attributes) of fraud by first querying domain experts, second calculating conditional probabilities of fraud for each indicator and third Probit regressions to determine most significant indicators. The authors also use Prohit regressions to predict fraud and adjusts the threshold to suit company fraud policy on automobile property damages. Artis *et al* [28] compares a multinomial logit model (MNL) and nested multinomial logit model (NMNL) on a multiclass classification problem. Both models provide estimated conditional probabilities for the three classes but NMNL uses the two step estimation for its nested choice decision tree. It was applied to automobile insurance data. Mercer [29] described least-squares stepwise regression analysis for anomaly detection on aggregated employee's applications data.

Other techniques include expert systems, association rules, and genetic programming. Expert systems have been applied to insurance fraud. Major and Riedinger [30] have implemented an actual five-layer expert system in which expert knowledge is integrated with statistical information assessment to identify medical insurance fraud. Pathak *et al* [31], Stefano and Gisella [32] and Von Altrock [33] have experimented on fuzzy expert systems. Deshmukh and Talluru [34] applied an expert system to management fraud. Chiu and Tsai [35] introduce a Fraud Patterns Mining (FPM) algorithm, modified from *Apriori*, to mine a common format for fraud-only credit card data. Bentley [36] uses genetic programming with fuzzy logic to create rules for classifying data. This system was tested on real home insurance claims and credit card

transaction data [36]. None of these papers on expert systems, association rules, and genetic programming provide any direct comparisons with the many other available methods and techniques.

The above supervised algorithms are conventional learning techniques which can only process structured data from single 1- to-1 data tables. Further research using labeled data in fraud detection can benefit from applying relational learning approaches such as Inductive Logic Programming (ILP) and simple homophily-based classifiers [37] on relational databases. Perlich and Provost [37] also present novel target-dependent aggregation methods for converting the relational learning problem into a conventional one.

2. Hybrid Algorithms:

2.1 Supervised Hybrid (A + B + C + D):

Popular supervised algorithms such as neural networks, Bayesian networks, and decision trees have been combined or applied in a sequential fashion to improve results. Chan *et al* [38] utilizes naive Bayes, C4.5, CART, and RIPPER as base classifiers and stacking to combine them. They also examine bridging incompatible data sets from different companies and the pruning of base classifiers. The results indicate high cost savings and better efficiency on credit card transactions. Phua *et al* [6] 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.

2.2 Supervised/ Unsupervised Hybrid (A + B + C + D)

There is extensive work on labeled data using both supervised and unsupervised algorithms in telecommunications fraud detection. Cortes and Pregibon [39] propose the use of signatures (telecommunication account summaries) which are updated daily (time-driven). Fraudulent signatures are added to the training set and processed by supervised algorithms such as a tree, slipper, and model-averaged regression. The authors remark that fraudulent toll-free numbers tend to have extensive late night activity and long call durations. Cortes and Pregibon [39] use signatures assumed to be legitimate to detect significant changes in calling behavior. Association rules are used to discover interesting country combinations and temporal information from the previous month. A graph-theoretic method [39] is used to visually detect communities of interest of fraudulent international call accounts. Cahill *et al* [40] assign an averaged suspicion score to each call (event-driven) based on its similarity to fraudulent signatures and dissimilarity to its account's normal signature. Calls with low scores are used to update the signature and recent calls are weighted more heavily than earlier ones in the signature.

Two studies on telecommunications data show that supervised approaches achieve better results than unsupervised ones. With AUC as the performance measure, Moreau *et al* [41] show that supervised neural network and rule induction algorithms outperform two forms of unsupervised neural networks which identify differences between short-term and long-term statistical account behavior profiles. The best results are from a hybrid model which combines these four techniques using logistic regression. Using true positive rate with no false positives as the performance measure, Taniguchi *et al* [42] claim that supervised neural networks and Bayesian networks on labeled data achieve significantly better outcomes than unsupervised techniques such as Gaussian mixture models on each non-fraud user to detect anomalous phone calls.

Unsupervised approaches have been used to segment the insurance data into clusters for supervised approaches. Williams and Huang [43] applies a three step process: *k*-means for cluster detection, C4.5 for decision tree rule induction, and domain knowledge, statistical summaries and visualization tools for rule evaluation. Williams [43] use a genetic algorithm, instead of C4.5, to generate rules and to allow the domain user, such as a fraud specialist, to explore the rules and to allow them to evolve accordingly on medical insurance claims. Brockett *et al* [46] present a similar methodology utilising the Self Organising Maps (SOM) for cluster detection before backpropagation neural networks in automobile injury claims. Cox [45] uses an unsupervised neural network followed by a neuro fuzzy classification system to monitor medical providers' claims.

3. Semi-Supervised Algorithm with only legal (non fraud) data (C):

Kim *et al* [10] implements a novel fraud detection method in five steps: **First**, generate rules randomly using association rules algorithm *Apriori* and increase diversity by a calendar schema; **second**, apply rules on known legitimate transaction database, discard any rule which matches this data; **third**, use remaining rules to monitor actual system, discard any rule which detects no anomalies; **fourth**, replicate any rule which detects anomalies by adding tiny random mutations; and **fifth**, retain the successful rules. This system has been and currently being tested for internal fraud by employees within the retail transaction processing system.

Murad and Pinkas [46] use profiling at call, daily, and overall levels of normal behavior from each telecommunications account. The common daily profiles are extracted using a clustering algorithm with cumulative distribution distance function. An alert is raised if the daily profile's call duration, destination, and quantity exceed the threshold and standard deviation of the overall profile. Aleskerov *et al* [47] experiment with auto-associative neural networks (one hidden layer and the same number of input and output neurons) on each credit card account's legal transactions. Kokkinaki [48] 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.

4. Unsupervised Algorithm with unlabeled data (A + C + E + F):

Link analysis and graph mining are hot research topics in antiterrorism, law enforcement, and other security areas, but these techniques seem to be relatively under-rated in fraud detection research. A white paper [49] describes how the emergent group algorithm is used to form groups of tightly connected data and how it led to the capture of an actual elusive fraudster by visually analyzing twelve months worth of insurance claims. There is a brief application description of a visual telecommunications fraud detection system [45] which flexibly encodes data using color, position, size and other visual characteristics with multiple different views and levels. The intuition is to combine human detection with machine computation.

Cortes *et al* [39] examines temporal evolution of large dynamic graphs' for telecommunications fraud detection. Each graph is made up of subgraphs called Communities Of Interest (COI). To overcome instability of using just the current graph, and storage and weightage problems of using all graphs at all time steps; the authors used the exponential weighted average approach to update subgraphs daily. 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* [39] 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 [50] recommend Peer Group Analysis to monitor inter-account behavior over time. It compares the cumulative mean weekly amount between a target account and other similar accounts (peer group) at subsequent 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 thirteen weeks and future time window is four weeks on credit card accounts. Bolton and Hand [50] also suggest Break Point Analysis to monitor intraaccount behavior over time. It detects rapid spending or sharp increases in weekly spending within a single account. Accounts are ranked by the *t*-test. The fixed-length moving transaction window contains twenty-four transactions: first twenty for training and next four for evaluation on credit card accounts.

IV. FRAUD DETECTION CASES

1. Credit Card Fraud Detection:

Unsupervised approach is employed to this model. Usually, the result of unsupervised approach is a new explanation or representation of the observation data, which will then lead to improved future responses or decisions. Unsupervised methods do not need the prior knowledge of fraudulent and non-fraudulent transactions in historical database, but instead detect changes in behavior or unusual transactions. These methods model a baseline distribution that represents normal behavior and then detect observations that show greatest departure from this norm. In supervised methods, models are trained to discriminate between fraudulent and non-fraudulent behavior so that new observations can be assigned to classes.
Supervised methods require accurate identification of fraudulent transactions in historical databases and can only be used to detect frauds of a type that have previously occurred. An advantage of using unsupervised methods over supervised methods is that previously undiscovered types of fraud may be detected. Supervised methods are only trained to discriminate between legitimate transactions and previously known fraud.

2. Computer Intrusion Detection:

Many intrusion detection systems base their operations on analysis of audit data generated by the operating system. An audit trail is a record of activities on a system that are logged to a file in chronologically sorted order. An intrusion detection system is needed to automate and perform system monitoring by keeping aggregate audit trail statistics. Intrusion detection approaches can be broadly classified into two categories based on model of intrusions: misuse and anomaly detection.

Misuse detection attempts to recognize the attacks of previously observed intrusions in the form of a pattern or a signature (for example, frequent changes of directory or attempts to read a password file) and directly monitor for the occurrence of these patterns [51], [52]. Misuse approaches include expert systems, model-based reasoning, state transition analysis, and keystroke dynamics monitoring [53]. Since specific attack sequences are encoded into misuse detection system, known attacks can be detected very reliably with a low false alarm rate. Misuse detection is simpler than anomaly detection. However, a primary drawback of misuse detection is that it is not possible to anticipate all the different attacks because it looks only known patterns of abuse.

Anomaly detection tries to establish a historical normal profile for each user, and then use sufficiently large deviation from the profile to indicate possible intrusions [52], [20]. Anomaly detection approaches include statistical approaches, predictive pattern generation, and neural networks. The advantage of anomaly detection is that it is possible to detect novel attacks against systems, because it compares current activities against statistical models for past behavior, not tied with specific or pre-defined patterns. However, there are some of the weaknesses of this approach. It is likely to have high rates of false alarm. Unusual but legitimate use may sometimes be considered anomalous. Statistical measures of user profile can be gradually trained, so intruders can train such systems over a period of time until intrusive behavior is considered normal. Also, it is not able to identify the specific type of attack that is occurring. Moreover, the anomaly detection systems are computationally expensive because of the overhead of keeping track of and updating several system profile metrics.

3. Telecommunication Fraud Detection:

Neural networks have been widely used in fraud detection. Neural Networks can actually calculate user profiles in an independent manner, thus adapting more elegantly to the behavior of the various users. Neural Networks are claimed to substantially reduce operation costs. A project of the European Commission, ASPeCT, investigated the feasibility of the implementations with a rulebased approach and neural networks approach, both supervised and unsupervised approach based on data in toll tickets [55]. Three approaches were presented in [42] based on toll tickets (call records stored for billing purposes). First, a feed-forward neural network based on supervised approach is used to learn a non-linear discriminative function to classify subscribers using summary statistics. Second, density estimation with Gaussian mixture model is applied to modeling the past behavior of each subscriber and detecting any abnormalities from the past behavior. Third, Bayesian networks are used to define probabilistic models given the subscribers' behavior.

4. Terrorist Detection:

Bio-terrorism detection aims to detect irregularities in temporal data. Similar to fraud detection, data has to be partially simulated by injecting epidemics, and performance is evaluated with detection time and number of false positives. Wong *et al* [56] apply Bayesian networks to uncover simulated anthrax attacks from real emergency department data. Hutwagner *et al* [57] describe the use of cumulative sum of deviations in the Early Aberration Reporting System (EARS). Goldenberg *et al* [58] use time series analysis to track early symptoms of synthetic anthrax outbreaks from daily sales of retail medication (throat, cough, and nasal) and some grocery items (facial tissues, orange juice, and soup). Other epidemic detection papers include application of sliding linear regression to usage logs of doctors' reference database and HMMs to influenza time series.

5. Financial Crime Detection:

Financial crime here refers to money laundering, violative trading, and insider trading and the following are brief application descriptions which correspond to each type of monitoring system for the United States government. The Financial Crimes Enforcement Network AI System (FAIS) [59] operates with an expert system with Bayesian inference engine to output suspicion scores and with link analysis to visually examine selected subjects or accounts. Supervised techniques such as casebased reasoning, nearest neighbor retrieval, and decision trees were seldom used due to propositional approaches, lack of clearly labeled positive examples, and scalability issues. Unsupervised techniques were avoided due to difficulties in deriving appropriate attributes. It has enabled effectiveness in manual investigations and gained insights in policy decisions for money laundering.

The National Association of Securities Dealers' (NASD) Regulation Advanced Detection System (ADS) [60] uses a rule pattern matcher and a sequence matcher cast in two- and three- dimensional visualizations to generate breaks or leads. The rule pattern matcher detects predefined suspicious behaviors; whilst the sequence matcher finds temporal relationships between events from market data which exists in a potential violation pattern. Association rules and decision trees are used to discover new patterns or refined rules which reflect behavioral changes in the marketplace. It has been successfully used to identify and correct potential violative trading on the NASDAQ National Market. Senator [59] argues that propositional data mining approaches are not useful for the ADS.

The Securities Observation, News Analysis, and Regulation (SONAR) [58] use text mining, statistical regression, rule-based inference, uncertainty, and fuzzy matching. It mines for explicit and implicit relationships among the entities and events, all of which form episodes or scenarios with specific identifiers. It has been reported to be successful in generating breaks the main stock markets for insider trading (trading upon inside information of a material nature) and misrepresentation fraud (falsified news).

Use of large amounts of unstructured text and web data such as free-text documents, web pages, emails, and SMS messages, is common in adversarial domains but still unexplored in fraud detection literature. Zhang *et al* [61] presents Link Discovery on Correlation Analysis (LDCA) which uses a correlation measure with fuzzy logic to determine similarity of patterns between thousands of paired textual items which have no explicit links. It comprises of link hypothesis, link generation, and link identification based on financial transaction timeline analysis to generate community models for the prosecution of money laundering criminals.

V. CONCLUSION

This paper provides a comprehensive survey in fraud detection studies. It defines the adversary, the types and subtypes of fraud, the technical nature of

data, performance metrics, and the methods and techniques. After identifying the limitations in methods and techniques of fraud detection, this paper shows that this field can benefit from other related fields. Specifically, unsupervised approaches from counterterrorism work, actual monitoring systems and text mining from law enforcement, and semi-supervised approaches contribute to future fraud detection research. However, Fawcett and Provost [5] showed that there are no guarantees when they successfully applied their fraud detection method to news story monitoring but unsuccessfully to intrusion detection.

Due to the security issues, only a few approaches for credit card detection are available in public. Among them, neural networks approach is a very popular tool. However, it is difficult to implement because of lack of available data set. 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.

VI. REFERENCES

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

[2] Falcon Fraud Manager, Falcon Fraud Manager – Fair Isaac Corporation www.fairisaac.com 2008.

[3] Entrust, 2008 Entrust www.entrust.com. 2008.

[4] StreamBase, 2008 StreamBase www.streambase.co.uk (2008).

[5] Fawcett, T. & Provost, F. Adaptive Fraud Detection. *Data Mining and Knowledge Discovery* **1**(3): 291-316. 1997.

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

[7] SAS Institute. *Using Data Mining Techniques for Fraud Detection: A Best Practices Approach to Government Technology Solutions, Whitepapers*. http://www.sas.com, 1996.

[8] Foster, D. & Stine, R. Variable Selection in Data Mining: Building a Predictive Model for Bankruptcy. *Journal of American. 2004*

[9] *Statistical Association* **99**: 303-313. Ezawa, K. & Norton, S. Constructing Bayesian Networks to Predict Uncollectible Telecommunications Accounts. *IEEE Expert* **October**: 45-51. 1996.

[10] Kim, H., Pang, S., Je, H., Kim, D. & Bang, S. Constructing Support Vector Machine Ensemble. *Pattern Recognition* **36**: 2757-2767. 2003.

[11] Little, B., Johnston, W., Lovell, A., Rejesus, R. & Steed, S. Collusion in the US Crop Insurance Program: Applied Data Mining. *Proc. of SIGKDD02*, 594-598. 2002.

[12] Wheeler, R. & Aitken, S. Multiple Algorithms for Fraud Detection. *Knowledge-Based Systems* **13**(3): 93-99. 2000

[13] Barse, E., Kvarnstrom, H. & Jonsson, E. (2003). Synthesizing Test Data for Fraud Detection Systems. *Proc. of the 19th Annual Computer Security Applications Conference*, 384-395. 2003.

[14] McGibney, J. & Hearne, S. An Approach to Rules-based Fraud Management in Emerging Converged Networks. *Proc. Of IEI/IEEE ITSRS 2003*. 2003.

[15] Shao, H., Zhao, H. & Chang, G. Applying Data Mining to Detect Fraud Behaviour in Customs Declaration. *Proc. of 1st International Conference on Machine Learning and Cybernetics*, 1241-1244. 2002.

[16] Massey, K. Massey, Combating eFraud – a next generation approach, *Financial Insights* White Paper. 2005.

[17] Fair Isaac. The evolving threat of card skimming, *Fair Isaac* White Paper. 2005.

[18] Sherman, E. Fighting Web Fraud. *Newsweek* June 10. 2002.

[19] Fawcett, T. "In Vivo" Spam Filtering: A Challenge Problem for KDD. *SIGKDD Explorations* **5**(2): 140-148. 2003.

[20] Ghosh, S. & Reilly, D. Credit Card Fraud Detection with a Neural Network. *Proc. of 27th Hawaii International Conference on Systems Science* **3**: 621-630. 2004.

[21] Barse, E., Kvarnstrom, H. & Jonsson, E. Synthesizing Test Data for Fraud Detection Systems. *Proc. of the 19th Annual Computer Security Applications Conference*, 384-395. 2003.

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

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

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

[25] Ezawa, K. & Norton, S. Constructing Bayesian Networks to Predict Uncollectible Telecommunications Accounts. *IEEE Expert* **October**: 45-51. 1996.

[26] Viaene, S., Derrig, R. & Dedene, G. A Case Study of Applying Boosting Naive Bayes to Claim Fraud Diagnosis. *IEEE Transactions on Knowledge and Data Engineering* **16**(5): 612- 620. 2004.

[27] Belhadji, E., Dionne, G. & Tarkhani, F. A Model for the Detection of Insurance Fraud. *The Geneva Papers on Risk and Insurance* **25**(4): 517-538. 2000.

[28] Artis, M., Ayuso M. & Guillen M. Modelling Different Types of Automobile Insurance Fraud Behaviour in the Spanish Market. *Insurance Mathematics and Economics* **24**: 67-81. 1999.

[29] Mercer, L. Fraud Detection via Regression Analysis. *Computers and Security* **9**: 331-338. 1990.

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

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

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

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

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

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

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

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

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

[39] Cortes, C. & Pregibon, D. (2001). Signature-Based Methods for Data Streams. *Data Mining and Knowledge Discovery* **5**: 167- 182.

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

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

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

[43] Williams, G. Evolutionary Hot Spots Data Mining: An Architecture for Exploring for Interesting Discoveries. *Proc. Of PAKDD99*. 1999.

[44] Brockett, P., Derrig, R., Golden, L., Levine, A. & Alpert, M. Fraud Classification using Principal Component Analysis of RIDITs. *Journal of Risk and Insurance* **69**(3): 341-371. 2002.

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

[46] Murad, U. & Pinkas, G. Unsupervised Profiling for Identifying Superimposed Fraud. *Proc. of PKDD99*. 1999.

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

[48] Kokkinaki, A. 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. 1997

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

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

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

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

[53] S. E. Smaha and J.Winslow. Misuse detection tools. In *Computer Security Journal 10(1)*, pages 39 – 49, Spring 1994.

[54] J. Ryan, M.-J. Lin, and R. Miikkulainen. Intrusion detection with neural networks. In M. I. Jordan, M. J. Kearns, and S. A. Solla, editors, *Advances in Neural Information Processing Systems*, volume 10. The MIT Press, 1998.

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

[56] Wong, W., Moore, A., Cooper, G. & Wagner, M. Bayesian Network Anomaly Pattern Detection for Detecting Disease Outbreaks. *Proc. of ICML03*, 217-223. 2003.

[57] Hutwagner, L., Thompson, W. & Seeman, M. The Bioterrorism Preparedness and Response Early Abberation Reporting System (EARS). *Journal of Urban Health: Bulletin of the New York Academy of Medicine* **80**(2): 89-96. 2003.

[58] Goldberg, H., Kirkland, J., Lee, D., Shyr, P. & Thakker, D. The NASD Securities Observation, News Analysis \& Regulation System (SONAR). *Proc. of IAAI03*. 2003.

[59] Senator, T., Goldberg, H., Wooton, J., Cottini, M., Khan, U., Klinger, C., Llamas, W., Marrone, M. & Wong, R. The Financial Crimes Enforcement Network AI System (FAIS). *AAAI* **16**(4): Winter, 21-39. 1995.

[60] Kirkland, D., Senator, T., Hayden, J., Dybala, T., Goldberg, H. & Shyr, P. The NASD Regulation Advanced Detection System. *AAAI* **20**(1): Spring, 55-67. 1999.

[61] Zhang, M., Salerno, J. & Yu, P. Applying Data Mining in Investigating Money Laundering Crimes. *Proc. of SIGKDD03*, 747-752. 2003.