Introduction

This credit card has recently become very attractive to fraudsters with changes in their activities during the last few decades as a result of increase in technological development

Credit card fraud takes place whenever an unauthorised user gains access to credit card or information contained in the card without permission from the card owner.

We have created a "Matching algorithm" that helps in fraud detection. It uses the hunts algorithm to form decision trees.

This algorithm has been divided into two parts

1. Online Credit card fraud detection

2. Offline Credit card fraud detection

Online Credit card fraud detection

This type of fraud includes online transactions to make purchases, shopping , etc

Parameters for fraud detection

*Credit card details

*IP address

*Email

*Purchase cost

*Frequency of purchase

*Location-(shipping,billing address)

Algorithm

S1 Enter transaction details

S2 if(card no & cvv = in-valid)

S3 if(IP address = valid)

O/P = re-enter

S4 else(IP address = in-valid)

Jump to step-7

S5 else(card no & cvv = valid)

S6 if(IP address = valid)

O/P = Legal

S7 else(IP address = in-valid)

S8 if(Email-ID = valid)

Jump to step-12

S9 else(Email-Id = in-valid)

10 if(location = valid)

O/P = Legal

11 else(location = in-valid)

12 if(amount = valid)

O/P = Legal

13 else(amount = in-valid)

14 if(frequency = valid)

O/P = Legal

15 else(frequency =in- valid)

O/P = Fraud

Offline Credit card fraud detection

This type of frauds include misuse of physical credit cards as a result of stolen cards, forged cards, lost cards etc.

Parameters for fraud detection

*Transaction type

    Swipe and pay

    Touch and pay

*IP address - device used to pay

*Purchase cost

*Frequency of purchase

*Pin entry

Algorithm

S1 Enter transaction details

S2 let transactionType(TouchPay, SwipePay)

S3 if(transactionType = swipePay)

S4 if(pin = valid)

S5 if(ip-address = valid)

O/P = Legal

S6 else(ip-address = in-valid)

S7 if(amount = valid)

S8 if(frequency = valid)

O/P = Legal

S9 else(frequency = in-valid)

O/P = Fraud

S9 else(amount = in-valid)

O/P = Alert(amount exceeded)

11 else(pin = in-valid)

12 if(ip-address = in-valid)

O/P = fraud

13 else(ip-address = valid)

if(re-entered pin = valid)

Jump to step -S4

14 else(re-entered pin = valid)

O/P = fraud

15 else(transactionType = touchPay)

16 Jump to step-5

App setup

1. Training data set:

   It contains Legal and fraud transactions of credit card this training data set is fed to hunt's algorithm

2. Hunt's algorithm:

   This algorithm uses a training data set to form a decision tree of parameters which is to be analysed for fraud detection.

3. Matching algorithm:

   a) The matching algorithm detects to which pattern the incoming transaction matches more

   b) A sample of current transaction and recent transaction from the past is fed to algorithm

   c) If the incoming transaction is matching more with legal pattern of the particular customer, then the algorithm returns "0" (i.e., legal transaction)

   d) If the incoming transaction is matching more with fraud pattern of that customer, then the algorithm returns "1" (i.e., fraud transaction)