ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/345260528

Neural Network in Fraud Detection

Conference Paper · August 2011

CITATIONS
0

READS
1,318

2 authors:

Suvendra Kumar Jayasingh
Biju Patnaik University of Technology
26 PUBLICATIONS **69** CITATIONS
SEE PROFILE

Anil Kumar Swain
9 PUBLICATIONS **12** CITATIONS
SEE PROFILE

All content following this page was uploaded by Suvendra Kumar Jayasingh on 04 November 2020.

The user has requested enhancement of the downloaded file.

Neural Network in Fraud Detection

Suvendra Kumar Jayasingh
Lecturer in Computer Science
Institute of Management And Information Technology (I.M.I.T.), Cuttack
Biju Patnaik University of Technology, Odisha
sjayasingh@gmail.com

Anil Kumar Swain
Asst. Professor in Computer Science & Engineering
Hi-Tech College of Engineering (HCE), Bhubaneswar
Biju Patnaik University of Technology, Odisha
anilkumarswain@gmail.com

Abstract-The purpose of the paper is to test the use of artificial neural networks (ANNs) as a tool in fraud detection. Utilizing exogenous and endogenous factors as input variables to ANNs and in developing seven different models, an average of 90 per cent accuracy was found in the fraud detection prediction model. It has, therefore, been demonstrated that ANNs can be used by auditors to identify fraud-prone companies. Whilst previous researchers have looked at empirical predictors of fraud, fraud risk assessment methods and mechanically fraud risk assessment methods, no other research has combined both exogenous and endogenous factors in developing ANNs to be used in fraud detection. Thus, auditors can use ANNs as complementary to other techniques at the planning stage of their audit to predict if a particular audit client is likely to have been victimized by a fraudster. Fraud detection is a continuously evolving discipline and requires a tool that is intelligent enough to adapt to criminals strategies and ever changing tactics to commit fraud. Despite the best efforts of the FBI and other law enforcement organizations, fraud still costs American companies an overwhelming $400 billion [2] each year. With the relatively recent growth of the Internet into a global economic force, credit card fraud has become more prevalent. It is in a company and card issuer's interest to prevent fraud or, failing this, to detect fraud as soon as possible. Otherwise consumer trust in both the card and the company decreases and revenue is lost, in addition to the direct losses made through fraudulent sales. The prevention of credit card fraud is an important application for prediction techniques. One major obstacle for using neural network training techniques is the high necessary diagnostic quality: Since only one financial transaction of a thousand is invalid no prediction success less than 99.9% is acceptable. Due to these credit card transaction proportions complete new concepts had to be developed and tested on real credit card data. This paper shows how advanced data mining techniques and neural network algorithm can be combined successfully to obtain a high fraud coverage combined with a low false alarm rate.

Index Terms- *Artificial Neural Network, Data Mining, Sentinel, Neural Fraud Management System, Knowledge Discovery in Databases, Automatic Modeling System, Falcon Fraud Manager*

I. INTRODUCTION

The prediction of user behavior in financial systems can be used in many situations. Predicting client migration, marketing or public relations can save a lot of money and other resources. One of the most interesting fields of prediction is the fraud of credit lines, especially credit card payments[5]. For the high data traffic of 400,000 transactions per day, a reduction of 2.5% of fraud triggers a saving of one million dollars per year. Certainly, all transactions which deal with accounts of known misuse are not authorized. Nevertheless, there are transactions which are formally valid, but experienced people can tell that these transactions are probably misused, caused by stolen cards or fake merchants. So, the task is to avoid a fraud by a credit card transaction before it is known as "illegal". With an increasing number of transactions people can no longer control all of them. As remedy, one may catch the experience of the experts and put it into an expert system. This traditional approach has the disadvantage that the expert's knowledge, even when it can be extracted explicitly, changes rapidly with new kinds of organized attacks and patterns of credit card fraud. In order to keep track with this, no predefined fraud models but automatic learning algorithms are needed. This paper deals with the problems specific to this special data mining application and tries to solve them by a combined probabilistic and neuro-adaptive approach for a given data base of credit card transactions.

II. DETECTING FRAUD

Traditional ways of data analysis have been in use since long time as a method of detecting fraud. They require complex and time-consuming investigations that deal with different domains of knowledge like financial, economics, business practices and law. Fraud often consists of many instances or incidents involving repeated transgressions using the same method. Fraud instances can be similar in content and appearance but usually are not identical. The first industries to use data analysis techniques to prevent fraud were the telephony companies, the insurance companies and the banks. One early example of successful implementation of data analysis techniques in the banking industry is the Falcon fraud assessment system, which is based on a neural network shell. Retail industries also suffer from fraud at Point Of Sale (POS). Some supermarkets have started to make use of digitized closed-circuit television (CCTV) together with POS data of most susceptible transactions to fraud. Internet transactions have recently raised big concerns. Kerr (2002) shown that internet transaction fraud is 12 times higher than in-store fraud. Fraud that involves cell phones, insurance claims, tax return claims, credit card transactions etc represent significant problems for governments and businesses, but yet detecting and preventing fraud is not a simple task[7]. Fraud is an adaptive crime, so it needs special methods of intelligent data analysis to detect and prevent it. These methods exist in the areas of Knowledge Discovery in

ISBN : 978-93-81361-22-1 Excel Publishers, New Delhi

Databases (KDD), Data Mining, Machine Learning and Statistics. They offer applicable and successful solutions in different areas of fraud crimes.

Fraud occurs in the following areas:

- Credit Card Fraud
- Internet Transaction Fraud / E-Cash fraud
- Insurance Fraud and Health Care Fraud
- Money Laundering
- Intrusion into computers or computer networks
- Telecommunications Fraud
- Voice Over IP (VOIP) Fraud
- Subscription Fraud / Identity Theft

III. WHY TO USE NEURAL NETWORK

Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques. A trained neural network can be thought of as an "expert" in the category of information it has been given to analyse. This expert can then be used to provide projections given new situations of interest and answer "what if" questions. Other advantages include:

1. Adaptive learning: An ability to learn how to do tasks based on the data given for training or initial experience.
2. Self-Organisation: An ANN can create its own organisation or representation of the information it receives during learning time.
3. Real Time Operation: ANN computations may be carried out in parallel, and special hardware devices are being designed and manufactured which take advantage of this capability.
4. Fault Tolerance via Redundant Information Coding: Partial destruction of a network leads to the corresponding degradation of performance. However, some network capabilities may be retained even with major network damage.

IV. FRAUD DETECTION USING NURAL NETWORK

Although there are several fraud detection technology exist based on Data mining, Knowledge Discovery and Expert System etc. but all these are not capable enough to detect the fraud at the time when fraudulent transaction are in progress due to very less chance of a transaction being fraudulent .It has been seen that Credit card fraud detection has two highly peculiar characteristics. The first one is obviously the very limited time span in which the acceptance or rejection decision has to be made. The second one is the huge amount of credit card operations that have to be processed at a given time. To just give a medium size example, millions of Visa card operations take place in a given day, 98% of them being handled on line. Of course, just very few will be fraudulent (otherwise, the entire industry would have soon ended up being out of businesses), but this just means that the haystack where these needles are to be found is simply enormous.

A. Working principle

Neural network based fraud detection is based totally on the human brain working principal. Neural network technology has made a computer capable of think. As human brain learn through past experience and use its knowledge or experience in making the decision in daily life problem the same technique is applied with the credit card fraud detection technology[2]. When a particular consumer uses its credit card, there is a fix pattern of credit card use , made by the way consumer uses its credit card. Using the last one or two year data neural network is train about the particular pattern of using a credit card by a particular consumer. As shown in the figure the neural network are train on information regarding to various categories about the card holder such as occupation of the card holder, income, occupation may fall in one category, while in another category information about the large amount of purchased are placed, these information include the number of large purchase, frequencies of large purchase, location where these kind of purchase are take place etc. within a fixed time period. In spite of pattern of credit card use neural network are also trained about the various credit card fraud face by a particular bank previously. Based on the pattern of uses of credit card, neural network make use of prediction algorithm on these pattern data to classify that weather a particular transaction is fraudulent or genuine. When credit card is being used by unauthorized user the neural network based fraud detection system check for the pattern used by the fraudster and matches with the pattern of the original card holder on which the neural network has been trained, if the pattern matches the neural network declare the transaction ok.

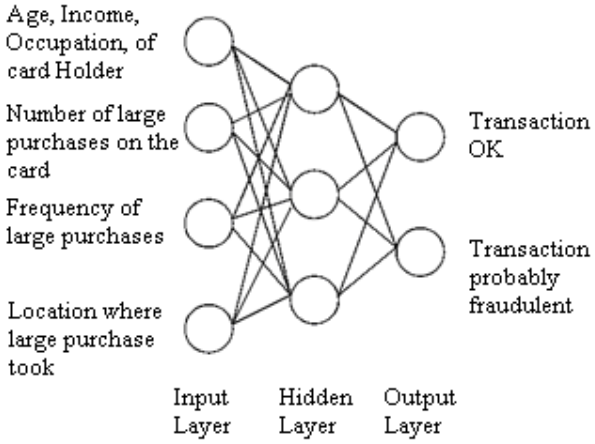

***Figure 1**: Layer of Neural Network in Credit Card*

When a transaction arrives for authorization, it is characterized by a stream of authorization data fields that carry information identifying the cardholder (account number) and characteristics of the transaction (e.g., amount, merchant code). There are additional data fields that can be taken in a feed from the authorization system (e.g., time of day). In most cases, banks do not archive logs of their authorization files. Only transactions that are forwarded by the merchant for settlement are archived by the bank's credit card processing system. Thus, a data set of transactions was

composed from an extract of data stored in Bank's settlement file. In this extract, only that authorization information that was archived to the settlement file was available for model development.

B. Fraud Detection

Matching the pattern does not mean that the transaction should exactly match with the pattern rather the neural network see to what extent there exist difference if the transaction is near by the pattern then the transaction is ok otherwise if there is a big difference then the chance of being a transaction illegal increases and the neural network declares the transaction a fault transaction[4]. The neural network is designed to produce output in real value between 0 and 1 .If the neural network produces output that is below .6 or .7 then the transaction is ok and if the output is above .7 then the chance of being a transaction illegal increases. There are some occasions when the transaction made by a legal user is of a quite difference and there are also possibilities that the illegal person made use of card that fit into the pattern for what the neural network is trained. Although it is rare, yet if the legal user can't complete a transaction due to these limitation then it is not much about to worry But what about the illegal person who is making use of card , here also works human tendency to some extent when a illegal person gets a credit card he is not going to make use of this card again and again by making number of small transaction rather he will try to make as large purchase as possible and as quickly that may totally mismatch with the pattern for what the neural network is trained. In the design of neural network-based pattern recognition systems, there is always a process of business (e.g., jewelry store, consumer electronics, restaurant, hotel, etc.) History descriptors contain features characterizing the use of the card for transact-ions and the payments made to the account over some immediately prior time interval. Other descriptors can include such factors as the date of issue (or most recent reissue) of the card. This can be important for the detection of NRI (non-receipt of issue) fraud.

V. CASE STUDY AND DISCUSSION

For the analysis, a sample set of 5,850 fraud transactions and 542,858 legal transactions were taken, ordered by their time stamps. It should be noted that the data mining algorithm has a high runtime complexity. Therefore, only 30,000 of the legal transactions were used. The resulting values for the confidence were compared to the whole set of transactions. In the following Figure 2, the performance of the rule diagnosis is shown as function of the generalization level.

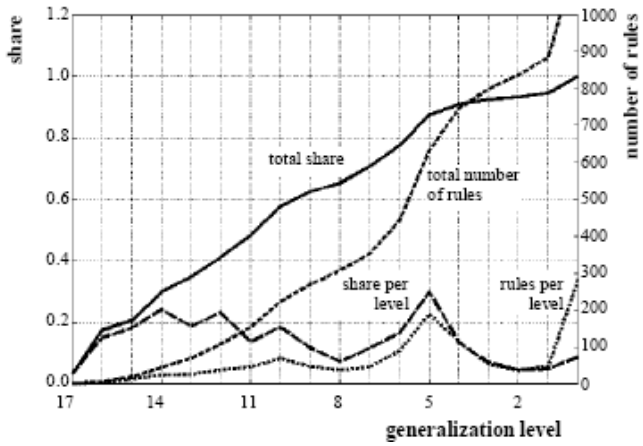

Figure 2 *The Performance of the Rule Diagnosis*

For each generalization level, i.e. for each number of wildcards, a set of active, non-generalized rules exists. They are denoted as "rules per level". Each set detects a certain part of the fraud, measured as "share per level". We can see that the main part of the share and the rules are obtained for level 5 and above. Certainly, the more rules we take the better we perform. But, the less general the rules are, the more the performance will depend on statistical variations of the fraud data. If we take all the 747 rules from generalization level 4 up to level 17 we obtain a moderate confidence for the fraud detection on the set of all transactions, see Table 1.

#rules	% Correct Diagnosis			Confidence%
	Legal	Fraud	Total	
747	99.73	90.91	99.64	25.14
510	99.97	83.08	99.79	75.17
0	*99.9*	*0.0*	*99.9*	*0.0*

Table 1 *Fraud detection vs. confidence*

However, when we select only those rules which also preserve their confidence sufficiently on the whole transaction set, we obtain 510 rules. Certainly, with less rules the fraud diagnosis probability decreases slightly, but, as we see in the table, our main goal, the confidence in the diagnosis, is dramatically increased up to 75 % due to the high proportion of legal data which are less misclassified. This is also true when we use the real proportion for legal vs. misuse transactions of 1000:1 which are shown in round brackets in Table 1. Additionally, the diagnosis performance is even better than the constant, "stupid" diagnosis mentioned before and noted in the last table row.

"Credit card fraud - Alive & Well in Australia"

Unfortunately credit card fraud is a fact-of-life for all merchants who accept credit card payments as part of their business operation. With the increasing transition to online merchandising via the Internet, online credit card fraud is a serious issue. A business requires a sound order-confirmation-system if one wants to avoid getting 'ripped-off', being subject to bank 'charge-backs' and/or constantly arranging refunds for fraudulent transactions.

Fortunately there is a simple 1-2-3 Step process that will almost guarantee us of success in avoiding being the victim of

online credit card fraud. In almost a decade of accepting credit cards online, our company has avoided falling prey to the credit card scammers (even though we average 2 - 10 fraudulent attempts per month).

Prevention Method	Never	Rarely	Some-times	Mostly	Always
Phone or Email the customer to confirm order		5%	42%	4%	44%
Check customer details in phone directory	25%	24%	24%	3%	24%
Reject suspicious orders	25%	24%	24%	3%	25%

Method of avoiding online credit card fraud

1. Confirm ALL orders via email, and request telephone and street address details
2. Do not accept transactions from web-based email addresses, eg. Hotmail, Yahoo, Gmail, etc. press the 'customer' for their ISP email account, eg. name@bigpond.com, name@ozemail.com.au, etc.
3. Contact the bank's merchant support people if one has the slightest doubt about a transaction, they are there to help us and would much rather have one seeks their assistance prior to initiating a 'mini-disaster'.

Table 2 *Credit Card Fraud Cases reported in 2010*

Australian credit card fraud statistics

The information of Table 2 is taken from the Australian Institute of Criminology and summarizes credit card fraud cases reported in 2010 and refers to ALL credit card fraud, not just online transactions (more info from AIC)[11]. As one can see below, less than half of credit card merchants even bother to do any verification.

Manual fraud prevention techniques, similar to the 3 Step Plan, are VERY effective, but one must apply them to all transactions that are not from a trusted customer. Manual screening of orders prior to sending the goods can save the aggravation, financial loss, etc.

VI. TECHNIQUES USED FOR FRAUD DETECTION

Techniques used for fraud detection fall into two primary classes: statistical techniques and artificial intelligence. Examples of statistical data analysis techniques are:

- Data preprocessing techniques for detection, validation, error correction, and filling up of missing or incorrect data.
- Calculation of various statistical parameters such as averages, quantiles, performance metrics, probability distributions, and so on. For example, the averages may include average length of call, average number of calls per month and average delays in bill payment.
- Models and probability distributions of various business activities either in terms of various parameters or probability distributions.
- Computing user profiles.
- Time-series analysis of time-dependent data.
- Clustering and classification to find patterns and associations among groups of data.
- Matching algorithms to detect anomalies in the behavior of transactions or users as compared to previously known models and profiles. Techniques are also needed to eliminate false alarms, estimate risks, and predict future of current transactions or users.

Fraud management is a knowledge-intensive activity. The main AI techniques used for fraud management include:

- Data mining to classify, cluster, and segment the data and automatically find associations and rules in the data that may signify interesting patterns, including those related to fraud.
- Expert systems to encode expertise for detecting fraud in the form of rules.
- Pattern recognition to detect approximate classes, clusters, or patterns of suspicious behavior either automatically (unsupervised) or to match given inputs.
- Machine learning techniques to automatically identify characteristics of fraud.
- Neural networks that can learn suspicious patterns from samples and used later to detect them.

VII. HOW DO NEURAL NETWORKS HELP IN FRAUD DETECTION

The inherit nature of neural networks is the ability to learn is being able to capture and represent complex input/output relationships. The motivation for the development of neural network technology stemmed from the desire to develop an artificial system that could perform "intelligent" tasks similar to those performed by the human brain. Neural networks resemble the human brain in the following two ways: [4]

1. A neural network acquires knowledge through learning.
2. A neural network's knowledge is stored within inter-neuron connection strengths known as synaptic weights. The true power and advantage of neural networks lies in their ability to represent both linear and non-linear relationships and in their ability to learn these relationships directly from the data being modelled. Traditional linear models are simply inadequate when it comes to modelling data that contains non-linear characteristics.

VIII. WHAT IS SENTINEL

Sentinel is a complete solution designed to prevent, detect, analyze and follow up banking fraud in any entity or corporation in the financial business. Specific fraud detection solutions may include:

- Credit
- Debit
- ATM

With Sentinel one company can monitor the activities of accounts, cardholders and merchants by using a robust and powerful technology based on rules, parameters and indicators. In other words, one can obtain immediate results from the moment one installs the software[9].

Sentinel allows us to:

- Process data from any origin, whether it comes from transactions, merchants or cardholders.
- Monitor issuer, acquirer or banking activities.
- Examine information by strategic business units such as countries, regions, banks, etc.
- Analyze data from a managerial perspective, through a technology known as "Business Intelligence."
- Evaluate the performance of the rules created in the system and the profit generated by them.
- Minimize risk and loss due to banking fraud.

IX. WHAT IS NEURAL FRAUD MANAGEMENT SYSTEMS (NFMS)

The Neural Fraud Management System is a completely automated and state-of-the-art integrated system of neural networks, Fraud Detection Engine, Automatic Modeling System (AMS), supervised clustering, and system retune.

Combined with Sentinel the Neural Fraud Management System (NFMS) can automatically scale the relative importance of fraud to non-fraud, group symbols to reduce dimensionality, and evolve over time to detect new patterns and trend types in frauds[3].

By adding the intelligence of neural network technology to an already successful rule-based system, one can increase the detection of legitimate fraud transactions up to 80% with as low as 1% false detections or less!

X. HOW DOES NFMS WORK

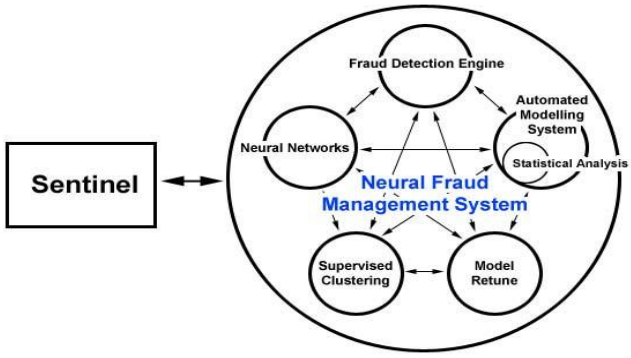

Figure 3 *Working Principle of NFM*

- The Neural Networks are completely adaptive able to learn from patterns of legitimate behavior and adapting to the evolving of behavior of normal transactions and patterns of fraud transactions and adapting to the evolving of the behavior of fraud transactions. The recall process of the Neural Networks is extremely fast and can make decisions in real time.
- Supervised Clustering uses a mix of traditional clustering and multi-dimensional histogram analysis with a discrete metric. The process is very fast and can make decisions in real time.
- Statistical Analysis ranks the most important features based on the joint distribution per transaction patterns. In addition, it finds the optimal subset of features and symbols with maximum information and minimum redundancy[9].
- The Fraud Detection Engine can apply the generated model by AMS on input data stream and output the detection results by specified model: Neural Networks, Clustering, and Combined. The Fraud Detection Engine supports both Windows and UNIX platforms.
- Retuning the basic model created by AMS to adapt to the recent trend of both the legitimate behavior and fraud behavior and update the model for Fraud Detection Engine.
- The Automatic Modeling System (AMS) chooses the important inputs and symbols, train and create clustering and neural network models.

XI. NEURAL FRAUD DETECTORS CONSTRUCTION AND TESTING

Visa security incorporates Fair Isaac's Falcon Fraud Manager, a neural network platform that utilizes sophisticated fraud risk scoring to capture relationships and patterns often missed by traditional fraud detection methods. This advanced system allows us to design customized anti-fraud strategies to successfully detect and avoid fraudulent activity[8]. The

system also provides operational and statistical reports to help us measure the success of the anti-fraud program.

Primary system components include:

a. **Falcon Debit**. In conjunction with the Visa authorization system, the Falcon Debit scoring engine uses complex statistical models to calculate a fraud score for each transaction. If the score indicates a high probability of fraud, the system can create and send a fraud case to an analyst for review, block subsequent transaction attempts, or both. The fraud score also may be used to make real-time authorization decisions.

b. **Falcon Expert**. Falcon Expert provides the ability to define rules for automated fraud prevention protocols. This customizable feature allows the addition of other relevant transaction data fields, in addition to the fraud score, when determining fraud actions.

c. **Flash Fraud Rules**

Flash Fraud Rules provide a parameter-driven set of rules to help catch and block suspect transactions falling into specific risk categories. Flash Fraud Rules are temporary rules to catch isolated fraud and stop authorization requests prior to approval. They may be used alone or in conjunction with Falcon.

The following fields may be used to block fraudulent transactions: [5]

- Merchant country code
- Merchant category code
- Merchant ZIP code
- Acquiring network ID
- PAN entry mode
- Transaction amount range
- CVV checked indicator
- CVV result
- BIN
- Prior Falcon score
- Visa Advanced Authorization Risk Score or Risk Condition Code
- Visa CAMS alert ID

d. **Call Center Services**

Fraud Call center services.

Visa Cardholder Support Services (CSS) offers a high quality, turnkey fraud call center solution for financial institutions using Falcon Fraud Manager. At one's option, one may use CSS support around the clock (full-service plan) or part-time (shared-service plan)[11]. Whichever option we choose, Visa fraud analysts monitor the fraud scores, notify cardholders of suspicious activity, and respond to cardholders' inquiries related to their fraud situations. Visa fraud analysts monitor suspicious transaction activity and, based on rules defined by the financial institution and fraud scores, call the cardholders if they suspect unauthorized use[10]. If a cardholder is unavailable when a fraud analyst calls, the analyst leaves a message including a toll-free number, unique to the financial institution, to encourage a return call. Analysts also work proactively to block confirmed fraudulent or high-risk transactions, helping to minimize fraud losses.

Hot card/card activation services.

In addition, CSS supports hot card using and card activation services. CSS can accept lost/stolen card notifications and card activation requests 24/7 from the cardholders. Around-the-clock hot carding helps protect the cardholders and financial institution from potential fraudulent activity. Full-time Voice Response Unit (VRU) capabilities enable cardholders to activate their new or reissued cards whenever it's most convenient for them.

e. **Authorization Services**

Authorizations edit checks

Risk edits and authorization processing options help reduce the fraud exposure. Edit checks may be set at the financial institution, card group, or individual cardholder level[2]. One may set limits separately for cash and POS activity, and timeframes may be set for single- or multiple-day periods[6].

Visa Fraud Protection Programs

For greater card program protection and reduced fraud, these programs validate additional data in the authorization message:

- **Cardholder Verification Value (CVV)**. Validates a unique three-digit code on the magnetic stripe of all cards to detect counterfeit or re-encoded cards.
- **Cardholder Verification Value 2 (CVV2)**. Verifies a unique value, printed on the reverse side of the card, to reduce fraudulent card-not-present transactions.
- **Dynamic Cardholder Verification Value (DCVV)**. Validates a dynamic three-digit code provided by the chip on a contactless card to detect fraud.

- **Address Verification Service (AVS)**. Enables merchants to confirm a cardholder's billing address to prevent fraud in the card-not-present environment.

Verified by Visa (VbV)

VbV makes Internet purchases safer by authenticating a cardholder's identity in real time during an online Visa card transaction. Cardholders are asked to enter a password to validate their identity during the authorization process.

Visa Advanced Authorization

Visa Advanced Authorization, an enhancement to the Visa Net authorization message, is a risk evaluation system that provides risk information directly for 100 percent of Visa Net-processed authorizations (initiated with a U.S.-issued Visa card). Robust risk information enables us to make real-time decisions that can potentially stop losses with the first transaction[12]. Visa Debit Processing Service has developed fraud rules to stop activity based on Visa Advanced Authorization scores.

Stand-in processing

Visa authorizes transactions on behalf of the host system when it is unavailable or when one has chosen Visa to process a certain transaction on its behalf. Before authorizing a transaction, Visa reviews the cardholder file, the specified limits, and the transaction data check options to handle the transaction according to the specifications[10].

Suspect activity reporting

A suite of reports can help identify excessive or abnormal cardholder activity levels. Configurable reports can monitor transaction counts and dollar limits for single- or multiple-day periods.

XII. ADVANTAGES

- Significantly reduces losses due to fraud.
- Identify new fraud methods to reduce fraud losses and minimize false positives.
- It can work in real time, online or batch modes.
- Reinforce customer trust.
- Improve operational efficiencies.
- The system could develop better models by customizing the model to the Banks unique environment.
- Build and update models as the new business requirements or changes in the environment.
- The system gives us the flexibility to easily incorporate data from many sources to the neural models.
- One has the ability to build one's own custom model, in house, without being an expert in AI programming. The final user could use the wizard-based interface to create new models or change the existing ones.
- Combine multiple Artificial Intelligence technologies to identify suspicious activity (clustering, neural networks, rules, profiles).
- It provides all life cycle to avoid fraud, including the stages: monitoring, preventing, detecting, registering, learning, self building.
- Boosts analyst productivity and improves effectiveness of fraud operations.
- Non intrusive implementation and easy to integrate with standard protocols: XML, SOAP / Web Services. Additionally NFMS provides API to enable an easy integration in the Bank environment if necessary.

XIII. CONCLUSION

Using data from a credit card issuer, a neural network based fraud detection system was trained on a large sample of labeled credit card account transactions and tested on a holdout data set that consisted of all account activity over a subsequent two-month period of time. The neural network was trained on examples of fraud due to lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud and NRI (non-received issue) fraud[9]. The network detected significantly more fraud accounts (an order of magnitude more) with significantly fewer false positives (reduced by a factor of 20) over rule-based fraud detection procedures. We discuss the performance of the network on this data set in terms of detection accuracy and earliness of fraud detection. The system has been installed on an IBM 3090 at Mellon Bank and is currently in use for fraud detection on that bank's credit card portfolio. Fraud is a million dollar business and it is increasing every year. The PwC global economic survey 2007 suggests that close to 50% of companies worldwide reported fallen victim to fraud in the past two years. Fraud involves one or more persons who intentionally act secretly to deprive another of something of value, for their own benefit. Fraud is as old as humanity itself and can take an unlimited variety of different forms. However, in recent years, the development of new technologies has also provided further ways in which criminals may commit fraud (Bolton and Hand 2002)[15]. In addition to that, business reengineering, reorganization or downsizing may weaken or eliminate control, while new information systems may present additional opportunities to commit fraud.

XIV. REFERENCES

[1] David J. Montana, "Neural Network Weight Selection Using Genetic Algorithms" Bolt Beranek and Newman Inc. July 2003

[2] Erik Bothelius, "Fraud detection in the Internal Account System for Payment Service Providers." May 8 2005

[3] Mubeena Syeda, YanQing and Yi-Pan, "Parallel Granular Network for Credit Card Fraud Detection", IEEE 2002

[4] Rajesh Parekh, Jihoon Yang and VasantHonavar, "Constructive Neural Network Learning Algorithms for Pattern Classification" IEEE 2000.
[5] The New England Debit Card Task Force, "Best Practice Guide for Managing Debit Card Fraud" IEEE July 2005.
[6] Philip K. Chan, Wei Fan, Andres L. Prodromidis and Salvatore J, " Distributed Data Mining in Credit Card Fraud Detection" IEEE December 1999.
[7] Fawcett T. And Provost F.(1997). Adaptive fraud detection Journal of Data Mining and Knowledge Discovery 1(3) 291-316
[8] Dong, W., Quan-yu, W., Shou-yi,Z., Feng-xia,L., Da-zhen,W.(2004). A Feature Extraction Method for Fraud Detection in Mobile Communication Networks, Proceedings of 5th World Congress on Intelligent Control and Automation, pp.1853-1856
[9] Bolton R.J. and Hand D.J.(2002). Statistical Fraud Detection: a review. Statistical Science, 17(3):235-255
[10] Hoath, P.(1998). Telecoms fraud, the gory Details. Computer Fraud & Security 20(1):10-14
[11] Phua, C., Lee, V., Smith, K. And Gayler, R..(2005). A Comprehensive Survey of Data Mining-Based Fraud Detection Research, Artificial Intelligence Review.

[12] J. J. HOPFIELD Neural networks and physical systems with emergent collective computational abilities. Proc. NatL Acad. Sci. USA Vol. 79, pp. 2554-2558, April 1982 Biophysics.

[13] Fukushima, Kunihiko (1975). "Cognitron: A self-organizing multilayered neural network". *Biological Cybernetics* 20 (3-4): 121–136. doi:10.1007/BF00342633. PMID 1203338.

[14] McCulloch, Warren; Pitts, Walter, "A Logical Calculus of Ideas Immanent in Nervous Activity", 1943, Bulletin of Mathematical Biophysics 5:115-133.

[15] Brown EN, Kass RE, Mitra PP. (2004). "Multiple neural spike train data analysis: state-of-the-art and future challenges". *Nature Neuroscience* **7** (5): 456–61. doi:10.1038/nn1228. PMID 15114358

ISBN : 978-93-81361-22-1 Excel Publishers, New Delhi

View publication stats