Hessisches Kompetenzzentrum
für Hochleistungsrechnen

CYWARN – Entwicklung von Strategien und Technologien zur Analyse und Kommunikation der Sicherheitslage im Cyberraum

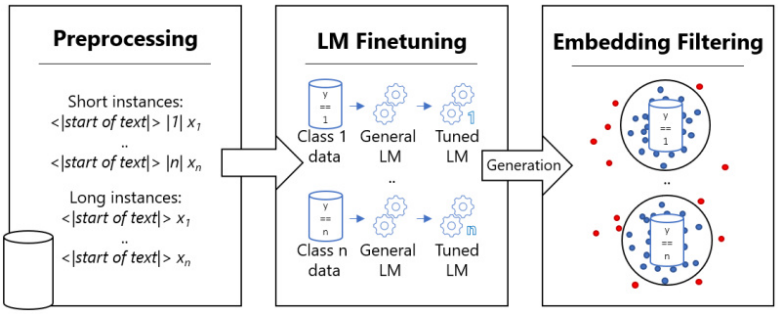


Figure 1: The process of the data augmentation method

Introduction

The increase in complex cyber-attacks illustrates the vulnerability of society and information infrastructure. In addition to technologies for information and IT security, early warning systems and reaction strategies are needed to strengthen civil security. So-called Computer Emergency Response Teams (CERTs) are the central point of contact for preventive and reactive measures in the event of IT security incidents. Due to the confusing information situation in cyber-attacks, the evaluation and target group-specific preparation is a major challenge for these teams. The aim of the CYWARN project is to support CERTs with new strategies and technologies for recording, analysing and communicating the cyber situation. A demonstrator will be created that enables the automated collection of public data sources as well as data evaluation with credibility analysis and information prioritization. The use of resource intensive machine learning and especially deep learning methods is necessary for the evaluation.

Methods

In the CYWARN project, textual deep learning methods are used for the analysis of the various data sources. These classifier methods are enriched, for example, by sophisticated data augmentation methods that artificially enlarge the training data. In addition, we use novel Few Shot Learning techniques so that the classifiers can be quickly trained on upcoming vulnerabilities or other cybersecurity incidents. These Few Shot Learning approaches essentially rely on large pre-trained language models that have an initial knowledge and understanding of text resources. In our project, such a language model is adapted for the field of cyber security in order to increase the suitability to the field of application. As a further novel approach, metadata-

Project Manager
Markus Bayer

Researchers
Dr. Marc-André Kaufhold, Philipp Kühn and Thea Riebe

Principal Investigator
Prof. Dr. Christian Reuter

Project Term
2021 - 2022

Clusters
Lichtenberg Cluster Darmstadt

Software
TensorFlow, PyTorch

Institute
Department of Computer Science

University
Technische Universität Darmstadt

JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN
TECHNISCHE UNIVERSITÄT DARMSTADT
UNIKASSEL VERSITÄT
Philipps Universität Marburg

based indicators and explanatory deep learning will be combined in order to establish transparency for algorithmic decisions and to investigate its influence, acceptance and user confidence in the algorithms and the entire CYWARN demonstrator.

Results

The first results of the project were successfully realised with the Lichtenberg Cluster. In a first step, we developed and tested different methods for data augmentation. From these results we deduced that a textual generation method is best suited for the artificial enlargement of datasets. In addition, we have trained a comprehensive language model on a judiciously selected cybersecurity dataset, which forms the basis for further classifiers. This language model will be used, for example, in Few Shot Learning, which will be the next goal of this project. In a separate phase, we also experimented with using the National Vulnerability Database to train a severity prediction classifier. Severity levels are a valuable indicator for assessing how important a piece of information is to a cybersecurity professional. In a later phase of the project, we will also analyse explainable AI methods to increase the transparency of the algorithms.

Discussion

The current results of the project are very promising. The developed method for data augmentation leads to very good performance improvements. It is very valuable for deep learning research as a whole, but requires a lot of computing resources, which makes it difficult to use in smaller research groups or companies. The cybersecurity-specific language model can be very important for the research field. Especially since we show that it is more suitable for cybersecurity tasks than general language models currently used in this domain. This language model will be the basis for the Few Shot Learning approach that is currently being developed. Unfortunately, training a classifier for severity score prediction did not yield the hoped-for results. Nevertheless, we will try to look at the problem from a different perspective by including more sources.

Publications

Bayer, M.; Kaufhold, M.; Buchhold, B.; Keller, M.; Dallmeyer, J.; Reuter, C.: Data Augmentation in Natural Language Processing: A Novel Text Generation Approach for Long and Short Text Classifiers, Int. J. Mach. Learn. & Cyber. (2022) https://doi.org/10.1007/s13042-022-01553-3

Last Update: 2022-05-02 17:14