Deep Learning

Anomaly Detection using Autoencoders
Proposal Phase

Problem Statement

Anomaly detection is the process of pointing out outliers in data. These outliers can be held differently according to the observations. In medical purposes, it can be crucial to point out these outliers as they formulate the search problem, detecting a rare disease. In other fields, like communication, it is necessary to remove outliers from data. Outliers can occur in data collection for several reasons for example:

- Lightning strike while collecting data from a phone
- Electrical outage while collecting data from a device connected to power outlet

These types of outliers can affect a model training negatively. Whether they are the target or not, anomalies need to be detected.

Motivation

Anomaly detection is a difficult problem. Common machine learning techniques like density based clustering work poorly when data is non-linearly separable. On the other hand, neural networks are difficult to train for anomaly detection because of the sparsity of the class of interest. The breakthrough happened with deep learning models like AutoEncoders (AE) and Generative Adversarial Networks (GANs). Using AE will enable us to detect different sorts of anomalies like fraudulent credit cards, transactions, identities, etc. With the help of some extensions and data preprocessing, we can apply anomaly detection over streaming data like CCTV and images.

State of the art

There are different models working with Variational AutoEncoders (VAE), Memory Augmented AutoEncoders (MemAE), Deviation Networks (DevNet).

The following is the Area Under the Curve (AUC) for the surveyed papers:

- LSTM-VAE: 0.87
- DevNet: 0.916
- MemAE: 0.941

Survey

Many models were surveyed for specific types of detection. We found that the anomaly detection is a more general and difficult problem.

LSTM-VAE

This model works on multimodal signals obtained from a feeding robot. Instead of a normal VAE, the model uses LSTM in the encoding and decoding. The model then uses an anomaly detector (more on that later) that takes the threshold parameter from the latent layer.

DevNet

This model is not related to AE; however we can use some of its ideas. This model proposed the usage of an Anomaly Scoring network and a Gaussian prior. A vector anomaly score along with its prior parameters is then evaluated in a Z-Score deviation loss function.

MemAE

This model acts on the fact that AE can sometimes generalize on anomalies and sometimes generate anomalies as its reconstructions. As proposed, this model adds a memory in between the Encoding and Decoding stages. This memory holds the prototypical

representation of normal inputs. Reconstruction of anomalies is more restricted and the generalization effect is minimized.

Model Description and Updates

In building our model, we will take on the different approaches from the three models:

1. Using LSTM in encoding and decoding
2. Using a memory element
3. Replace the typical anomaly detector with a deviation loss function

A typical anomaly detector measures the difference between the original encoded input and a reconstructed decoded output. It then compares this difference to a threshold set by the latent hidden layer. On the other hand, the deviation loss function takes into account the probabilistic properties of the sample space, which is more effective.

We think that using the extensions of each model will work on different types of problems and generalize on the usage of the model.

Model Evaluation

The model will be evaluated on two criterias:

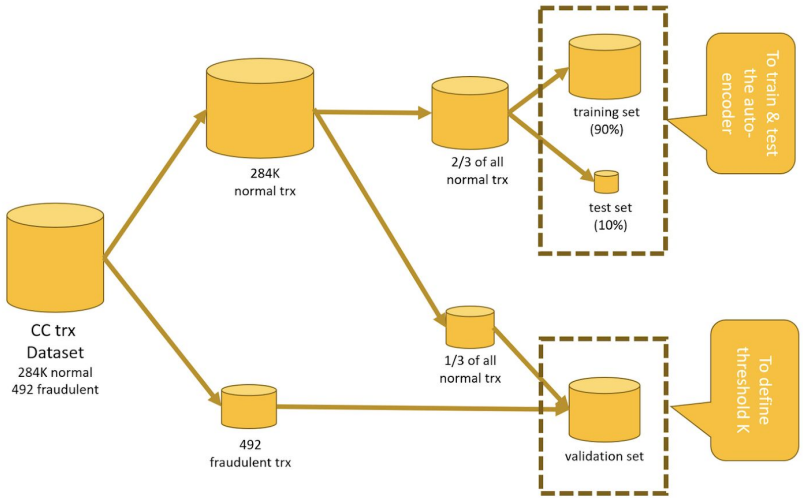
- Can it outperform the three surveyed models
- How well it performs on different problems involving anomaly detection

Following the steps of the DevNet paper, we can observe the performance on different datasets that deal with outliers like: fraud, marketing campaigns, medical purposes, and security. Plots will be mainly ROC plots. Metrics will focus on F1 since the data is naturally skewed.

Datasets Survey and Description

We surveyed datasets that involved software logs, fraud transactions and fraud credit cards. We chose a dataset for fraud detection of online transactions. This dataset was posted on a very recent competition on Kaggle thorugh IEEE-CIS. This dataset has the benefit of having many samples and also not a small number of anomalies. It still needs some preprocessing and cleaning.

In our approach, we would like to split our train, test, validation sets using a specific method as shown in the figure below.



Grad statement

Our graduation project is about performing sentiment analysis on arabic tweets. The dialect used is Modern Standard Arabic (MSA). The task aims to use Narrow Convolutional Neural Networks (NCNN) to capture syntactical relevance between words. In order to do that, words need to be mapped. We use a NLP technique called word embedding where a single word is mapped to a 100-D or 300-D vector depending on the use case.

Resources

Dataset:

https://www.kaggle.com/c/ieee-fraud-detection/data

Dataset description:

https://www.kaggle.com/c/ieee-fraud-detection/discussion/101203

LSTM-VAE:

https://www.paperswithcode.com/paper/a-multimodal-anomaly-detector-for-robot

DevNet:

https://www.paperswithcode.com/paper/deep-anomaly-detection-with-deviation

MemAE:

https://www.paperswithcode.com/paper/memorizing-normality-to-detect-anomaly-memory

Training-Test-Validation Data Workflow:
https://www.dataversity.net/fraud-detection-using-a-neural-autoencoder/#