DSC 680

Author: Felipe Castillo

Term: Spring 2023

Spam Detector in UiPath Robotic Process Automation

Topic : Robotic process automation (RPA) is an important player in the 21st century. UiPath has recognized the need to incorporate artificial intelligence (AI) into their processes. The integration of RPA and AI can help solve various issues, including spam detection.

Business Problem: RPA on its own is limited to non-changing processes. Automation requires a repetitive nature, and bots are non-intelligent entities that cannot distinguish between changing factors. For example, catching email spam would be almost impossible with RPA alone. Email spam has plagued businesses and individuals, causing harm. Therefore, a joint RPA/AI project aimed at catching spam is needed.

Datasets: The data that will be gathered mostly consists of spam email content, and the objective is to obtain as many real and spam emails as possible. One great source of data sets is Kaggle's spam and ham data set.

Method: I plan to use two different classification models to distinguish between emails that are spam and those that are not. To do this, the emails will need to be cleaned and inspected for optimal results. Once the models have been trained, they will be connected to the UiPath AI center. After connecting to the AI center, I will build a pipeline to use in UiPath studios. I will create a simple state machine that takes in emails and tests them against the created models. This should produce a classifier for spam and non-spam emails. The goal is to filter out spam while allowing non-spam emails. The aim is to build confidence in an intelligent bot process.

Ethical Considerations: There is a chance that an important email could be flagged, causing businesses to lose trust in the robot's ability to distinguish between spam and non-spam. I almost fell for a convincing Facebook spam once. If the email spammers keep changing up their spam to look more realistic, could the bot pick it up? Additionally, there is a question regarding business retraining ability. If I offer a way for a human to inspect the email and approve or deny, if they mess up, it could set a precedent that the bot will not predict correctly. Either way, to make it production-worthy, it will require a lot of training.

Challenge/Issue: There are many challenges that come with this project. First, I have never integrated AI into a bot before. It requires me to request the enterprise version of UiPath, which gives me access for two months. Secondly, UiPath requires a certain format and folder structure to be able to integrate it with UiPath. Additionally, this method is somewhat new and there is not a lot of material out there on how to connect everything effectively. If I get stuck, it will be hard to get unstuck. Lastly, testing it will also be a hassle because I have never used the machine learning integration offered by UiPath Studios.

Reference:

Building ML Packages. UiPath AI Center™. (n.d.). Retrieved March 17, 2023, from https://docs.uipath.com/ai-fabric/v0/docs/building-ml-packages

Mahmood, M. S. (2021, June 30). *ML classifier performance comparison for spam emails detection- part 1*. Medium. Retrieved March 17, 2023, from https://towardsdatascience.com/ml-classifier-performance-comparison-for-spam-emails-detection-77749926d508

Banoula, M. (2023, March 10). *Naive Bayes classifier - machine learning [updated]: Simplilearn*. Simplilearn.com. Retrieved March 17, 2023, from https://www.simplilearn.com/tutorials/machine-learning-tutorial/naive-bayes-classifier

Yiu, T. (2021, September 29). *Understanding random forest*. Medium. Retrieved March 17, 2023, from https://towardsdatascience.com/understanding-random-forest-58381e0602d2