Credit Card Fraud Detection

G.Divya, Department of Computer Applications,
Mr. R. Ambikapathy., M.C.A., M.Phil.,Assistant Professor,
Krishnasamy college of Engineering and Technology,Cuddalore.

ABSTRACT

The most accepted payment mode is credit card for both online and offline in today's world, it provides cashless shopping at every shop in all countries. It will be the most convenient way to do online shopping, paying bills etc. Hence, risks of fraud transaction using credit card has also been increasing. In the existing credit card fraud detection business processing system, fraudulent transaction will be detected only by a manual report case. It is difficult to find out fraudulent and regarding loses will be barred by issuing authorities. In this paper, it is shown that credit card fraud can be detected using web application during transactions. This application helps to obtain a high fraud coverage combined with a low false alarm rate.

Keywords: Internet, online shopping, credit card, e-commerce security, fraud detection, Hidden Markov Model.

1.Introduction

In day to day life credit cards are used for purchasing goods and services with the help of virtual card for online transaction or physical card for offline transaction. In a physical-card based purchase, the cardholder presents his card physically to a merchant for making a payment. To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the credit card. If the cardholder does not realize the loss of card, it can lead to a substantial financial loss to the credit card company. In online payment mode, attackers need only little information for doing fraudulent transaction (secure code, card number, expiration date etc.). In this purchase method, mainly transactions will be done through Internet or telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information. The only way to detect this kind of fraud is to analyze the spending patterns on every card and to figure out any inconsistency with respect to the "usual" spending patterns. Fraud detection based on the analysis of existing purchase data of cardholder is a promising way to reduce the rate of successful credit card frauds. Since humans tend to exhibit specific behavioristicprofiles, every cardholder can be

represented by a set of patterns containing information about the typical purchase category, the time since the last purchase, the amount of money spent, etc. Deviation from such patterns is a potential threat to the system

2. Existing System

In existing system,the credit card fraud detection system is a highly researched field, there are many different algorithms and techniques for performing the credit card fraud detection system. One of the earliest system is CCFD system using markov model. Some other various existing algorithms used in the credit cards fraud detection system includes Cost sensitive decision tree (CSDT), support vector machine (SVM), Random forest,etc. credit card fraud detection(CCFD) is also proposed by using neural networks. The existing credit card fraud detection system using neural network follows the whale swarm optimization algorithm to obtain an inceptive value. It the uses BP network to rectify the values which are found error. All of these techniques has some serious disadvantages such as decreasing accuracy levels, lack of efficiency, sometimes classifying the normal transactions as fraud transactions and vise versa.

DISADVANTAGES:

- A victim becomes heavily indebted, sometimes bankrupt because of credit card fraud.
- It unable to pay their debt will, as a penalty, see an increase in their credit score. This will result in them not being able to get loans.

3. Proposed System

It is shown that credit card fraud can be detected using web application during transactions. This application helps to obtain a high fraud coverage combined with a low false alarm rate.The Credit card fraud detection system is initiated for detecting the fraud transactions from the number of transactions made by the card holders. The transactions done by credit card holders are derived in the form of datasets. Datasets are nothing but data that are already being posted by the companies and researchers for the purpose of data mining. .This technique is mainly used to differentiate the fraud transactions from the original transactions done by the card holders. Initially the transaction data are stored in a confluence form.

ADVANTAGES

- It achieve good accuracy rates in order to detect the fraud in the credit cards.
- By this application outperformed and prevented the frauds in any online transaction through credit cards .

4. Methodology

Modules Used:

- New card

- Admin
- User
- Bank
- Company
- Security data
- Verification
- User modules

5.Module Description:

New card

In this module, the client gives there data to enlist another card. The data is about their contact subtle elements. They can make their own particular login and secret key for their future utilization of the card it has transaction process, withdraw details and deposit details.

Admin modules

Admin views all details and knows the transaction process that are handled by the users.

User modules

In this module, the customer gives there information to enroll a new account. The information is all about their contact details. They can create their own login and password for their future use of the card. This module is performed after the verification and if the user is not the fraudster then only the transaction is performed according to the cardholder want.This module deals with the overall profile of the user which is related to the transaction. The differentiate transaction Id noted as fraud.

Bank modules

In this modules, Transaction process is performed .This transactions includes providing a communications device to a vendor and a credit card owner. The credit card owner initiates a credit card transaction by communicating to a credit card number withdraw details and deposite details. During the time of transaction fraud may detect.

Company modules

Company modules has the details of product with their sub category and price details.

Security data

In Security data module it will get the data detail and its store's in database. On the off chance that the card lost then the Security data module frame emerge. It has an arrangement of question where the client needs to answer the effectively to move to the exchange area.

It contain instructive protection and enlightening self-assurance are tended to decisively by the creation bearing people and elements a put stock in intends to client, secure, pursuit, process, and trade individual as well as private data.

Verification

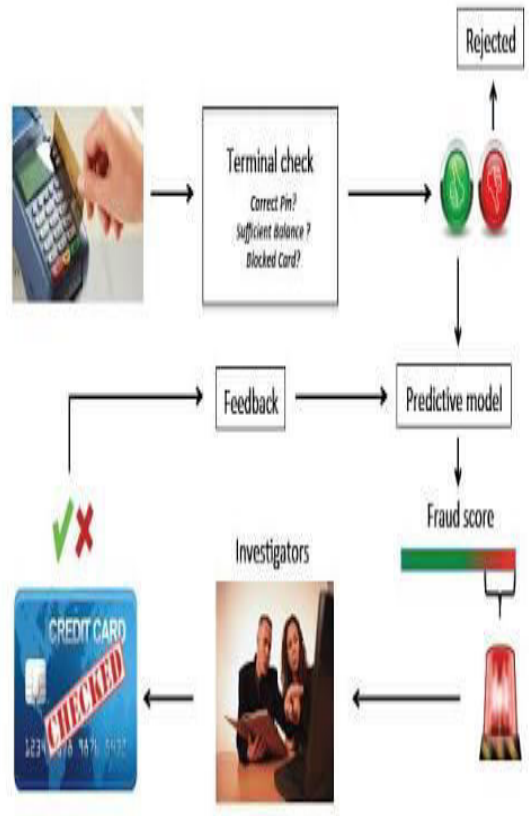
Check data is furnished concerning an exchange between a starting gathering and a confirmation looking for party, the check data being given by a third, checking party, in view of classified data in the ownership of the starting party. In check

the procedure will looks for card number and if the card number is right the pertinent procedure will be executed. On the off chance that the number isn't right, mail will be sent to the client saying the card no has been square and he can't do the further exchange.

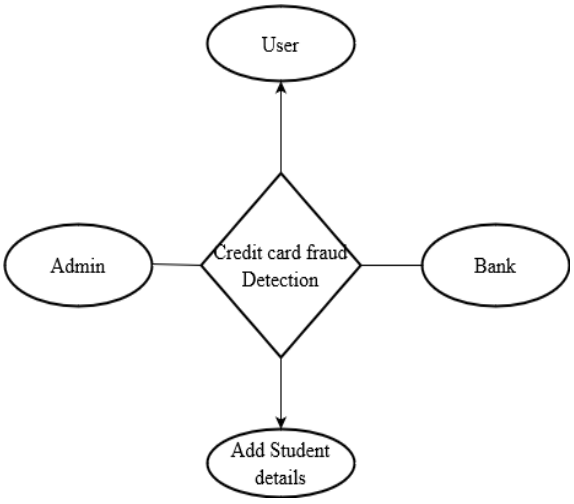
User modules

User is the main module. This module is performed after the verification and if the user is not the fraudster then only the transaction is performed according to the cardholder want.This module deals with the overall profile of the user which is related to the transaction.

6.System Architecture



7.DATAFLOW DIAGRAM:



8.SCOPE FOR FUTURE ENHANCEMENTS

The project has covered almost all the requirements. Further requirements and improvements can easily be done since the coding is mainly structured or modular in nature. Improvements can be appended by changing the existing modules or adding new modules.Oneimportant development that can be added to the project in future is file level backup, which is presently done for folder level.

9.CONCLUSION

Although there are several fraud detection techniques available today but none is able to detect all frauds completely when they are actually happening, they usually detect it after the fraud has been committed. This happens because a very minuscule number of transactions from the total transactions are actually fraudulent in nature. So we need a technology that can detect the fraudulent transaction when it is taking place so that it can be stopped then and there and that too in a minimum cost.

10.References

- Beginning ASP.NET 4: in C# and VB by ImarSpaanjaars.
- Programming ASP.NET 3.5 by Jesse Liberty, Dan Maharry, Dan Hurwitz.
- Beginning ASP.NET 3.5 in C# 2008: From Novice to Professional, Second Edition by Matthew MacDonald.
- Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, "Graphical Password Authentication Using Cued Click Points" ESORICS, LNCS 4734, pp.359-374,Springer- Verlag Berlin Heidelberg 2007.
- Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd, "Reducing Shoulder-surfing by Using Gazebased Password Entry", Symposium On Usable Privacy and Security (SOUPS) , July 18-20, 2007, Pittsburgh,PA, USA.

SITES REFERRED:

http://www.asp.net.com

http://www.dotnetspider.com/

http://www.dotnetspark.com