International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-1, October 2013

Fraud Detection in Banking

M Madhavi, M V R Srivatsava

Abstract— as a customer we may face the potential target for fraudulent activities. In the present scenario the customer is the prime victim of all the fraudulent activities that drag him to a great lose. Due to unpredictable nature of mankind, would eventually lead to manipulation of any transactions or they may lead to theft of details. This survey paper deals with the different types of techniques that help to find the fraudulent activities in the banking sector.

Index Terms— Electronic fraud, Identity theft, Credit/Debit card fraud, Data mining techniques

I. INTRODUCTION

A bank is the connection between customers that have capital deficits and customers with capital surpluses. It is a intermediate node for financial credentials that accepts deposits and channels into different capital marketing activities either directly or indirectly .The main duty of bank is to maintain economic feasibility for both business and commercial purposes. In the present scenario, computerized banking are predominant where multiple transaction occur for fraction of seconds through internet .The transactions include like withdraw, deposit ,fund transfer from one account to another. As increasing numbers of businesses and consumers rely on the Internet and other forms of electronic communication to conduct transactions; illegal activity using the very same media is similarly on the rise. Fraudulent schemes conducted via the Internet are generally difficult to trace and prosecute, and they cost individuals and businesses millions of dollars each year. A fraud is a Wrongful or criminal deception intended to result in financial or personal gain that leads to civil violation. Generally banking frauds include Electronic fraud, Identity theft, and Credit/Debit card fraud that may occur through internet.

Electronic fraud**:**

It is a fraudulent activity which involves deception through internet for financial gain.

Identity theft: The fraudulent acquisition of information of a person in order to gain benefits generally for the purpose of financial aspect.

Credit/Debit card fraud:

Credit card and debit card fraud is a crime whereby your credit or debit card can be reproduced in order to use the credit balance to obtain a financial advantage. In the present scenario banking sector developed fraud detection systems at their own assets bases. Recent studies on attacks realized the financial institutions that importance of global fraud detection which connects to local detection system. Improved fraud detection thus has become essential to maintain the viability of the banking system [1].

Improved fraud detection thus has become essential to maintain the viability of the banking system. Large-scale data-mining techniques,[2] can improve on the state of the art in commercial practice. Scalable techniques to analyze massive amounts of transaction data that efficiently compute fraud detectors in a timely manner is an important problem, especially for e-commerce. Besides scalability and efficiency, the fraud-detection task exhibits technical problems that include skewed distributions of training data [3], [4] and non-uniform cost per error, both of which have not been widely studied in the knowledge discovery and data mining community.

II. EXISTING SYSTEM

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

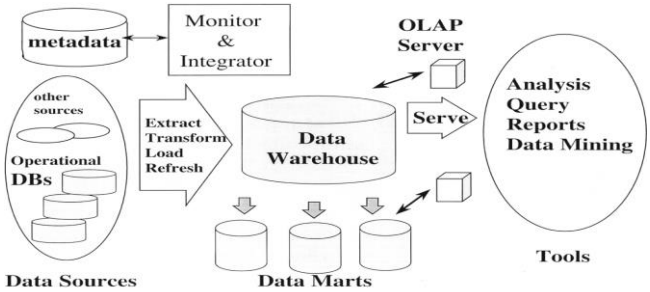
III. PROPOSED SYSTEM

The proposed system survey has been made for all types of fraudulent activates in banking sector like Electronic fraud, Identity theft, and Credit/Debit card fraud etc.We provide authorized access sending a random number that is generated through different random numbers .

IV. RELATED WORK

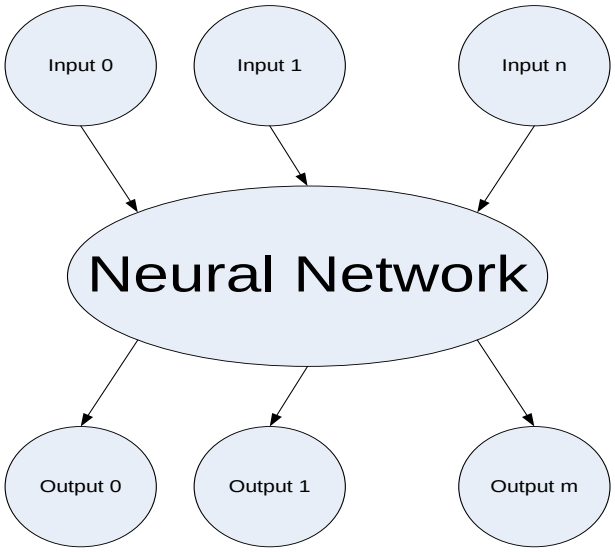
Data mining is a process that uses a variety of data analysis tools to discover patterns and relationships in data that may be used to make valid predictions. Data mining does collecting, exploring and selecting the right data are critically important. To best apply these advanced techniques, they must be fully integrated with a data warehouse as well as flexible interactive business analysis tools. Many data mining tools currently operate outside of the warehouse, requiring extra steps for extracting, importing, and analyzing the data. Different data mining techniques include clustering, neural networks, statistics etc.

Manuscript published on 30 October 2013.
***** Correspondence Author (s)
M. Madhavi*, Asst professor CSE, Kluniveristy, Vijayawaada, India
M V R Srivatsava, CSE, KL Univeristy, Vijayawaada, India.



Source: Modifications made from Han and Kamber (2001)

Neural Networks:



Neural networks are of particular interest because they offer a means of efficiently modeling large and complex problems in which there may be hundreds of predictor variables that have many interactions.(Actual biological neural networks are incomparably more complex.) Neural nets may be used in classification problems (where the output is a categorical variable) or for regressions (where the output variable is continuous). A neural network starts with an *input layer*, where each node corresponds to a predictor variable. These input nodes are connected to a number of nodes in a *hidden layer*. Each input node is connected to every node in the hidden layer. The nodes in the hidden layer may be connected to nodes in another hidden layer, or to an *output layer*. The output layer consists of one or more response variables. The *architecture* (or topology) of a neural network is the number of nodes and hidden layers, and how they are connected. In designing a neural network, either the user or the software must choose the number of hidden nodes and hidden layers, the activation function, and limits on the weights. While there are some general guidelines, you may have to experiment with these parameters. One of the most common types of neural network is the *feed-forward back propagation* network. For simplicity of discussion, we will assume a single hidden layer. Back propagation training is simply a version of gradient descent, a type of algorithm that tries to reduce a target value (error, in the case of neural nets) at each step.

The algorithm proceeds as follows.

Feed forward: The value of the output node is calculated based on the input node values and a set of initial weights. The values from the input nodes are combined in the hidden layers, and the values of those nodes are combined to calculate the output value.

Back propagation: The error in the output is computed by finding the difference between the

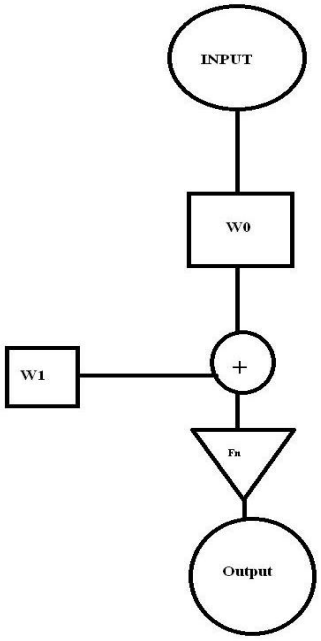
Calculated output and the desired output (i.e., the actual values found in the training set).Next, the error from the output is assigned to the hidden layer nodes proportionally to their weights. This permits an error to be computed for every output node and hidden node in the network. Finally, the error at each of the hidden and output nodes is used by the algorithm to adjust the weight coming into that node to reduce the error.

In this context we use feed forward for our calculation.

V. ALGORITHM

1. Algorithm for Credit/Debit card fraud detection:

whenever any transaction is performed by the third party user using credit card or debit card for example shopping, buying utensils, vegetables etc for each transaction a predictor variable (i.e. the account number of user) or the initial weight allocated to the credit/debit cards will be taken as input value will be sent to the hidden layer where the actual calculation are performed to verify the actual card owner. If it is said to be valid then an verification number is sent the card owner. He has to acknowledge by entering the verification code before transaction .otherwise it is treated as fraudulent activity and the credit/ debit card will be blocked.



Here,

F(x) [linear threshold]

W0 = random (0, 1)

W1 = random (0, 1)

Z=F ( )

ALGORITHM:

Input:

X=Account number.

Y=random (AlphaNumeric)

W0=weight assigned to the Account.

W1=weight assigned to account holder.

Output:

Step1:

```
for i= to 3
{
{
do
{
        "Enter the pin number of card";
         MatchPin(x);
W0=1;
}
else "wrong attempt, blocked";
W0=0;
}
do
        {
"Enter the secret code for transaction"
 if match (Y) == 1 then W1=1;
        else W1=0;
}
function F ( )
{
if (W0==1 && W1==1)
        return 1;
        else
        return 0;
        }
        Z= F ( );
        if Z==1 "allow" else "disallow and block"
        "Your card failed three attempts"
        }
```

2. Techniques for identity theft:

Identity fraud may occur when someone steals personal information, opens credit card accounts in the victim's name without permission, and charges merchandise to those accounts. Conversely, identity fraud does not occur when a credit card is simply stolen. Stealing one's credit card may be consumer fraud, but is not identity fraud. Identity fraud is a synonym of unlawful identity change. It indicates unlawful activities that use the identity of another person or of a non-existing person as a principal tool for merchandise procurement.

Identity fraud can occur without identity theft, as in the case where the fraudster has been given someone's identity information for other reasons but uses it to commit fraud, or when the person whose identity is being used is colluding with the person committing the fraud.

One case of identity fraud is when the PlayStation Network was hacked into, and the man responsible for this took the information from everyone who had their credit card information installed on the Network. It took three months to fix the problem, when it occurred. Moreover, identity fraud does not necessarily involve colluding or theft of another's personal information; it can also involve the use of fake names, ID cards, falsified or forged documents, and lying about his or her own age to simply "hide" his or her true identity. Reasons for this type of identity fraud may include wanting to purchase tobacco or alcohol as a minor as well as desire to continue playing on a certain sports team or organization when that person is really too old to compete.

The secret code that is sent to mobile serves as authenticated Agent and that avoids identity theft. Because it is the most secured way of transaction.

VI. CONCLUSION

This survey paper provides the idea of secure electronic transaction in an efficient way.Authenctication through mobile agent is the new idea that would help the targeted customer to get rid of electronic fraudulent activities such as identity theft and credit/debit card frauds. Algorithm provides the detailed view of implementing the secured transaction in neural networks. We prefer neural networks because information passes and decision making strategies are very rapid in this network system.

VII.ACKNOWLEDGEMENT

I would thank my guide Ms.M.Madhavi for giving guidelines over the topic and helped in making this paper in an efficient way.

REFERNCES

In the context of this paper "Fraud Detection in Banking Using Data Mining – Neural Networks" the references include

[1] Ogwueleka, F. N. (2008). Credit card fraud detection using data mining techniques. Ph.D. Dissertation. Department of Computer Science. Nnamdi Azikiwe University, Awka, Nigeria.

[2] Data Mining: Concepts and Techniques Jiawei Han and Micheline Kamber. *(References)*

[3] Fawcett, T; and Provost, F. (1997). Adaptive fraud detection. Data Mining and Knowledge Discovery, 1(3).

[4] Types of frauds in banking sector at "http://www.anz.com/personal/ways-bank/security/online-security/threats-banking-safety/fraud-types/"

Ms.M.Madhavi works at KLUniversity situated at vaddeswaram. She completed her B.Tech from KL college of engineering and M.Tech from JNTU Hyderabad. Presently working as assistant. Professor as designation. She has done many research papers on data Base and its related topics.

M V R Srivatsava is presently pursuing B.Tech from KLUniversity in the branch of COMPUTER SCIENCE AND ENGINEERING has done many paper presentations and poster presentation on data mining and data base related topics.