DFE604-2020F: Final Project Proposal
머신러닝을 이용한 신용카드 부정사용 탐지 모델 개발

Seongil Park

Abstract

많은 신용카드 회사들이 결제 사기 방지를 위해 FDS 시스템을 개발하여 운영하고 있지만 대부분 Rule 기반으로 구성되어 있고, 24시간 모니터링 하는 인력을 채용하여 야간 부정 사용에 대해 대응하고 있다. 머신러닝을 통해서 이러한 부정 사용을 방지 또는 탐지할 수 있는 모델을 개발, 카드사와 사용 고객들의 피해를 방지하고자 한다.

1. Introduction

1.1. Motivation

지난 7월 금융감독원이 국회에 제출한 자료에 따르면 신용카드 결제 사기는 최근 3년 간 약 100만건에 달하고, 승인 시도 금액은 약 1680억원이었다. 실제로 결제가 성공하여 부정 사용된 금액만 약 199억원이고 이에 따라 국내 카드사가 부담한 피해 금액 약 115억원이었다. 금융회사들은 FDS 시스템을 구축하여 운영하고 있지만 해커들의 지속적인 공격으로 그 피해는 갈수록 증가하고 있다. 이번 프로젝트를 통해서 신용카드 부정 사용을 탐지하는 머신러닝 모델 개발을 통해서 FDS 시스템이 더욱 고도화 될 수 있는 기반을 마련하고자 한다.

1.2. Related works

현재까지는 룰 기반의 탐지 방법이 많이 사용되고 있으나 최근 머신러닝 또는 딥러닝 기반의 이상탐지 또는 하이브리드 탐지 방법이 도입되고 있다. 주요 머신러닝 알고리즘으로는 규칙 유도(Rule Induction), 랜덤포레스트(Random Forest), 서포트벡터머신(Support Vector Machine), 자기조직화맵(SOM), 은닉마코브모델(HMM), 유전알고리즘(GA), 딥러닝(Deep Learning) 등이 있다. 국외 금융회사들의 머신러닝 기반 FDS 현황을 살펴보자면 아래와 같다.

- **Paypal :** 딥러닝 기반으로 고객 1억7천만명이 발생시킨 40억건의 거래 정보를 학습하여 사기 탐지 수행
- **Sul America :** 보험금 지급 청구의 약 20%가 사기, 남용 등에서 비롯된 것을 파악하고, 보험금 지급 과정에서 정확성, 유효성 등을 확인하고자 딥러닝 기반 시스템을 도입

1.3. Challenges

본 프로젝트에서 사용할 데이터는 매우 불균형한 데이터로 전체 데이터 중 약 0.172% 만이 사기 트랜잭션으로 분류되었다. 이처럼 적은 데이터는 학습을 위해 충분히 필요한 데이터가 필수적인데 단순히 증식하는 방법은 오버피팅을 초래할 수도 있기 때문에 원본 데이터와 피처 값들을 아주 약간만 변경하여 증식시키고자 한다. 이를 통해 SMOTE(Synthetic Minority Over-sampling Technique)를 사용할 예정이다.

2. Datasets

국내 카드사에서 제공된 데이터는 없기 때문에 본 프로젝트에서는 Kaggle의 Credit Card Fraud Detection 경진대회에서 사용한 데이터를 사용하기로 한다.

3. Current status

Kaggle의 데이터셋을 준비하여, 기본적인 데이터 분석을 위한 사전 검토를 마쳤으며, 로지스틱 회귀와 LightGBM을 적용하여 분석을 하기 위해 해당 라이브러리에 대한 테스트를 진행중이다.

4. Goals to achieve throughout this project

한 학기 동안 배운 내용을 실제 프로젝트 수행을 통해서 실제 업무에서 사용할 수 있는 기본 지식을 다지고자 한다.

5. Brief schedule

짧은 기간안에 진행되어야 하는 프로젝트로 약 1.5개월 동안 아래와 같이 진행하고자 한다.

- **11월 :** 데이터 수집, 분석 환경 구축, EDA, 모델 설계
- **12월 :** 모델 구현, 튜닝 및 프로젝트 산출물 정리

6. Comparison with SOTA and baseline

데이터 가공 유무에 따라 정밀도, 재현율, ROC-AUC의 변화를 비교하여 신용카드 부정사용과 같은 재현율이 중요한 모델에서 우수한 성능을 나타낼 수 있는 모델은 어떤 것인지 파악할 예정이다.