Project Design

Credit Card Fraud detection using Machine Learning and Deep Learning models

Subject: CM3070
Student: 190128812

Template: Machine Learning and Neural Networks – Public dataset

Table of contents

Introduction

Frauds perpetrated in digital payments, and in particular using credit cards, are a constant threat to users and cause damages for billions of dollars every year.[1]
It is therefore important to have a secure system that allows users to use their credit cards in absolute safety; for this reason it is necessary to have an efficient system for detecting fraud in real time.

Overview of the project

My project aims to create a system for the real time detection of fraud attempts in credit card payments, using Machine Learning and Neural Networks techniques.

In order for the fraud detection system to be used in a real-world scenario, it will have to:

- be effective in detecting fraud
- produce few false positives
- be fast in classifying payment transactions.

Since transactions have to be executed very quickly, a system that is too slow in analyzing new transactions would unacceptably slow down operations and would in fact be unusable in a production system. If we consider that the number of transactions processed every second is in the order of thousands, we can guess how crucial it is to have components working in real or near real time.

Domain and users

The project falls within the domain of digital credit card payments and the software developed will be installed on a server owned by a banking institution or a company that handles digital payments.
The users, in the strict sense of the term, will be the companies themselves, who will use the software for real-time fraud detection. In reality, however, the concept of user extends to all persons who will use, albeit transparently and unknowingly, their credit card to make a payment online or at a physical Point Of Sale (POS).

The idea for this project came from both a work interest, as I currently work for a multinational company that handles digital payments, and a personal interest, as a credit card user.
Since the number of fraud attempts in this sector is constantly increasing and evolving in the methods used, as a user I am concerned about the risks involved in using credit cards, especially in online payments. Understanding therefore what methods financial institutions use to prevent fraud, and how these methods could be improved, is of great interest to me.

Project structure

The project aims to find a model that, by combining different Machine Learning (ML) and Deep Learning (DL) techniques, is able to detect fraud attempts in credit card payments, generating as few false positives as possible and having analysis performance of new transactions in the order of milliseconds.

Different techniques and algorithms will be used to create AI models, taking inspiration from the research reviewed, and their performance will be compared in terms of both fraud detection and execution time (both for data training and 'live' transaction analysis).

The ultimate goal is to create an unsupervised Deep Leaning model that eliminates the need for prior labeling of data, thereby saving considerable time.

The project starts with the analysis of the available dataset and data cleaning.
Since payment transactions may contain sensitive data, I will necessarily have to check for their presence and remove them if necessary, to avoid ethical and privacy issues.

The dataset used[2] is available on Kaggle.com and includes about 300,000 transactions, of which only about 0.2% are transactions labeled as fraudulent. This large imbalance between the two classes of the dataset implies the need to use oversampling techniques of the minority class, so that AI algorithms can perform optimally.
I will initially test the best known oversampling techniques (SMOTE, ...) and then compare them with more advanced methods, such as GAN neural networks, and its variants.

The new balanced dataset will then be used for training models using statistical ML algorithms (Logistic Regression, SVM, KNN, etc.) and finally for training an unsupervised Deep Neural Network model.
My ultimate goal is to test whether unsupervised DNN models, currently state of the art, are indeed superior in terms of fraud detection and in terms of execution speed.

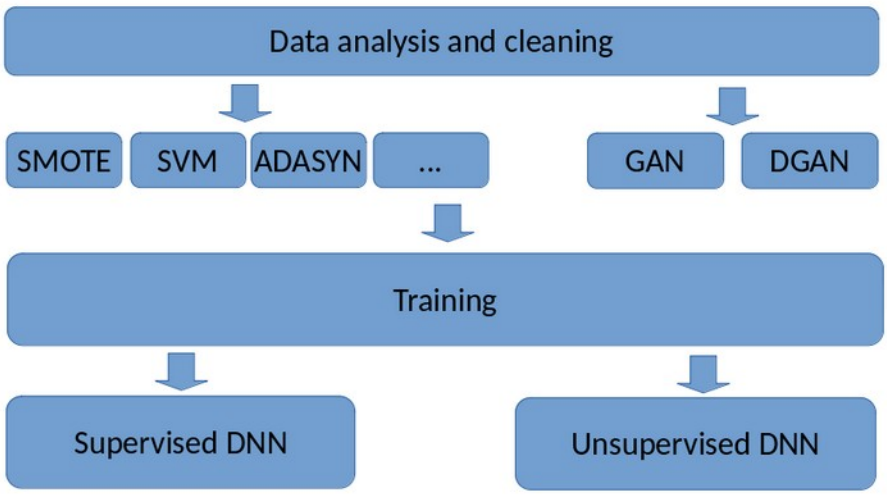


Figure 1: Project structure

The final phase of the project will be devoted to model evaluation, which I will discuss in the dedicated section below.

Technologies and methods

This project will be described in a Jupyter Notebook, where descriptive parts will alternate with parts of python code.
The descriptive parts will serve to clarify the purpose of the project, explain its various steps, introduce theoretical concepts and present final conclusions.
The code part will be written in Python, using native and third-party libraries for the realization of artificial intelligence models.

The difficulty of this project is both in reproducing techniques used in previous research, for which no code exists, and in combining them.

Several of the techniques and algorithms used will necessarily require their study, as they have not been taken into account during the lessons previously held; this entails the need for precise planning of the time to be dedicated to the various parts of the project.

Some of Python Libraries used:
Keras, TensorFlow, Numpy, Sklearn, Pandas, Matplotlib

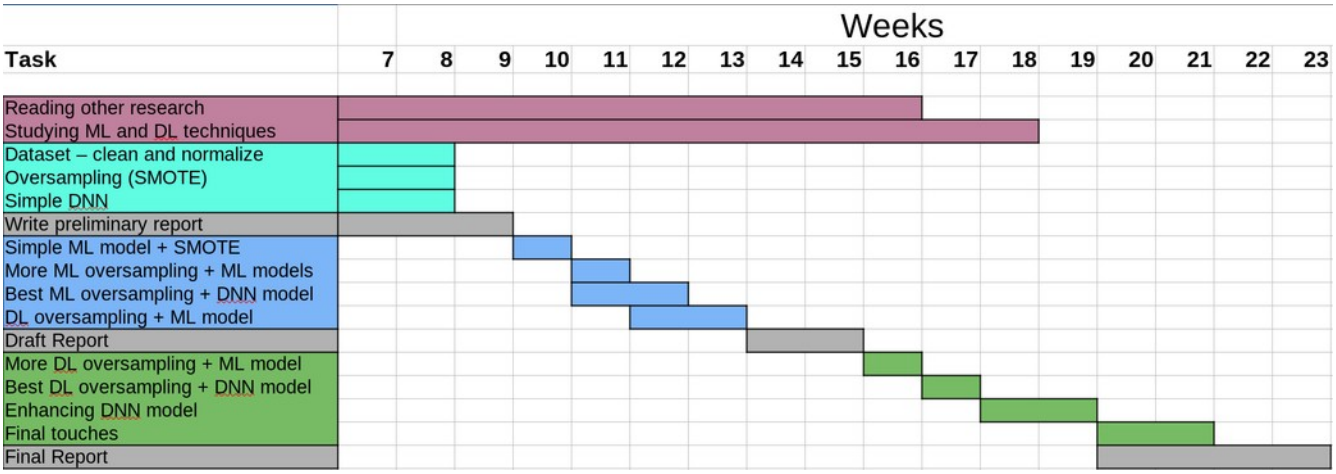
Some of the techniques and algorithms used:
Oversampling techniques (SMOTE, ADASYN, ...)
Logistic Regression, SVM, kNN, AdaBoost, etc.

Work plan

For the realisation of the project, I will have to continue reading previous research to see if there are any interesting techniques I can use to improve the model I am creating. I will also have to study the theory of many of the techniques that I found in the research and that I want to use, since they have not been covered in the course of study or for which I have a basic knowledge.
In my work plan I have therefore decided to continue with the reading of the research up to week 16, and with the study up to week 17; at that point I will no longer introduce any new techniques or algorithms and will concentrate on improving the model created up to that point.
In parallel I will obviously have to continue with the development of the fraud detection system.
For the preliminary report, since the development of the most difficult part of the project is required, I will create a Deep Learning Network for fraud detection, but using SMOTE for oversampling the data, instead of using a DGAN for this purpose, which is the final goal.

In the following weeks I will create a Machine Learning model using different statistical algorithms for evaluation, evaluating the performance of other data oversampling techniques, until the creation of a GAN network that performs this purpose.

Starting from week 17, I will start building the final model, evaluating the best method of oversampling the data, in combination with an unsupervised DNN for fraud detection.
The last weeks will be used for writing the final report and for correcting and improving the project details.



Evaluation

The models created will be compared in their performance in detecting fraud but also in the speed of analyzing new transactions. The time required to train the models themselves will also be examined, in order to get a complete picture of the resources required to use the models in a real-world scenario.

For the evaluation of the detection performance, I will use different evaluation methods (accuracy, precision, F1, ...), also analyzing the confusion matrix to check the amount of false negatives (FN) and false positives (FP) detected, which, although in different terms, represent a cost for the payment management company.

Initially I will compare the performances of the models created to find the best combination between oversampling technique and ML algorithm for fraud detection.
The comparison will take into great consideration the time performances, eliminating the models considered too slow, even if with better detection performances.

Then I will evaluate the use of GAN and DGAN for data oversampling, and compare them with the results obtained by the other methods.
The final model will use the best evaluated oversampling technique, in combination with a Deep Neural Network.

The comparison will test whether Deep Neural Network models prove superior to Machine Learning models for this specific purpose, and which combinations of techniques are most effective.

References

[1] payment-card-fraud-losses-reach-32-34.
[2] Credit Card Fraud Detection Dataset. Retrieved from
https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud