State-of-the-Art Report
Anomaly detection using Autoenders and Methods to Improve them

Cozmina Scorobete
Advisory: Darian Onchiș
Facultatea de Matematică și Informatică
Universitatea de Vest, Timișoara, România

January 17, 2025

Overview

Introduction

1. **Motivation:** Personal interest in anomaly detection using autoencoders

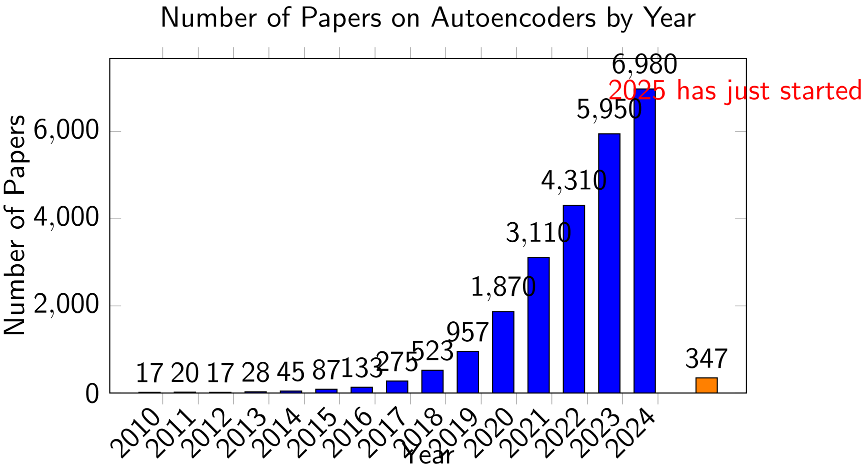
Introduction

1. **Motivation:** Personal interest in anomaly detection using autoencoders
2. **Context:** How does XAI impact and improve the accuracy of machine learning models(unsupervised learning - autoencoders)

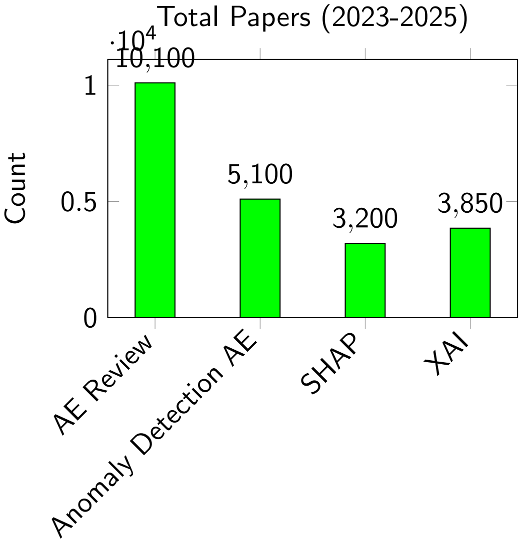
Introduction

1. **Motivation:** Personal interest in anomaly detection using autoencoders
2. **Context:** How does XAI impact and improve the accuracy of machine learning models(unsupervised learning - autoencoders)
3. **Aim:** The main purpose of the report is to verify if XAI methods impact the accuracy and performance of the model

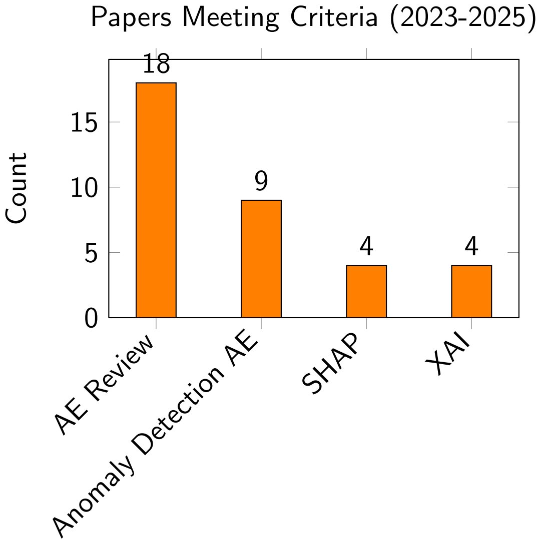
Pappers from 2010-2025



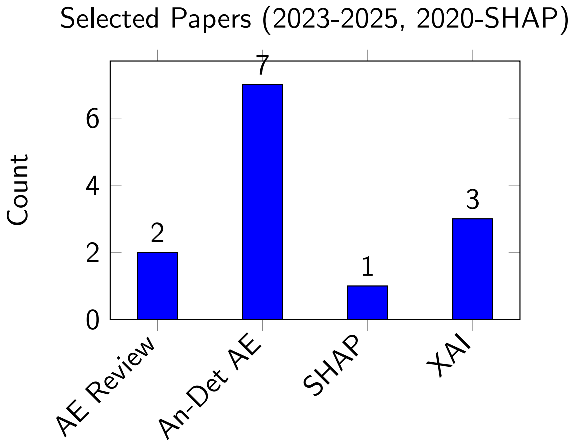
Paper Selection



Paper Selection



Paper Selection



Methodology Overview

1. **Data Selection:** CICIDS2017 dataset as the benchmark the same dataset used in [RZ21].

Methodology Overview

1. **Data Selection:** CICIDS2017 dataset as the benchmark the same dataset used in [RZ21].
2. **Model Building:** I have decided to try to reproduce the work presented in [RZ21]

Methodology Overview

1. **Data Selection:** CICIDS2017 dataset as the benchmark the same dataset used in [RZ21].
2. **Model Building:** I have decided to try to reproduce the work presented in [RZ21]
   - **Model 1** Autoencoder architecture for anomaly detection with traditional structure.

Methodology Overview

1. **Data Selection:** CICIDS2017 dataset as the benchmark the same dataset used in [RZ21].
2. **Model Building:** I have decided to try to reproduce the work presented in [RZ21]
   - **Model 1** Autoencoder architecture for anomaly detection with traditional structure.
   - **Model 2** Add feauture selection and than train a traditional model.

Methodology Overview

1. **Data Selection:** CICIDS2017 dataset as the benchmark the same dataset used in [RZ21].
2. **Model Building:** I have decided to try to reproduce the work presented in [RZ21]
   - **Model 1** Autoencoder architecture for anomaly detection with traditional structure.
   - **Model 2** Add feauture selection and than train a traditional model.
   - **Model 2** Optimize the model with SHAP.

Methodology Overview

1. **Data Selection:** CICIDS2017 dataset as the benchmark the same dataset used in [RZ21].
2. **Model Building:** I have decided to try to reproduce the work presented in [RZ21]
    - **Model 1** Autoencoder architecture for anomaly detection with traditional structure.
    - **Model 2** Add feauture selection and than train a traditional model.
    - **Model 2** Optimize the model with SHAP.
3. **Evaluation Metrics:**

Methodology Overview

1. **Data Selection:** CICIDS2017 dataset as the benchmark the same dataset used in [RZ21].
2. **Model Building:** I have decided to try to reproduce the work presented in [RZ21]
   - **Model 1** Autoencoder architecture for anomaly detection with traditional structure.
   - **Model 2** Add feauture selection and than train a traditional model.
   - **Model 2** Optimize the model with SHAP.
3. **Evaluation Metrics:**
   - Accuracy, AUC, Precision, Recall, F1-score.

Comparison of Approaches (Part 1)

Method	Challenges	Strengths	Metrics
Standard Autoencoder [SY14]	1. Struggles in datasets with high noise. 2. Does not have feature correlation.	1. Good on nonlinear datasets. 2. Efficient from a computation view.	Lorenz Dataset: Autoencoder AUC = 0.85 vs PCA AUC = 0.6. Improved anomaly detection with PCA.
RDA [ZP17]	1. High computational cost. 2. Sensitive to hyperparameters.	1. Effective in noisy data.	MNIST Digits: 30% better anomaly detection accuracy than standard autoencoders for high-noise data. Structured Anomalies: F1-score = 0.64 compared to Isolation Forest (F1 = 0.37).
LSTM Autoencoder [PLV19]	1. Performance correlated to hyperparameter tuning.	1. Effective on sequential datasets. 2. Better performance than classic methods.	Rare Sound Detection: 87% accuracy.

Comparison of Approaches (Part 2) I

Method	Challenges	Strengths	Metrics
SHAP_Model [RZ21]	1. High computational cost. 2. Requires careful dataset selection.	1. Improves anomaly detection by focusing on key features. 2. Provides interpretability by explaining which features contribute to anomalies.	CICIDS2017 Dataset: Accuracy = 94%, AUC = 0.969.
Model_1 [RZ21]	1. Inefficient due to redundant and irrelevant features. 2. Lower performance.	1. Can handle all features without preprocessing or selection.	CICIDS2017 Dataset: Accuracy = 81.9%, AUC = 0.819.

Comparison of Approaches (Part 2) II

Model_2 [RZ21]	1. May exclude important features. 2. Redundant features might not always degrade performance, leading to inconsistent results.	1. Reduces feature space, improving model efficiency.	CICIDS2017 Dataset: Accuracy = 84.3%, AUC = 0.843.

Comparison with My Model

Method	Paper	My Result
SHAP_Model (2021)	Accuracy = 94%, AUC = 0.969.	, AUC = 0.7194.
SHAP_Model (Baseline): Model_1	Accuracy = 81.9%, AUC = 0.819.	Accuracy = 93.17%, AUC = 0.9740..
Model_2	Accuracy = 84.3%, AUC = 0.843.	Not evaluated.

: The result from training on a part of the dataset

Comparison of Results

Method	**Paper**	**My Result**
SHAP_Model (2021)	Accuracy = 94%, AUC = 0.969.	,Could not compute.
SHAP_Model (Baseline): Model_1	Accuracy = 81.9%, AUC = 0.819.	Accuracy = 42%, AUC = 0.65568
Model_2	Accuracy = 84.3%, AUC = 0.843.	Accuracy = 42%, AUC = 0.5867.

: The result from training on the full dataset

Discussion

- Which model performed best?

Discussion

- Which model performed best?
- Was my research conclusive?

Discussion

- Which model performed best?
- Was my research conclusive?
- What would happen if anomalies are present in the training data?

Conclusion

- The comparative analysis shewed that SHAP could improve a model but that still remain to be decided in further research. I have analyzed different kind of models like LSTM-based autoencoders, RDA and Robust Deep Autoencoders, the paper present an analysis with their streamlets and challenges.

Future Work

- Try the SHAP model on better hardware

Future Work

- Try the SHAP model on better hardware
- Try different approaches on the same dataset

Future Work

- Try the SHAP model on better hardware
- Try different approaches on the same dataset
- Try different XAI methods to optimize the autoencoder

Thank You

Oleksandr I Provotar, Yaroslav M Linder, and Maksym M Veres.
Unsupervised anomaly detection in time series using lstm-based autoencoders.
In *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, pages 513–517. IEEE, 2019.

Khushnaseeb Roshan and Aasim Zafar.
Utilizing xai technique to improve autoencoder based model for computer network anomaly detection with shapley additive explanation (shap).
arXiv preprint arXiv:2112.08442, 2021.

Mayu Sakurada and Takehisa Yairi.
Anomaly detection using autoencoders with nonlinear dimensionality reduction.
In *Proceedings of the MLSDA 2014 2nd workshop on machine learning for sensory data analysis*, pages 4–11, 2014.

Chong Zhou and Randy C Paffenroth.
Anomaly detection with robust deep autoencoders.
In *Proceedings of the 23rd ACM SIGKDD international conference on knowledge discovery and data mining*, pages 665–674, 2017.