Anomaly Detection in SMS Applications

Robert Chavez, Kiera Conway

CSC 723 – Machine Learning for Cyber Security – Project Topic Proposal – Spring 2023

Proposal Content

Our group's final project for the Spring 2023 semester of CSC 723 will focus on machine learning models that are geared towards anomaly detection. The chosen field of study for our machine learning models is Short Message Service (SMS) spam. We will be leveraging various SMS spam data sets to train, test, and analyze various classification algorithms to find the most precise option to help determine if an SMS is considered spam. SMS has become one of the most popular sources of medium used for marketing and advertising. We feel that it is important to develop an understanding on how one can utilize machine learning to accurately detect SMS spam. The precision and accuracy will be determined using a combination of model scores, confusion matrices, and other applicable model metrics. While the math deriving most of these metrics will be computed using the Python library sklearn, any formulas used in the project will be thoroughly explained for reader clarity. Furthermore, the training and machine learning algorithms will be created using the Python scripting language and submitted alongside the final project report.

All scripts written for this project will be created using the Jupyter Notebook environment Kaggle. Our group has determined the chosen format to be submitted will be in the ".ipynb" Kaggle file format. Kaggle was selected as our main environment due to the abundance of data sets, the ability to directly import said data sets, and the facilitation of collaboration between group members. While each algorithm will be trained and tested in a separate notebook, the final report will consolidate the data in an organized manner. In an effort to better assist our team's coordinated efforts, we will leverage a shared GitHub repository for any additional materials which require group collaboration such as outlines, notes, and resources.

Since we will be classifying discrete, fixed, and binary values, such as SPAM vs HAM, our group will use various Supervised Classification algorithms. The three algorithms chosen to test, train, analyze, and compare results of are K-Nearest Neighbors (KNN), Decision Tree, and Naive Bayes (including Bayes' Theorem to calculate the joint density of dependent events). While each algorithm script may contain additional unique libraries, the primary libraries utilized in our project will be numpy, pandas, and sklearn. Our group will ensure each algorithm will be trained and tested using the data set SMSCollection.csv, which is derived from the spam-or-ham data set from Kaggle. Prior to testing, the data set will be thoroughly reviewed in Python by the group. The purpose of this review will be an initial effort to obtain general information related to the data set, such as relevant specific observations and statistical information. Post review, the team will ensure each step during the training and testing process will be explained using code examples for support and documentation purposes. Lastly, all three algorithms will be tested to compare which is the most suitable option for the SPAM classification.

All team member contributions will be equal as we share responsibility for project activities not limited to research, scripting, consolidation, writing, and reviewing. To ensure team success and accountability, the team set up a tentative schedule to track progress, milestones, and weekly meeting notes via a scheduled Discord call. The team will leverage these weekly meeting sessions to discuss plans and strategies relevant to the project. All research materials are to be submitted to a shared 'Data Dump' folder. In addition, script work is done via a shared notebook and written documents are regularly updated on our shared GitHub repository. Furthermore, the algorithms and report sections will be split evenly to maintain workload symmetry. As previously mentioned, all tools have been selected with cooperation as

the driving factor. In conclusion, we hope our project findings and research work towards minimizing SMS spam advertising and marketing by leveraging today's powerful tools and algorithms.

References

[1] A. S, "Spam (or) Ham," 20 February 2023. [Online]. Available: https://www.kaggle.com/datasets/arunasivapragasam/spam-or-ham.

[2] "ACM Journals," [Online]. Available: https://dl.acm.org/.

[3] "Science Direct," 2023. [Online]. Available: https://www.sciencedirect.com/.

[4] [Online]. Available: https://ieeexplore.ieee.org/Xplore/home.jsp.