Technique on how to detect Credit Card

Fraud Using Data Mining

By: Charine Tenerife

**Introduction**

Credit Card Fraud has a big impact on Credit Card Industry. Thus the fraudster are very tuned in to find more ways to access sensitive information like phishing and takeover tactics. Credit Card Fraud is someone who used your account to purchase either online or person without owner’s authorization. Fraudster may use your stolen credit card account, security code and PIN codes to different and unauthorized transactions. Credit card fraud happen whether online as well as offline. Nowadays credit card fraud is almost a wide issue for almost decade. With the use of Technology we could easily identify and detect the fraudster. Through the use of Data Mining that can be used to detect fraudulent credit card transaction. It’s well defined procedure that takes data as input and procedure pattern as output. Data Mining Technique also help to analyze and discover pattern as behavior and reliability of the customer that may be used to make valid prediction.

Data Mining uses various methods for fraud detection these are the Hidden Markov Model and Neural Network. When we say Hidden Markov Model it is used in detecting and analyzing the spending profile of credit card owner. Generally the profile are being divided into three types the lower profile, middle profile and higher profile. It easily to find out the fraudulent by keeping the consistent record of the usage of credit card. And the Neural Network is based on pattern recognition, classification, clustering, feature mining, ad prediction. It can be used to model the complex relationship between inputs and outputs to find patterns in data. Most of credit card company use chip technology rather than the magnetic stripe, as these are to be more difficult to hack in store purchases where chip are enabled. And it’s not easy to replicate the card over and over again. Because it creates a unique code of transaction that cannot be used again.

Just like the fraudster do it’s fairly easy to copy the magnetic stripe of credit card. After the fraudster skim the information from your card all the data will be burned into a blank counterfeit card. And will be used just like your original credit card. To keep our credit card safe and protected we should develop the possible ways to detect the fraudster. The idea that I want to proposed is an application that once a fraudster purchase like in a department store and when the teller swipe the card. The card will verify and appear the image of the original owner without using the signature but instead with the used of finger print or biometric. In that case the owner will automatically get notify in every transaction through their email from unknown transaction. This research aims to detect the fraudsters from malicious transaction.

**Methods**

The methods for Credit Card Fraud detection I used is based on Hidden Markov Model which does not require the fraud signature but still it is capable to detect frauds by just bearing in mind of cardholder’s spending habit. The implementation technique of Hidden Markov Model in order to detect the fraudster from different transaction through credit cards. It’s identify the spending profile of cardholder. The types of items and number of items purchased that are bought in a particular transaction are not known to the fraud detection system. But it concentrate to the amount of item purchased and used.

Its store the data of different transactions in a form of clustering that depends on the amount of transaction which be either in low, medium or high value. It tries to find out based on the spending behavior profile of the credit card holder, the billing address and shipping address. Thus the probabilities of initial set have chosen the spending behavioral profile of credit card holder and construct a sequence for further processing. If the fraud detection makes sure that the transaction is fraudulent it will raises an alarm and the issuing bank will automatically declines the transactions. The goal of this analysis is to give note about the fraudulent transactions to the issuing bank and to the merchant to take appropriate action by the issuing bank.



1. Fingerprint Matcher

In this figure with the use of finger print it’s hard for the fraudster to be able steal the information from the bank central of their database. It’s very secure than the PIN that anyone could simply looking over you as you enter it. When the credit cardholders matches the finger scanning it will direct to verification or else it will generate an error.

The flow of system are as follows:

First Start, Insert the card number. Check if it is valid account then send the OTP on user’s number. Insert the OTP number. If matches then image will appear and go for biometrics securities. Place the fingerprint to validate transaction. If pattern match then the transaction occurs successfully. Else then it will display a message that the transaction is failed and not recognized. Account does not exists then it will stop. The advantage of this system is to reduce the fraud detection and can find most the accurate detection using this model.

**Results**

In this work we consider three ranges which is the low (l), medium (m), and high (h). An example of this symbol let l = (0 – 10,000), m = (10,000 – 50,000), and h = (50000 to credit card limit) If a cardholder performs a transaction of 15,000 then the corresponding range or symbol is m. The real price of variety for every symbol is to configurable based on the expenditure routine of personal credit cardholders. HMM determine these prices rang dynamically by using the clustering algorithms. In other situations the issuing bank may want to allow the transaction but they will leave an email message or via sms for the credit card holder to notify them for a potential suspicious transaction. It would be secure in every transaction using the OTP via sms or email and detect the anomalous transaction when the card holder lost the card. In every transaction the issuing bank will get notify them so that they are aware about theirs credit cards and not to exceed to the credit limit. Based on the methods once the fraudster have made a transaction in a convenient store or malls and if they found out that it’s a scam the legitimate owner will get notify on it.

**Discussion**

To discussed the results of Hidden Markov Model in credit card fraud detection using this observation that will determine users spending profile. The purchase amount will be checked with spending profile of user. By the transition of the probabilistic calculation based on HMM, that concludes whether the transaction is real or fraudulent. If transaction may be concluded as fraudulent transaction then user must enter security information through the biometrics technology it could easily identify the legitimate owner of the credit card or they will take some question in a form of security purposes. If all the data are valid then it will allowed to perform the transaction or else it will be rejected.