Detect and act on Fraud

-Nehal Jain

Objective

To develop a system that can analyze past and real time transactions to raise an alarm or stop the fraudulent transactions but should allow the good orders to flow through seamlessly.

Organizations loses several millions of dollars due to online fraud. The fraudsters use stolen credit card details and place orders in ecommerce site. Organizations ends up losing money and reputation when these payments are rejected by the bank and the credit card owner. On the other side genuine customer transactions should not be marked as fraud and also they should not be made to wait too long for the fraud check.

Methodology

- Exploratory Data Analysis
  - Formulating the dataset
  - Making data visualizations
- Building the Model
  - Creating a python file which builds model based on training data
  - Choosing an optimal model by plotting the ROC (Receiver Operating Characteristic) curve
- Prediction script
- Database
  - To store each prediction the model makes in a database
- Web app
- Get live data
  - Adding examples to the database with predicted fraud possibilities
- Dashboard
  - Web frontend to present results
- Deployment

List of KPIs

- Shipping Time
- Distance between shipping and billing cities
- Quantity of order
- Payment info (Security codes)
- Payment method
- Unauthenticated access (Wrong card details)
- Authorization error while logging in
- Site visits before purchase

Conclusion

An appropriate decision tree model was found which helped in predicting the credit card frauds and further prevent them from happening with an accuracy of 95.92% +/- 2.68%.

It helped not only in detecting such transactions, stopping them but also in predicting them without incurring a huge cost on software system, manual operations team and customer experience.

Future Scope

- Integration of the FraudMiner model which would be built using Frequent Itemset Mining algorithm
  - Frequent itemsets are sets of items that occur simultaneously in as many transactions as the user defined minimum support.
  - It can be done by comparing the number of attributes in the incoming transaction matching with that of the legal pattern of the corresponding customer and the attributes matching with that of the fraud pattern of the corresponding customer.
- Verification using OTP


Thank You