Proceedings of the 2004 IEEE
International Conference on Networking, Sensing & Control
Taipei, Taiwan, March 21-23, 2004

Survey of Fraud Detection Techniques

Yufeng Kou, Chang-Tien Lu, Sirirat Sirwongwattana
Dept. of Computer Science
Virginia Polytechnic Institute
and State University
Falls Church, VA 22043, USA
{ykou,ctlu,ssiriwon}@vt.edu

Yo-Ping Huang
Dept. of Computer Science
and Engineering
Tatung University
Taipei, Taiwan 10451
yphuang@cse.ttu.edu.tw

Abstract

Due to the dramatic increase of fraud which results in loss of billions of dollars worldwide each year, several modern techniques in detecting fraud are continually evolved and applied to many business fields. Fraud detection involves monitoring the behavior of populations of users in order to estimate, detect, or avoid undesirable behavior. Undesirable behavior is a broad term including delinquency, fraud, intrusion, and account defaulting. This paper presents a survey of current techniques used in credit card fraud detection, telecommunication fraud detection, and computer intrusion detection. The goal of this paper is to provide a comprehensive review of different techniques to detect frauds.

Keywords: Fraud detection, computer intrusion, data mining, knowledge discovery, 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]." In the technological systems, fraudulent activities have occurred in many areas of daily life such as telecommunication networks, mobile communications, on-line banking, and E-commerce. 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.

Credit Card Fraud. Credit card fraud is divided into two types: offline fraud and online fraud. Offline fraud is committed by using a stolen physical card at storefront or call center. In most cases, the institution issuing the card can lock it before it is used in a fraudulent manner. Online fraud is committed via web, phone shopping or cardholder-not-present. Only the card's details are needed, and a manual signature and card imprint are not required at the time of purchase.

Computer Intrusion. Intrusion is defined as the potential possibility of a deliberate unauthorized attempt to access information, manipulate information, or render a system unreliable or unusable. Intruders may be from an outsider (or hacker) and an insider who knows the layout of the system, where the valuable data is and what security precautions are in place. Computer intrusion can be classified into two categories: misuse intrusions and anomaly intrusions. Misuse intrusions are well-defined attacks on known weak points of a system. Anomaly intrusions are based on observations of deviations from normal system usage patterns. These include attempted break-ins, masquerade attacks, leakage, denial of service, and malicious use [4].

Telecommunication Fraud. Fraud is costly to a network carrier both in terms of lost income and wasted capacity. The various types of telecommunication fraud can be classified into two categories: subscription fraud and superimposed fraud. Subscription fraud occurs from obtain-

0-7803-8193-9/04/$17.00 ©2004 IEEE

ing a subscription to a service, often with false identity details, with no intention of paying. Cases of bad debt are also included in this category. Superimposed fraud occurs from using a service without having the necessary authority detected by the appearance of unknown calls on a bill. This fraud includes several ways, for example, mobile phone cloning, ghosting (the technology that tricks the network in order to obtain free calls), insider fraud, tumbling (rolling fake serial numbers are used on cloned handsets so that successive calls are attributed to different legitimate phones), and etc.

In general, the objective of fraud detection is to maximize correct predictions and maintain incorrect predictions at an acceptable level [29]. 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. *False Negative rate* is the percentage of fraudulent transactions that are incorrectly identified as legitimate. In a fraud detection system, it is important to define performance metrics carefully. Several fraud detection techniques use metrics like the detection rate, false alarm rate, and average time of detection. The typical fraud detection techniques attempt to maximize accuracy rate and minimize false alarm rate.

2. Credit Card Fraud Detection

Credit card fraud detection is quite confidential and is not much disclosed in public. Some available techniques techniques are discussed as follows.

Outlier Detection. An outlier is an observation that deviates so much from other observations as to arouse suspicion that it was generated by a different mechanism [19]. Unsupervised learning approach is employed to this model. Usually, the result of unsupervised learning 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. Outliers are a basic form of non-standard observation that can be used for fraud detection. 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.

Bolton and Hand proposed unsupervised credit card fraud detection, using behavioral outlier detection techniques [5]. Abnormal spending behavior and frequency of transactions will be identified as outliers, which are possible fraud cases.

Neural Networks. A neural network is a set of interconnected nodes designed to imitate the functioning of the human brain [15]. Each node has a weighted connection to several other nodes in adjacent layers. Individual nodes take the input received from connected nodes and use the weights together with a simple function to compute output values. Neural networks come in many shapes and forms and can be constructed for supervised or unsupervised learning. The user specifies the number of hidden layers as well as the number of nodes within a specific hidden layer. Depending on the application, the output layer of the neural network may contain one or several nodes.

CARDWATCH [2] features neural networks trained with the past data of a particular customer. It makes the network process the current spending patterns to detect possible anomalies. Brause and Langsdorf proposed the rule-based association system combined with the neuro-adaptive approach [6]. Falcon developed by HNC uses feed-forward Artificial Neural Networks trained on a variant of a back-propagation training algorithm [16]. Machine learning, adaptive Pattern Recognition, neural networks, and statistical modeling are employed to develop Falcon predictive models to provide a measure of certainty about whether a particular transaction is fraudulent. A neural MLP-based classifier is another example using neural networks [11]. It acts only on the information of the operation itself and of its immediate previous history, but not on historic databases of past cardholder activities. A parallel Granular Neural Network (GNN) method uses fuzzy neural network and rule-based approach [34]. The neural system is trained in parallel using training data sets, and then the trained parallel fuzzy neural network discovers fuzzy rules for future prediction. CyberSource introduces a hybrid model, combining an expert system with a neural network to increase its statistic modeling and reduce the number of "false" rejections [9].

Research Issues. It is an interesting issue to incorporate spatial information to the detection system. For example, if the orders like big furniture or cars are purchased to ship to the address that is far away from the billing address, this transaction may be considered fraud. In meta-learning

techniques for credit card fraud detection, a meta-classifier is trained on the correlation of the predictions of the base classifier [32]. It would be meaningful to define effective selection metrics for deciding best base classifiers used for meta-learning. Currently, for simplicity reasons, all the base learners for credit card fraud detection use the same desired distribution. It would be interesting to implement and evaluate the credit card fraud detection system by using very large databases with skewed class distributions and non-uniform cost per error.

3. 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.

Misuese 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 [3, 13, 14, 20–22]. Misuse approaches include expert systems, model-based reasoning, state transition analysis, and keystroke dynamics monitoring [31]. 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 [14, 23, 28]. 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.

The techniques used in misuse detection and anomaly detection are described as follows:

Expert Systems. An expert system is defined as a computing system capable of representing and reasoning about some knowledge-rich domain with a view to solving problems and giving advice [24, 30]. Expert system detectors encode knowledge about attacks as if-then rules. NIDES developed by SRI uses the expert system approach to implement intrusion detection system that performs real-time monitoring of user activity [3]. NIDES consists of statistical analysis component for anomaly detection and rule-based analysis component for misuse detection.

Neural Networks. NNID (Neural Network Intrusion Detector) is an anomaly intrusion detection system implemented by a backpropagation neural network under UNIX environment [28]. It is trained to identify users based on what commands and how often they used during a day. It is easy to train and inexpensive because it operates off-line on daily log data. ANN (Artificial Neural Networks) provides the ability to generalize from previously observed behavior (normal or malicious) to recognize similar future unseen behavior for both anomaly detection and misuse detection [14]. It is implemented by a backpropagation neural network.

Model-based Reasoning. Model-based detection is a misuse detection technique that detects attacks through observable activities that infer an attack signature. There is a database of attack scenarios containing a sequence of behaviors making up the attack. Garvey and Lunt combined models of misuse with evidential reasoning [13]. The system accumulates more and more evidence for an intrusion attempt until a threshold is crossed; at this point, it signals an intrusion attempt. A pattern matching approach based on Colored Petri Nets to detect misuse intrusion is proposed by Kumar and Spafford [22]. It uses audit trails as input under UNIX environment.

Data Mining. Data mining approaches can be applied for intrusion detection. An important advantage of data mining approach is that it can develop a new class of models to detect new attacks before they have been seen by human experts. Classification model with association rules algorithm and frequent episodes is developed for anomaly intrusion detection [23]. This approach can automatically generate concise and accurate detection models from large amount of audit data. However, it requires a large amount of audit data in order to compute the profile rule sets. Moreover, this learning process is an integral and continuous part of an intrusion detection system because the rule sets used by the detection module may not be static over a long period of time. A team of researchers at Columbia University proposed the detection models using cost-sensitive machine

learning algorithms [33]. Audit data is analyzed by association rules algorithm in order to determine static features of attack data.

State Transition Analysis. State Transition Analysis is a misuse detection technique, which attacks are represented as a sequence of state transitions of the monitored system. Actions that contribute to intrusion scenarios are defined as transitions between states. Intrusion scenarios are defined in the form of state transition diagrams. Nodes represent system states and arcs represent relevant actions. If a compromised (final) state is ever reached, an intrusion is said to have occurred. STAT(State Transition Analysis Tool) is a rule-based expert system designed to seek out known penetrations in the audit trails of multi-user computer systems [21]. USTAT (UNIX State Transition Analysis Tool) is a UNIX-specific prototype of STAT [20].

Other Techniques. A genetic algorithm [7] is applied to detect malicious intrusions and separate them from normal use. A genetic algorithm is a method of artificial intelligence problem solving based on the theory of Darwinian evolution applied to mathematical models. This genetic algorithm was designed so that each individual represented a possible behavioral model. This approach provides a high detection rate and a low false alarm rate. Dokas and Ertoz proposed building rare class predictive models for identifying known intrusions [10]. This method can address the inability of standard data mining techniques when dealing with skewed class distribution.

Research Issues. Due to the incredibly large sizes of audit data, audit trail reduction is significant to retrieve information rapidly and efficiently. Relationship between the types, amount of omission and the accuracy of detection needs to be explored in depth. An attacker may perform several actions under different user identities. Non-parametric pattern recognition is useful when the statistical distribution of the underlying data is not available. The performance of intrusion detection system could be able to adapt to the increasement of the number of users. It would be interesting to analyze the performance impact by optimizing the set of commands and the size of the value intervals when network is used by large amount of users. To reduce the false alarm rate, statistical analysis approach should be developed to distinguish important and less important alarms.

4. Telecommunication Fraud Detection

Previous work in the telecommunication fraud detection has concentrated mainly on identifying superimposed fraud. Most techniques use Call Detail Record data to create behavior profiles for the customer, and detect deviations from these profiles. These approaches are discussed as follows.

Rule-based Approach.: A combination of absolute and differential usage is verified against certain rules in the rule-based approach mapped to data in toll tickets [25]. With differential analysis, flexible criteria can be developed to detect any usage change in a detailed user behavior history. Rule-based approach works best with user profiles containing explicit information, where fraud criteria can be referred as rules. Rule-discovery methodology combining two data levels, which are the customer data and behavior data (usage characteristics in a short time frame), is proposed in [27]. A rule-set is selected by using a greedy algorithm with the adjusted thresholds. PDAT is a rule-based tool for intrusion detection developed by Siemens ZFE. Due to its flexibility and broad applicability, PDAT is used for mobile fraud detection.

Rule-based analysis can be very difficult to manage because the proper configuration of such rules requires precise, laborious, and time-consuming programming for each imaginable fraud possibility. The dynamic appearance of multiple new fraud types demands that these rules be constantly adapted to include existing, emerging, and future fraud options. Moreover, it also presents a major obstacle to scalability. The more data the system must process, the more drastic is the performance downfall.

Neural Networks. 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 rule-based approach and neural networks approach, both supervised and unsupervised learning based on data in toll tickets [25]. Three approaches were presented in [35] based on toll tickets (call records stored for billing purposes). First, a feed-forward neural network based on supervised learning 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.

Visualization Methods. Visualization techniques rely on human pattern recognition to detect anomalies and are provided with close-to-real-time data feeds. The idea is that while machine-based detection methods are largely static, the human visual system is dynamic and can easily adapt to the ever-changing techniques used by the fraudsters. Visual data mining, combining human detection with machines for greater computational capacity, is developed by building a user interface to manipulate the graphical representation of quantities of calls between different subscribers in various geographical locations in order to detect international calling fraud [8].

Other Techniques. A call-based on-line fraud detection system based on a hierarchical regime-switching model is implemented by using subscriber data from real mobile communication network [18]. The model is trained by using the EM algorithm in an incomplete data setting [17]. After EM learning, the gradient-based discriminative training is used to improve the performance. Location awareness of the mobile phone can be used to detect cellular clones within a local system and to detect roamer clones [26]. Clones, by definition, will exist at a different location from the legitimate mobile phone. Clone detection within user's current system can be recognized by "too many locations" and "impossible locations".

Research Issues. The problem of uncollectible debt in telecommunication services is addressed by using a goal-directed Bayesian network for classification, which distinguishes customers who are likely to have bad debt [12]. Since unsupervised learning does not require a priori knowledge of fraudulent data, it may be used to filter out much normal behavior so that the successive supervised learning processing load is reduced for rule-based system and neural network-based system. Exhaustive rule generation is an interesting issue for rule based approach. The advantage is that the rule-generation step will not lose any of the possible candidates for good rules, and will not require complicated mechanisms. At present, the rule selection methodology is implemented by a greedy algorithm, which requires the predefined threshold. It would be interesting to implement non-greedy rule-selection procedures, which can create a more robust selection process.

5. Conclusions

In this paper, fraud detection in three areas, credit card fraud detection, computer intrusion detection, and telecommunication is discussed. It presents the characteristics of fraud types, the need of fraud detection systems, several current fraud detection techniques, and the possibility of future works.

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.

There are other interesting areas of fraud detection, not mentioned in this paper, such as voting irregularities, criminal activities in e-commerce, insurance claims fraud, warranty fraud and abuse, and health card fraud.

References

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

[2] E. Aleskerov, B. Freisleben, and B. Rao. Cardwatch: a neural network based database mining system for credit card fraud detection. In *Proceedings of Computational Intelligence for Financial Engineering*, pages 173–200, 1997.

[3] D. Anderson, T. Frivold, A. Tamaru, and A. Valdes. Next-generation intrusion detection expert system (nides), software users manual, beta-update release. Technical Report SRI–CSL–95–07, Computer Science Laboratory, SRI International, 333 Ravenswood Avenue, Menlo Park, CA 94025-3493, May 1994.

[4] S. Axelsson. Research in intrusion-detection systems: A survey. Technical Report 98–17, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, dec 1998.

[5] R. J. Bolton and D. J. Hand. Unsupervised profiling methods for fraud detection. In *conference of Credit Scoring and Credit Control VII, Edinburgh, UK, Sept 5-7*, 2001.

[6] R. Brause, T. Langsdorf, and M. Hepp. Credit card fraud detection by adaptive neural data mining. In *Proceedings of the 11th IEEE International Conference on Tools with Artificial Intelligence*, pages 103–106, 1999.

[7] A. Chittur. Model generation for an intrusion detection system using genetic algorithms. In *Ossining High school Honors Thesis*, 2001.

[8] K. C. Cox, S. G. Eick, G. J. Wills, and R. J. Brachman. Visual data mining: Recognizing telephone calling fraud. *J. Data Mining and Knowledge Discovery*, 1(2):225–231, 1997.

[9] CyberSource company. *Credit card fraud management.* http://www.cybersource.com, 1996.

[10] P. Dokas, L. Ertoz, V. Kumar, A. Lazarevic, J. Srivastava, and P.-N. Tan. Data mining for network intrusion detection. In *Proc. NSF Workshop on Next Generation Data Mining, Baltimore, MD, November*, 2002.

[11] J. R. Dorronsoro, F. Ginel, C. Sanchez, and C. S. Cruz. Neural fraud detection in credit card operations. volume 8, pages 827–834, 1997.

[12] K. J. Ezawa and S. W. Norton. Constructing bayesian networks to predict uncollectible telecommunications accounts. *Ieee Expert-Intelligent Systems & Their Applications*, 11:45–51, 1996.

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

[14] 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.

[15] S. Ghosh and D. L. Reilly. Credit card fraud detection with a neural-network. In J. F. Nunamaker and R. H. Sprague, editors, *Proceedings of the 27th Annual Hawaii International Conference on System Science. Volume 3 : Information Systems: DSS/Knowledge-Based Systems*, pages 621–630, Los Alamitos, CA, USA, Jan. 1994. IEEE Computer Society Press.

[16] K. Hassibi. Detecting payment card fraud with neural networks. In *Business application of Neural Networks, P.J.G. Lisboa, A.Vellido, B.Edisbury Eds. Singopore: World Scientific*, 2000.

[17] Hollmn and Jaakko. *Probabilistic Approaches to Fraud Detection, Licentiate's Thesis.* Helsinki University of Technology, Department of Computer Science and Engineering, 1999.

[18] J. Hollmn and V. Tresp. Call-based fraud detection in mobile communication networks using a hierarchical regime-switching model. In *Proceedings of the 1998 conference on Advances in neural information processing systems II*, pages 889–895. MIT Press, 1999.

[19] E. Hung and D. W. Cheung. *Parallel Algorithm for Mining Outliers in Large Database.* http://citeseer.nj.nec.com/hung99parallel.html, 1999.

[20] K. Ilgun. USTAT: A real-time intrusion detection system for UNIX. In *Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy*, pages 16–28, Oakland, CA, 1993.

[21] K. Ilgun, R. A. Kemmerer, and P. A. Porras. State transition analysis: A rule-based intrusion detection approach. *Software Engineering*, 21(3):181–199, 1995.

[22] S. Kumar and E. H. Spafford. A Pattern Matching Model for Misuse Intrusion Detection. In *Proceedings of the 17th National Computer Security Conference*, pages 11–21, 1994.

[23] W. Lee and S. Stolfo. Data mining approaches for intrusion detection. In *Proceedings of the 7th USENIX Security Symposium*, San Antonio, TX, 1998.

[24] T. F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. G. Neumann, H. S. Javitz, A. Valdes, and T. D. Garvey. A Real-Time Intrusion Detection Expert System (IDES) – Final Technical Report. Technical report, SRI Computer Science Laboratory, SRI International, Menlo Park, CA, Feb. 1992.

[25] 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.

[26] S. Patel. Location identity and wireless fraud detection. In *ICPWC'97 Technical Program, Lucent technologies, Wireless Secure Communications Lab*, 1997.

[27] S. Rosset, U. Murad, E. Neumann, Y. Idan, and G. Pinkas. Discovery of fraud rules for telecommunications¦challenges and solutions. In *Proceedings of the fifth ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 409–413. ACM Press, 1999.

[28] 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.

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

[30] M. Sebring, E. Shellhouse, M. Hanna, and R. Whitehurst. Expert system in intrusion detection: A case study. In *Proceedings of the 11th National Computer Security Conference*, pages 85–91, October 1988.

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

[32] S. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. Chan. Credit card fraud detection using meta-learning: Issues and initial results, 1997.

[33] S. J. Stolfo, W. Lee, P. K. Chan, W. Fan, and E. Eskin. Data mining-based intrusion detectors: An overview of the columbia ids project. In *ACM Transactions on Information and System Security, TISSEC*, volume 3, pages 5–14, 2001.

[34] M. Syeda, Y.-Q. Zhang, and Y. Pan. Parallel granular neural networks for fast credit card fraud detection. In *Proceedings of the 2002 IEEE International Conference*, volume 1, pages 572–577, 2002.

[35] M. Taniguchi, M. Haft, J. Hollmen, and V. Tresp. Fraud detection in communication networks using neural and probabilistic methods. In *Proceedings of the 1998 IEEE International Conference in Acoustics, Speech and Signal Processing*, volume 2, pages 1241–1244, 1998.