Zijun He & Erdun E

Final Project Proposal

COMP 4200 Artificial Intelligence

February 25, 2020

Abnormal Transaction Alert AI System

Problem statement with literature review

Nowadays, with the rapid development of online payment, the Internet finance industry keeps making breakthroughs and innovations. At the same time, the dark side of the web is also growing (Mejia), for example, fraud transactions. Because machines are usually cheaper and more efficient than humans, banks have invested heavily in artificial intelligence to reduce risky transactions, namely AI fraud detection. In our project, our goal is to build models to predict risky transactions by using two given data sets. The first one is a training data set consisting of payment samples with positive and negative labels along with some samples without labels. The second one is a testing data set consisting of samples with positive and negative labels, we need to use this testing set to predict abnormal transactions and to evaluate our models' performance. We choose this project not only because the topic is valuable, but also it is an interesting task for us to try different methods and models that we learned from different scholars. For example, we plan to associate classification models with risk management knowledge and social network analysis (Chiu et al.). Even we can try graph embedding ideas by considering the uniqueness of data sets (Goyal et al.) since each record corresponds to a hyperedge relationship among m vertices, where m is the number of attributes considered. There are only two relationship types: normal and fraud.

Problem analysis

First, we are going to use machine learning methods. We are going to represent the state of the world by using the input of 298 features. It is reasonable since each row of the records from the given data sets consists of 298 features and one label. These 298 features represent the world that our AI will operate upon. We will use these features as input and train our models in order to generate a correct label.

Second, these features of record as a state will generate a new state that is characterized by a label. And for each prediction, we compare our prediction result with the given correct label, if we correctly predict the label, then we say this prediction is good. We also have some methods to evaluate a model's prediction. For example, we can use a confusion matrix to calculate its false positive rate and true positive rate.

What is more, the task environment is partially observable, this is because although we have 298 features, we still can't record all the information of a transaction, some information seems irrelevant, but we don't know if it is really irrelevant since we don't record them, and we don't have chance to analyze them. Besides, it is a single agent since a model will not influence another one. It can be stochastic, for example, although our inputs are fixed, the task environment is partially observable. There might be some useful hidden relationship behind an abnormal transaction but we don't collect. Without observing these important relationships and features, the task environment is stochastic.

If we use our model to predict each testing data, it is episodic since the present prediction won't affect the next prediction. The task environment is static since the environment won't change while an agent is deliberating. In addition, the task environment is discrete because of distinct states.

In the end, for the performance measure, we consider if all fraud transactions can be caught. What's more, we care about the accuracy, since we don't want to confuse users if they are not criminals but they are caught by our models, they will be frustrated. All the features consist of our agent's environment.

Data set or other source materials

The data we will use is from the ATEC competition website of Ant Financial, a subsidiary of Alibaba. atec_anti_fraud_train.csv is the training set, and atec_anti_fraud_test.csv is the test set. In these documents, there will be thousands of transfer records, which will make the calculation difficult. These records have the following three characteristics. The first one is sample imbalance. While 99.99 percent of trades are normal, the number of abnormal transactions is very small. Second, some transactions have no labels, this is because they are failed by the company's risk control system, but this part of data is extremely important. Third, lawbreakers constantly change their way to fool the AI system. What is more, we have too many features which are 298, and we don't know their exact names and meanings. According to these characteristics, the main tasks for us is to understand algorithms, adjust parameters and integrate models, we don’t need so much professional background since we are not given by meanings of these features.

We can import data sets through python tools and packages. We will consider extracting some useful features or combine some related features. We will also deal with the imbalance, for instance, regarding testing set, since the original dataset has a very small percentage of fraud cases (since unlabeled records are probably fraud), it makes more sense to have a higher percentage of fraud cases in the test data (e.g., 30% to 50%). For example, we could use 60% of the total dataset for training. For the remaining 40% records, take all the fraud ones, plus a corresponding number of good transactions chosen randomly. We suspect that their test data may have closer percentages of two types of records than the training data. Likewise, we may try to adjust the percentage in the training data too. Having a bigger fraction of fraud records may affect the trained model. What’s more, we can separate types of users because different users group has different characteristics. For instance, some users are merchandises, they transfer their money densely in a short period of time. However, some users are normal people, like students, they won’t densely transfer their money, so it is better for us to divide them into different groups. Moreover, we may use two steps to enhance our accuracy, we may predict upon normal samples first, and then we consider predicting upon abnormal samples.

Last but not least, we may use the decision tree as a basic model, and then try some methods including random forest, Ada Boost, and GBDT. We will try to combine GBDT and DNN as well.

Deliverable and Demonstration

At the end of the project, the team will produce an abnormal transaction alert AI system. we will compare several models that will be able to process a large number of transfer records and identify problematic records to alert customers. The data with specified features can be connected to this AI system to obtain different transfer predictions.

Evaluation of results

First, we will compare real labels with our prediction results. We can create a confusion matrix and calculate the false positive rate and true positive rate. By using these values, we are going to draw a ROC curve (If we choose different threshold values, we can calculate different pairs of FPR and TPR, then we can connect them to get the ROC). We also define the following TPRs:

TPR1: TPR when the FPR is 0.001;

TPR2: TPR when the FPR is 0.005;

TPR3: TPR when the FPR is 0.01.

Grade of the model = 0.4 * TPR1 + 0.3 *TPR2 + 0.3 * TPR3

This evaluation method is common in the risk management area.

Major components and schedule

First, we are going to get the data sets. Then we need to read some papers and observe the data (one week). Third, we are going to decide the models we use and preprocess these data (three days). And then is model training and we should try multiple ways to improve our models’ performance (one week), In the end, we will write the report (four days, by March 28th). Model training includes several models such as random forest, GBDT, and neural networks. We will include some methods like cross-validation, parameter optimization.

References

Ghadban, Khaled. “How to Start Using AI to Combat Money Laundering.” Bobsguide, 26 Jan. 2020, www.bobsguide.com/guide/news/2018/Nov/19/how-to-start-using-ai-to-combat-money-laundering.

Mejia, Niccolo. “AI-Based Fraud Detection in Banking – Current Applications and Trends.” Emerj, Emerj, 21 Jan. 2020, emerj.com/ai-sector-overviews/artificial-intelligence-fraud-banking/.

Raj Shroff. “Artificial Intelligence for Risk Reduction in Banking: Current Uses.” Medium, Towards Data Science, 16 Jan. 2020, towardsdatascience.com/artificial-intelligence-for-risk-reduction-in-banking-current-uses-799445a4a152. Accessed 2 Feb. 2020.