

Credit Card Fraud Detection

The challenge is to recognize fraudulent credit card transactions so that the customers of credit card companies are not charged for items that they did not purchase.

Main challenges involved in credit card fraud detection are:

Enormous Data is processed every day and the model build must be fast enough to respond to the scam in time.

Imbalanced Data i.e most of the transactions (99.8%) are not fraudulent which makes it really hard for detecting the fraudulent ones

Data availability as the data is mostly private.

Misclassified Data can be another major issue, as not every fraudulent transaction is caught and reported.

Adaptive techniques used against the model by the scammers.

How to tackle these challenges?

The model used must be simple and fast enough to detect the anomaly and classify it as a fraudulent transaction as quickly as possible.

Imbalance can be dealt with by properly using some methods which we will talk about in the next paragraph

For protecting the privacy of the user the dimensionality of the data can be reduced.

A more trustworthy source must be taken which double check the data, at least for training the model.

We can make the model simple and interpretable so that when the scammer adapts to it with just some tweaks we can have a new model up and running to deploy.

Before going to the code it is requested to work on a jupyter notebook. If not installed on your machine you can use Google colab.

You can download the dataset from this link

If the link is not working please go to this link and login to kaggle to download the dataset.

Advantages

Due to Behavior 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.

The System will block the user for more than 3 invalid attempts.