ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

A Study on Fraud Detection Techniques: Credit Card

K.P.Thooyamani[1], R. Udayakumar[*2,]

[1]Professor, School of Computing, Bharath University, Chennai, Tamil Nadu, India

[2*]Associate Professor, Department of Information Technology, Bharath University, Chennai, Tamil Nadu, India

ABSTRACT: Many modern techniques in detecting fraud are continually evolved and applied to many business fields. Fraud detection techniques techniques involves monitoring the deeds of populations of users in order to approximate, detect, or avoid undesirable behavior Undesirable deeds is a broad term including delinquence fraud, intrusion, and account defaulting. This paper presents a study on current techniques used in credit card fraud detection techniques techniques, telecommunication fraud detection techniques techniques, and computer intrusion detection techniques. The goal is to present a complete review of different techniques to detect frauds.

KEYWORDS: Fraud detection techniques techniques , computer intrusion detection techniques , data mining, knowledge discovery, neural networks.

1. INTRODUCTION

The Association of Certified Fraud Examiners (ACFE) defined the term fraud as "the use of one's profession for personal enrichment through the conscious misuse or application of the employing organization's resources or assets [1]." In the hi-tech systems, fraudulent activities have occurred in numerous areas of daily life such as mobile communications, telecommunication networks, E-commerce and on-line banking. Fraud is increasing with the expansion of modern technology and global communication, resulting in substantial losses to the businesses. certainly, fraud detection techniques has become an important issue to be explored. Fraud detection techniques techniques involves identifying fraud as quickly as possible once it has been identified. Fraud detection techniques techniques are continuously developed to preserve the criminals in adapting to their strategies. Development of new fraud detection techniques methods is made more difficult due to the severe limitation of the exchange of ideas in fraud detection techniques[2]. The fraud cases have to be detected from the available huge data sets as the logged data and user behavior. Fraud is discovered from anomalies in data and patterns. The types of frauds in this paper include credit card frauds, telecommunication fraud techniques, and computer intrusion. Credit Card Fraud. Credit card fraud is divided into two types:1. offline fraud 2. online fraud. The Offline fraud is committed by using a stolen physical card at storefront.Online fraud is committed via web, phone shopping or card h older- not-present. Only the card's details are needed, and a manual signature and card imprint are not required at the time of purchase[3]. 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. Computer intrusion can be classified into two categories: misuse intrusions and anomaly intrusions. Misuse intrusions are attacks on well-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 different types of telecommunication fraud can he classified into two categories: subscription fraud and superimposed fraud. contribution fraud occurs from obtaining a subscription to a service, often with false identity de- tails, with no intention of paying. Fraud catching 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. The typical fraud detection techniques techniques attempt to exploit accuracy rate and minimize false alarm rate.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

II. CREDIT CARD FRAUD DETECTION TECHNIQUES

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

Outlier Detection. Outlier is an observation that deviates so much from other observations as to arouse suspicion that it was generated by a different mechanism . Unsupervised learning method **is** employed to this model.
generally, the result of unsupervised learning **is** a new explanation or representation of the observation data, which will then lead to improved future decisions. Unsupervised approaches do not need the prior knowledge of fraudulent and non-fraudulent transactions in historical database, but instead detect changes in performance or unusual transactions. These approaches model a baseline distribution that represents normal behavior and then detect observations that show best departure from this standard. Outliers are a basic form of non-standard observation that can be used for fraud detection techniques techniques. In supervised approaches, models are trained to discriminate between fraudulent and non-fraudulent behavior so new observations can be assigned to classes. This approach 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 techniques, 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 **[13].** 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 [12]. 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 [1 I]. 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 rulebasedapproach [34]. The neural system ***is*** trained in parallelusing 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

III. 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: mis**use** 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 [7]. Misuse approaches include expert systems, model-based reasoning, state transition analysis, and keystroke dynamics monitoring. Since specific attack sequences are encoded into misuse

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

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. Anomaly detection approaches include statistical approaches, predictive pattem 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 bed 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 anoma**lous.** 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 occuning. 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. 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. "ID (Neural Network Intrusion Detector) is an anomaly intrusion detection system implemented by a back propagation 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 [10]. It is implemented by a hack propagation 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 . 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. 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 pat? of an intrusion detection system because the rule sets used by the detection module may not he static over a long period of time. A team of researchers at Columbia University proposed the detection models using cost-sensitive machine learning algorithms [9]**.** 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**.** USTAT (UNIX State Transition Analysis Tool) is a UNIX-specific prototype of STAT**.**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

IV. TELECOMMUNICATION FRAUD DETECTION TECHNIQUES

Previous work in the telecommunication fraud detection techniques 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 rulebasedapproach mapped to data in toll tickets **.** 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 **.** 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 techniques[8]. Rule-based analysis can be very difficult to manage because the propcr configuration of such rulcs rcquircs 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 techniques. 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 **.** Three approaches were presented in 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 hy 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 techniques system based on a hierarchical regime-switching model is implemented by using subscriber data from real mobile communication network [IS]. The model is trained by using the EM algorithm in an incomplete data setting . 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 . 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 **'Yo0** many locations" and "impossible
locations".

V. CONCLUSIONS

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

detection techniques systems, several current fraud detection techniques 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 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 ***fol***low 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 techniques, 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] Investigoting Fraudulent Acfi, UNIVERSITY OF HOUSTON SYSTEM ADMNISTRATNE MEMOh!ANDUM. http://www.uhsa.uh.edu/samiAM/01C04.hhll, 2000.
[2] Saravanan, T., Srinivasan, V., Udayakumar, R., "A approach for visualization of atherosclerosis in coronary artery", Middle - East Journal of Scientific Research, ISSN : 1990-9233, 18(12) (2013) pp. 1713-1717.
[3] E. Aleskerov, B. Freisleben, and B. Rao. Cardwatch aneural network based database mining system for credit card fraud detection techniques. In Pmceedings of Computational Intelligence for Financial Engineering, pages 173-200,1997,
[4] Srinivasan V., Saravanan T., "Analysis of harmonic at educational division using C.A. 8332", Middle - East Journal of Scientific Research, ISSN : 16(12) (2013) pp.1768-1773
[5] D. Anderson, T. Frivold, A. Tamaru, and A. Valdes. Nextgeneration intrusion detection experf system (nides), software users manual, beta-update release. Technical Report
SRIXSL-9547, Computer Science Laboratory, SRI International, 333 Ravenswwd Avenue, Menlo Park, CA 94025- 3493, May 1994.
[6] Srinivasan V., Saravanan T., "Reformation and market design of power sector", Middle - East Journal of Scientific Research, ISSN : 16(12) (2013) pp. 1763-1767.
[7] 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.
[8] Srinivasan V., Saravanan T., Udayakumar R., "Specific absorption rate in the cell phone user's head", Middle - East Journal of Scientific Research, ISSN : 1990-9233, 16(12) (2013) pp.1748-1750.
[9] R. J. Bolton and D. J. Hand. Unsupervised profiling methods
for fraud detection techniques. In conference of Credit Scoring and Credit Connol VII, Edinburgh. UK, Sept 5-7,2001.
[10] R. Brause, T. Langsdorf, and M. Hepp. Credit card fraud detection techniques by adaptive neural data mining. In Proceedings of the I l t h IEEE International Conference on Tools with Am$ cia/ Intelligence, pages 103-106, 1999.
[11]Srivatsan P., Aravindha Babu N.,"Mesiodens with an unusual morphology and multiple impacted supernumerary teeth in a non-syndromic patient", Indian Journal of Dental Research, ISSN : 0970-9290, 18(3) (2007) pp. 138-140
[12] A. Chittur. Model generation for an intrusion detection system using genetic algorithms. In Ossining High schoolHonors Thesis, 2001.
[13] Vijayaragavan, S.P., Karthik, B., Kiran Kumar, T.V.U., "A DFIG based wind generation system with unbalanced stator and grid condition", Middle - East Journal of Scientific Research, v-20, i-8, pp:913-917, 2014.
[14] Thooyamani, K.P., Khanaa, V., Udayakumar, R., "Wireless cellular communication using 100 nanometers spintronics device based VLSI", Middle - East Journal of Scientific Research, v-20, i-12, pp:2037-2041, 2014.
[15] Vanangamudi, S., Prabhakar, S., Thamotharan, C., Anbazhagan, R., "Dual fuel hybrid bike", Middle - East Journal of Scientific Research, v-20, i-12, pp:1819-1822, 2014.
[16] Udayakumar, R., Kaliyamurthie, K.P., Khanaa, Thooyamani, K.P., "Data mining a boon: Predictive system for university topper women in academia", World Applied Sciences Journal, v-29, i-14, pp:86-90, 2014.
[17] Satheesh, S., Lingeswaran, K., "High efficiencytransformer less inverter for single-phase photovoltaic systems using switching converter", Middle - East Journal of Scientific Research, v-20, i-8, pp:956-965, 2014.