Credit Card Fraud Detection

Table of Contents

Introduction

Credit Card and Fraudulent Activities

- Credit card fraud refers to payment to another account controlled by criminal.
- This project focuses on using credit card activity data to identify credit card frauds.
- Frauds may include authorized (such as scamming) and unauthorized (such as skimming or account take-over)
  - Unauthorized fraudulent activities could demonstrate very different trait when comparing to card owner's usual consumption behavior
  - Authorized fraudulent activities usually would not demonstrate vastly different trait; they could be tracked from both ends (card owner end: owner likely to be deceived; criminal end: suspicious payment recipient).

Data source & analysis

Data source

- The dataset is from Kaggle. Its records are simulated credit card transactions generated from Sparkov, dated from 01/01/2019 – 12/31/2020. This dataset contains over 185k simulated credit card transaction activities, covering 1000 card owners and 800 merchants.
- Link: https://www.kaggle.com/kartik2112/fraud-detection
- The columns could be broadly divided into these types

Data & Variables

Variable Type	Variable name
identifier	“cc_num”: credit card number; identifier for each card “trans_num”: transaction number; identified for each transaction record
Transaction details	“trans_date_trans_time”: date and time of transaction “amt”: amount of this transaction
Customer information	“first”, “last”: first name and last name of card holder “gender”, “job”, “dob”: gender, job and date of birth of card holder “street”, “city”, “state”, “zip”, “lat”, “long”: living address of card holder
Merchant information	“merchant”, “category”: name and category of merchant “merch_lat”, “merch_long: address of merchant
Fraud information	“is_fraud”: class to identify if this transaction is fraud or not

Data Processing

Using the dataset

- Transaction profiling
  - Assumption: transaction patterns in one card is consistent, determined by the card owner. New transactions will likely follow old transaction patterns
  - To-do: build a profile for each card; a profile of transaction habits
  - Fraud: different transaction pattern could imply fraud; card could be operated by other people
- High risk card holder
  - Assumption: authorized frauds; some card holders are vulnerable to authorized frauds
  - To-do: use card owner information
- High risk merchant
  - Assumption: some merchants are high-risk
  - To-do: merchants that seldom show up; merchants highly associated with frauds

Modeling Choice

- The dataset contains a target value (is_fraud). Two methods for fraud detection.
- 1. Supervised Machine Learning
  - Use existing and derived columns to establish a model predicting is_fraud.
  - Concern: this method only identifies known fraud types; vulnerable to new fraud types
- 2. Unsupervised Machine Learning
  - Ignore fraud class; use existing and derived columns to group transactions by similarities; identify fraud by those transactions which are not similar to norm

Data Processing

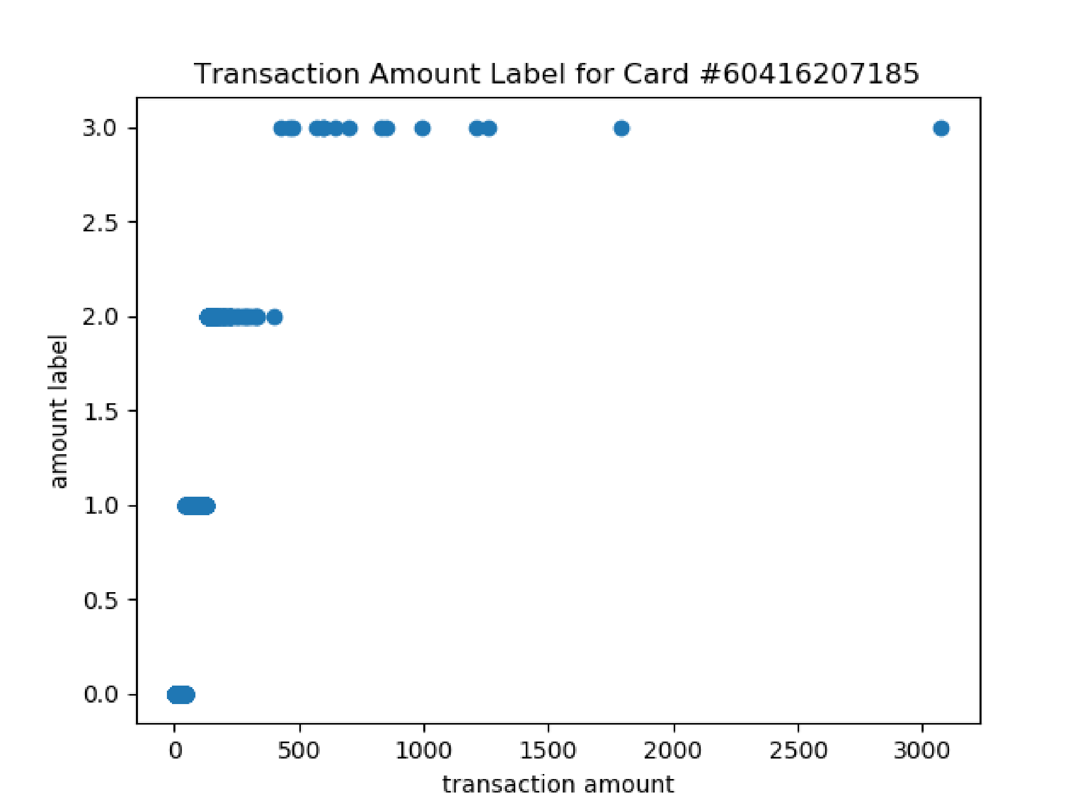
Dividing the dataset: real-world problem

- In practice,
  - Historical data -> process, analyze, cross-validate -> new data -> add to historical data and improve analysis
  - When cross-validating, no future data is attainable
- Divide the data by time
  - Total 2 years of data (01/01/2019 – 12/31/2020) [1.85m activities]
  - First 1.5 years for analysis and cross-validation [1.32m activities]
  - Last 0.5 year as future data (test for model applications) [0.53m activities]
- Imbalanced dataset
  - In first 1.5 years: 7.6k fraud transactions (r. 0.57%); hard to over-sampling/under-sampling with bootstrapping
  - Choose a different metrics in supervised models: Precision-Recall Curve
  - Apply stratified k-fold cross-validation
  - Add class weight in classification models

Profiling based on transactions

- Create derived variables for each card
- Transaction amount:
  - Thresholds for each card: extreme, high, medium, low
- Transaction address location
  - Compare card holder’s living address (latitude and longitude) and merchant location
  - Divide transaction into local, national and international
- Transaction datetime
  - Weekday: Mon, Tue, ..., Sun
  - Time of a day: morning, afternoon, evening, midnight
- Product type
  - No exact product type, approximated by merchant category
  - Create dummy variables for modeling

Labeling Transaction Amount



- Perform operation for each card number, assign four labels
- 3 – extreme
  - Refers to extremely high transaction amount based on the card's transaction history
  - Finding outliers using Z-score
    - Flag all points above $\mu+3\sigma$ (68-98-99 for normal distribution)
- 0, 1, 2 – low, medium, high
  - For the rest of the data, use k-means clustering on transaction amount, k=3
- Figure to the left illustrates amount and its derived label for one card

Profiling based on transactions

- Transaction pattern for each card is profiled: summarized into categorical variables
- Goal: run individual models on each card
- Profiling by customer vs profiling by card
  - One customer may treat cards differently: for example, one would buy more accommodation products with travel cards (more cashback on travel) and more commodity with shopping cards

Risk-to-Fraud

- Association between customer demographics and frauds
- Association between merchants and frauds

Modeling and Analysis

Modeling

- Card profiling
  - Model 1: Random forest (set of models)
    - Dataset: subset of
    - Dependent: fraud class (1, 0); Independent: amount label, address label, weekday label, time label, category dummies
- Customer and merchant risk-to-fraud
  - Model 2: High risk customers
    - Dependent: probability of fraud cases; Independent: customer demographics
  - Model 3: High risk merchants
    - Dependent: probability of fraud cases; Independent: merchant information
- Finalize modeling
  - For each transaction:

  Use model 1 to calculate the probability of fraud from card profile (transaction pattern)

  Use model 2 to obtain the probability of high-risk customers (from coefficients)

  Use model 3 to obtain the probability of high-risk merchants
  - Run final model:
    - Dependent: fraud class (1,0); independent: profile fraud prob, customer risk prob, merchant risk prob