Application of Neural Network in Fraud Detection Using Business Concepts

Asma Baloch and Muhammad Nadeem
SZABIST
Karachi, Pakistan

Abstract:

Intense global and local technological augment and diminishing trade barriers are making life difficult for businesses. At a time when customers have revolutionary expectations, sophisticated decision system modeling is pivotal to an organization's business strategy.

This era is e-payment focused, and emphasizes enhanced operational efficiencies. Other necessary attributes needed to compete successfully include facilitating customer services and satisfaction, risk management, decision support systems, major breakdown of trade barriers, enhanced security and privacy, market forces, better technology, communication etc.

Electronic payment system is essential for proper functioning of the electronic market on the Internet. The significance of electronic payment system is enhanced by the effective use of credit card system at the electronic market online.

However, the time has come to break down the psychological, culture and traditional barriers and adapt the value-added component of the secure electronic payment tool. Neural Network (NN) is a revolutionary changing process for online business trading and should be adopted for safety and security of one's own business, and to join the global bandwagon of technical trends.

1. INTRODUCTION

Today's financial scenario and the rapid changing face of computerized business are leading the path to global marketplace. Business battlefield is shifting to greater electronic standardization. Companies are uncertain about practicing automation standards and the demanding customer needs. In this complex combat zone, developing nations are at the stake of countenance of war clouds. Thy are not fast in customizing the technology and systems used by companies for their survival, security and transparency in the developed world.

Perhaps, it is paradoxical that these online businesses do not put to practice the security-safeguarding tool for the consistency and reliability of electronic payment systems. It is bizarre that the think tanks fail to understand the need for formation of security and measurability crucial for the commencement of e-world era. Hence, the outcome of fraudulent activities is critically required to look in! [1]

The above case has been initiated as a ground base idea to the problem formulation of this study. NN is a magnificent automated business world development solution packed up in diverse fields. It is useful in FD but its performance in the market is far from perfect. There is a need to recognize the vital needs of this system so that companies join the bandwagon of NN using business concepts, as practiced abroad.

2. UNDERSTANDING NN AND FD: KEY CONCEPTS AND GENERAL IMPLEMENTATION APPROACHES

Face of Electronic Payment System in Business

E-commerce expansion package with Electronic Payment System (EPS) based on the Internet has turned out spot. Majority of the present payment forms are single bank based and e-cash is lacking intelligibility and transparency. Internet is the only medium, which hooks up the whole world, and has set up unlimited commerce activities. EPS has an edge over the traditional manual-based transactions in reference to cost cutting in manufacturing, shipping and managing the physical material [2]. In addition to this, EPS has mainly affected the pace of circulation of money that used to take place before. Thus EPS will give a new road to the developing E-commerce on the net.

This system is developed by commercial banks and it is these banks that should setup their own payment gateways and authenticating centers. Hence, this would lead to order less competition and resource wasting. And better-enhanced model would follow a distributed electronic payment system.

The fast growing online commerce brings in new opportunities and new challenges for the traditional retailers and 'pure-play' web merchants.

Business-to-consumer commerce is projected to grow up to 150 billion dollars by 2004. Internet will become the key selling channel for the retailer sector. Business over the Internet has exposed merchants to a greater level of risk of losses due to fraud. Accountability strategies for card-not-present transactions and because of the anonymity, accomplishment and speed that the net provides for the con artist, risk management and fraud

prevention have become vital modules for every e-commerce infrastructure.

Prevention of credit card fraud is a vital function. Main barrier for using NN training techniques is the high essential analytical quality: As only one financial deal of a thousand is void, no prediction success less than 99.9 percent is satisfactory. New concepts are developed and tested on credit card fraud by using advanced data mining techniques and NN algorithm so as to acquire high fraud rate coverage.

3. PROPOSED BANK MODEL FOR CREDIT CARD FRAUD DETECTION IN PAKISTAN

In today's financial world, more and more transactions are carried out electronically and remotely. The opportunities for criminals to conduct fraudulent transactions rise with the complexity of the system. Credit card is one of the areas where fraudulent behavior is of great concern to financial institutions. Individual criminals steal credit cards and then use them toward purchases, through criminal groups that steal new credit cards or duplicate credit cards without the knowledge of their holders. Another form of fraud is customer-induced when customers claim that their card was stolen after making expensive purchases. Even though most credit card purchases today are electronically verified before the actual transaction, various opportunities for fraudulent behavior still exist. Most credit card companies already use sophisticated systems for FD.

The common problem of these systems is that they have to work with very little significant data. The only information they have is past customer history and information about the transaction. The objective for a purpose FD system is to identify as many cases of fraudulent behavior as possible. On the other hand, if they too easily decline non-fraudulent transactions, customers become dissatisfied and may switch to another credit card company.

Merchant accounts are subject to fraud in similar ways. Of course, it is easy to detect fraudulent behavior when a transaction is made from Karachi and Islamabad on the same card within half an hour or same amount (limit) transaction can be done same time from different places. But such easy cases are rare. More often, one has to evaluate that fraud is occurring, similar to when the BATCH detect from transaction behavior that from Point of sale terminal some X person all of a sudden makes six very long transactions in one week to a small location in Karachi.

Unfortunately, the willingness of companies to disclose system details about FD systems is very low. Companies are justifiably afraid that a disclosure or even the fact that they use a NN (Fuzzy Logic) FD system may help criminals to circumvent the system. The case study developed in this section stems from a project with a financial service provider who would like to remain anonymous. Any reference to the company will be as "ABC" corporation. ABC offers its customers both banking and insurance services. The advantage here is that information from both the insurance and banking background of the customer is accessible for detection of insurance fraud.

ABC's application uses a NN (Fuzzy Logic) system to evaluate each POS transaction in terms of BACTH Techniques to assess the likelihood of fraudulent behavior. In the field of POS Transaction, most fraud is not perpetrated by professional criminals but by otherwise law-abiding individuals with many different motives for their behavior. Thus, ABC wanted to implement a FD system that looks at multiple factors in every Transaction and selects only those where it assumes a certain degree of likelihood of fraud for manual review.

The output of the NN Fuzzy Logic system is twofold. First, a degree of likelihood of fraud is assessed by the NN system. A second output variable (Reason) gives an indication why a certain POS transaction was considered to be possibly fraudulent by the NN Fuzzy Logic system. The purpose system model is based on parameters as follows:

- PAN # (Personal Authorization Number)
- From Account Checking
- To Account Type
- Transaction Type
- Transaction Amount
- Transaction Reference Number
- Transaction Approval
- System Trace Audit Number
- Batch Number
- Transaction Date
- Transaction Time
- Response Code
- Merchant ID
- Terminal ID
- Merchant Location

The degree of likelihood of fraud is computed by the NN Fuzzy Logic system as a number between ZEROZERO and ZEROONE. ZEROZERO indicates that it was evaluated as totally non-fraudulent, while ZEROONE indicates a very high likelihood of fraud. After an insurance claim is assessed by the NN logic system, its degree of likelihood of fraud is compared to a threshold value pre-determined by ABC. If the result is lower than the threshold, the claim is immediately paid out to the customer. If the result is higher than the threshold, the claim is passed on to a claims auditor together with the Reason result of the NN Fuzzy Logic system. The claims auditor will then manually review the claim and decide the steps to be taken.

NN-Supported Fraud Detection

To protect the proprietary information of ABC, the NN (Fuzzy Logic) FD system presented in this section is

simplified and the rules and membership functions contained within are modified. The NN (Fuzzy Logic) system uses the following seven input parameters and variables (These parameters can vary from merchants to merchants and Banks):

1. Number of claims in the last 12 months (NumClaim)
2. Amount of current claim (Amount)
3. Time (CustSince)
4. Average balance on all banking accounts over the last 12 months (AvgAmnt)
5. Number of overdrafts over the last 12 months (NumOvr)
6. Annual income of customer (Income)
7. Recent changes in status (StatChng)

Application Processing and POS Parameter (Online Transaction)

8. Merchant Limit
9. Batch Number Sale and Refund (Set frequency for Batch Processing)
10. Amount Trend
11. PAN Sequence

These input variables can be divided into three groups. Each group represents a certain aspect of a claim. Input variables 1 to 3 give information about the insurance contract and the claim itself. Input variables 3 and 4 describe the banking background of the customer, and input variables 6 and 7 provide the personal background of the customer. The idea behind the structure of the NN (Fuzzy Logic) system as shown by Figure 1 is that no one of these seven input variables alone can significantly identify fraudulent behavior. Only the combination of different facts can provide a good indication of possible fraud. Hence, the NN (Fuzzy Logic) system draws its conclusion from three different sub-assessments of insurance history (HistIns), banking history (HistBank), and personal background (Personal).

Insurance History Evaluation

The linguistic variable HistIns expresses the degree to which the customer uses the insurance contract. To evaluate insurance history, three input variables are used. The first input variable (NumClaim) gives an indication of how often the customer has used the insurance in the past year. The second input variable (Amount) expresses how significant the current claim is. The third input variable (CustSince) takes into account how long the insurance contract has been in existence. This evaluation delivers an indicator of how much the customer has exercised their insurance contract in the past and present.

Banking History Evaluation

The linguistic variable HistBank evaluates the banking history of the customer and its relevance to his or her insurance claim. The two input variables for this evaluation are the average total balance on all banking accounts of the customer (AvgAmnt) and the number of over-drafts on checking accounts (NumOvr). This evaluation can deliver indicators that the customer is in a critical financial situation, and, therefore, suggest a motive for fraudulent behavior.

The variable StatChang is entered as a NN variable, but it is actually a non-NN variable since the possible degrees of truth are only Zero and One. However, more than one term of StatChng may have a degree of truth of one. For example, a customer could have been both divorced and laid off within the last four months. The assessment of the variable (Personal) detects possible motives within the customer's lifestyle that could motivate fraudulent behavior.

Fraud Evaluation Policy

The determination of the likelihood of fraud is contained in the rules of the four upper rule blocks. The lowest rule block contains the rules that provide the reason for which an insurance claim has been selected for an auditor's review. The NN Fuzzy Logic rules contain the actual fraud evaluation policy and analyze whether certain patterns for a possible fraud exist. For example, an insurance claim by a customer that has frequently made claims over the past year and is claiming a large amount would be evaluated as not likely to be fraudulent if he has a stable personal background and no cash problems.

Determination of the Acceptance Threshold by Field Test

A field test involved 1200 arbitrarily selected insurance claims filed with ABC. All 1200 cases were reviewed by the NN Fuzzy Logic FD system. At the same time, experienced auditors also reviewed all 1200 cases. The experienced auditors classified 117 cases as "possibly fraudulent." These cases were the ones selected for further review in the routine operations of ABC.

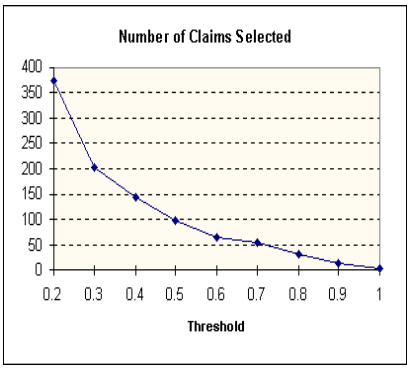

Figure 1: Because the NN (Fuzzy Logic) FD system associates each claim with a number between 00 and 01, the number of claims selected for scrutiny depends on the threshold

Figure 1 shows the relation between threshold value and the number of claims selected for manual review. For example, if a threshold of 0.477 for the NN Fuzzy Logic FD system is selected for the 1200 cases, a total of 117 cases are selected for manual review —the same number as the auditors came up with. The interesting part is that the 117 cases, which the NN Fuzzy Logic FD evaluated with Fraud 0.477, are not the same 117 cases the auditors selected. Only 89 of the cases were the same.

ABC then had all 145 cases selected by either the NN Fuzzy Logic FD system or by the auditors manually reviewed for fraud. Of the 89 cases selected by both the auditors and the NN Fuzzy system, fraudulent behavior was found in 34 cases. This corresponds to a 38 percent hit rate. Of the 28 cases selected by only the auditors, fraudulent behavior was found only in three cases. This corresponds to an 11 percent hit rate. Of the 28 cases selected by only the NN Fuzzy Logic FD system, fraudulent behavior was found in six cases. This corresponds to a 22 percent hit rate.

Testing Different Threshold Values

ABC was quite surprised that the NN Fuzzy Logic system was capable of detecting six fraudulent cases that the auditors did not detect. To evaluate how many more fraudulent claims could be found when more claims were selected, the selection threshold of the NN Fuzzy Logic system was lowered to 0.4 and to 0.3. Then, the additional claims were reviewed. Table 1 shows the results for both cases in an overview.

	Number Selected	Number Fraudulent	Hit Rate
Auditors	117	37	31.6%
Neural Network Fuzzy Logic System (Th.: 0.477)	117	40	34.2%
Neural Network Fuzzy Logic System (Th.: 0.4)	144	46	32.9%
Neural Network Fuzzy Logic System (Th.: 0.3)	201	48	23.9%

Table 1: Comparison of number of fraudulent claims detected

Lowering the review threshold for the NN Fuzzy Logic system to 0.4 will select 144 cases for review. Of these additional 27 cases, six turned out to be fraudulent. This corresponds to a 22.2 percent rate of fraudulent claims in the additional claims. This hit rate is much lower than the hit rate for the first 117 selected cases. In other words, reviewing 27 more cases than the previously selected 117 reveals six more fraudulent cases. Lowering the review threshold even more, down to 0.3, will select 201 cases for review. Of these additional 57 cases, only two were found to be fraudulent. This corresponds to a hit rate of just 3.5 percent. ABC used these results to decide on a threshold value of 0.4 in the final system. Lowering the threshold from 0.477 to 0.4 revealed six more fraudulent claims that cost ABC considerably more than the effort of reviewing 27 more cases. Ultimately, the effort of also reviewing the remaining 999 cases that were neither selected by the NN Fuzzy Logic system nor the auditors would have been unwarranted. The actual information on how many fraudulent claims both the auditors and the NN Fuzzy Logic system did not select would have been interesting. However, the fact that expanding the selection from 144 cases to 201 cases only revealed two more fraudulent claims provides for the assumption that the remaining fraudulent claims would be in the range of eight cases.

4. CONCLUSION

There are a number of problems in implementing the sophisticated fraud prevention tool NN, specifically in Pakistan. Firstly, we are a third world country, where such tools implementation is difficult. There is larger market persistent for fraudulent activities as compared to the advanced countries, where enhanced NN tools are used for fraud prevention and secure electronic transactions.

Pakistan can build an enhanced electronic payment system for secure and transparent transactions. But the right attitude has to be developed before fraudulent activities can be eliminated. The tag of a blacklisted country known for deceptive actions must go.

Foreign banks operating in Pakistan are indeed doing a marvelous job. These banks are 90 percent automated; remaining 10 percent constraints are imposed by the local regulations. But the major chunk of security and privacy is still untouched. We can see and enhance the ray of light, if proper direction is illuminated. Initially things would not happen right away, neither will they be easy and speedy, nor will it be cheap, yet it will be worth it.

Success will depend on the speed with which organizations adapt to the change. Or as Bill Clinton said, “Make, Change our Friends NOT enemy". It is predicted that large organizations compared to the smaller organizations will be slower in adopting the change.

However, there are a number of agencies that help the suffering victims through proper reporting. These agencies work out the aftermath of fraud. Post-fraud working helps in getting hold of the con artist.

ABC’s Pakistan application (identity kept anonymous on request) uses a NN (Fuzzy Logic) system to evaluate each POS transaction in terms of BACTH Techniques to assess the likelihood of fraudulent behavior. In the field of POS Transaction, most fraud is not perpetrated by professional criminals but rather by otherwise law-abiding individuals with many different motives for their behavior. Thus, ABC has implemented a FD system that looks at multiple factors in every Transaction and selects only those where it assumes a certain degree of likelihood of fraud for manual review.

REFERENCES:

[1] Dodel and Shingal, Jean-Pierre and Rajjan, 1995, symbolic/NeuralRecognition of Cursive Amounts on Bank cheques, IEEE, Concordia University, Montreal, Canada, Volume # 1(0-8186-7128-9)

[2] Zhao, Oiang Xu, Hong, 2000, Distributed Electronic Payment System Based on Bank Union, IEEE, Northeastern University, Shenyang, Volume # 0-7695-0589-2