CREDIT CARD FRAUD DETECTION

****

|  |  |  |
| --- | --- | --- |
| **Enrollment Number** | **Name** | **Batch** |
| 16103063  16103186  16103144  16103193 | Shivam Kumar Singh  Yasharth Pathak  Abhishek Choudhary  Somil Rastogi | B8  B8  B8  B8 |

Credit card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.

In proposed system, we present a behaviour and Location Analysis (BLA). Which does not require fraud signatures and yet is able to detect frauds by considering a cardholder’s spending habit. Card transaction processing sequence by the stochastic process of an BLA. The details of items purchased in Individual transactions are usually not known to any Fraud Detection System (FDS) running at the bank that issues credit cards to the cardholders. Hence, I feel that BLA is an ideal choice for addressing this problem. Another important advantage of the BLA -based approach is a drastic reduction in the number of False Positives transactions identified as malicious by an FDS although they are actually genuine. An FDS runs at a credit card issuing bank. Each incoming transaction is submitted to the FDS for verification. FDS receives the card details and the value of purchase to verify, whether the transaction is genuine or not. The types of goods that are bought in that transaction are not known to the FDS. It tries to find any anomaly in the transaction based on the spending profile of the cardholder, shipping address, and billing address, etc. If the FDS confirms the transaction to be of fraud, it raises an alarm, and the issuing bank declines the transaction.

The credit card fraud detection features uses user behaviour and location scanning to check for unusual patterns. These patterns include user characteristics such as user spending patterns as well as usual user geographic locations to verify his identity. If any unusual pattern is detected, the system requires reverification.

The system analyses user credit card data for various characteristics. These characteristics include user country, usual spending procedures. Based upon previous data of that user the system recognizes unusual patterns in the payment procedure. So now the system may require the user to login again or even block the user for more than 3 invalid attempts.

Core Features:

* The system stores previous transaction patterns for each user.
* Based upon the user spending ability and even country, it calculates user’s characteristics.
* More than 20 -30 % deviation of users transaction (spending history and operating country) is considered as an invalid attempt and system takes action.

Advantages

* Due to behaviour and location analysis approach, there is a drastic reduction in the number of False Positives transactions identified as malicious by an FDS although they are actually genuine.
* The system stores previous transaction patterns for each user.
* Based upon previous data of that user the system recognizes unusual patterns in the payment procedure.

We will use the following Python libraries.

1. NumPy (for documentation:<http://www.numpy.org/>)
2. Pandas (for documentation:<http://pandas.pydata.org/>)
3. Scikit-Learn (for documentation:<http://scikit-learn.org/stable/>)
4. itertools (<https://docs.python.org/3/library/itertools.html>)

It contains the predictive analysis using machine learning algorithms of the Credit Card Fraud Detection. Overall we are trying to implement a machine learning algorithm from the scikit-learn python library which has a number of algorithms to classify whether or not the card owner is a fraud utilising the information about his past transactions behaviour.