Anomaly Detection using AutoEncoders

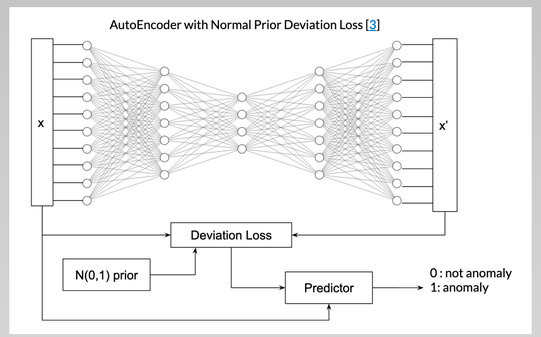
Abdelrahman Ibrahim, Mahmoud Gamal

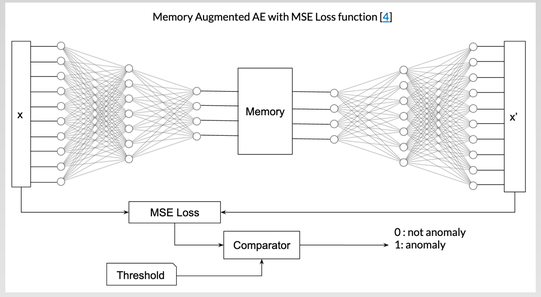
Faculty of Engineering, Alexandria University

Problem

- Motivation: Detect abnormal behaviour
- Abnormal behaviour (outliers) can be found in bank transactions, credit cards, medical research, and communication
- Technique: Using AutoEncoders to successfully reconstruct transactions and sequences
- AutoEncoders can generalize and start generating anomalies themselves

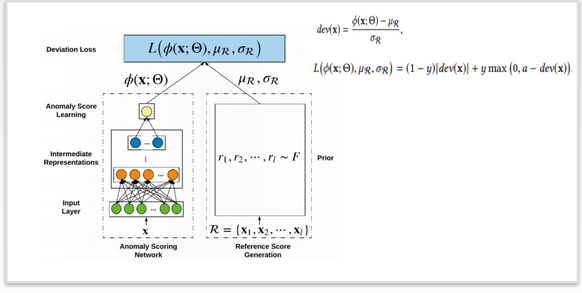
Models





Model Description

- Deviation Loss AE (DevAE) is a normal AE
- Loss function used is Deviation Loss Function
- Prior distribution is Normal with mean 0 and variance 1
- Output is predicted based on the anomaly score (threshold is learned)



Results

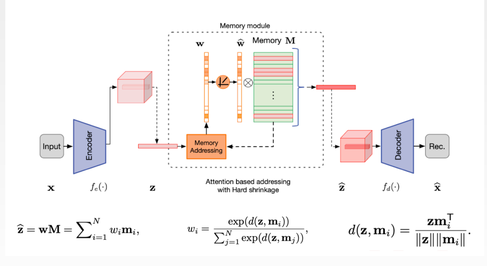
Table: Test Results

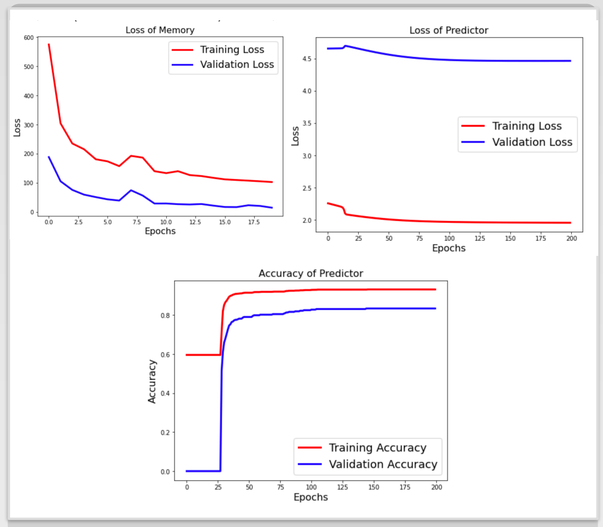
Model	MemAE	AE-DEV
Loss	3.02	0.2
Accuracy	0.979	0.998
Precision	0.679	0.002
Recall	0.681	0.848
F1	0.68	0.002

Table: Test Results on only anomalies

Model	MemAE	AE-DEV
Loss	4.8	4.39
Accuracy	0.686	0.851
Precision	1.0	1.0
Recall	0.686	0.848
F1	0.814	0.916

- Memory Augmented AE (MemAE) is a regular AE with the latent layer replaced with a memory element
- Loss function used is MSE
- Output is predicted based on a threshold



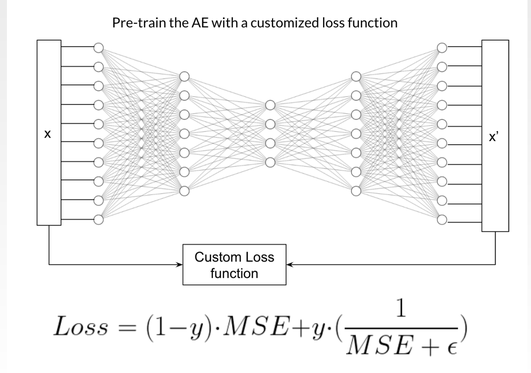


Discussion

- AE are trained on non anomalous data in order to capture the features that constitute a normal input
- Abnormal inputs' reconstructions are very different from the inputs themselves which is a sign of an anomaly
- A good estimate of how far are these constructions is the mean squared error and cosine proximity.
- MSE yielded better results because its range is not bounded unlike the cosine proximity

Other Approaches

- Pre-training the Normal AE with a custom loss function
- Penalize negative (anomalous) reconstructions more then normal reconstructions



Data

Fraud detection on transactions data found on Kaggle

- IEEE Transaction fraud [1]
- Credit card fraud detection [2]

Training

- MemAE and the AE in DevAE are trained on all non anomalous data
- The predictor of the DevAE is trained over anomalous and non-anomalous data
- MemAE threshold is a hyper-parameter set based upon the largest linear separation
- The Normal AE in DevAE is pre-trained using either the MSE or the custom loss function.

Conclusion

- Curse of dimensionality is a real issue and requires domain knowledge. It is very hard to pinpoint a set of features on which a model can learn if a behaviour is anomalous or not.
- It is not necessarily true that using the memory and dev loss together improve the detection problem
- One can enforce a probabilistic distribution on the output of his network and judge by performing statistical tests
- Oversampling and undersampling are very effective go to solutions when it comes to unbalanced data
- Training the model on several stages until it is fully complete is a useful technique.
- In situations like this a trade off between Precision and recall arises.

Refrences

1. https://www.kaggle.com/c/ieee-fraud-detection/data
2. https://www.kaggle.com/mlg-ulb/creditcardfraud
3. https://arxiv.org/abs/1911.08623
4. https://arxiv.org/abs/1904.02639