***[Computer Engineering and Sciences]***

| **Project Name** | **Framework to Analyze Behavior of Social Media Bots** |
| --- | --- |
| Team Lead: | Cody Manning |
| Team Member(s): | Gabriel Silva, Liam Dumbell, Cody Manning, Nickolas Falco |
| Faculty Advisor(s): | Dr. Khaled A. Slhoub, Department of Electrical Engineering and Computer Science, Florida Institute of Technology |

**\*\*Do not change font size or text color above this message/delete this before completion. The category will be put in by Staff after submission \*\***

**Project Description:**

Social media has become a driving force in many people's lives. Connecting with people has never been easier than it is in modern society. Whether it is meeting new people, connecting with old friends, or even showcasing yourself to potential employers; social media is a huge factor in how we socialize with people. This new technology brings new challenges however; as social media has become increasingly infested with entities known as ‘bots’. Bots are nonhuman pieces of software that are created for the purposes of automating tasks. A person may create a bot that automatically translates what a user says in Spanish into English, for example. Not all bots are created to help people however. Some people have created bots that serve malicious purposes. These bots act like real people, and may be used to steal information or annoy users who unknowingly interact with them. The rise of AI companions like ChatGPT have made this kind of thing even more prevalent. Our framework is created for the purpose of being able to detect these bots, and possibly differentiate them from the bots that are created for beneficial purposes. The framework was created to work on the ‘Reddit’ social media platform, but the backbone and ideas of the project could be extended to other social media platforms, with some tweaking depending on the features of the social media it is being adapted to.

**Features:**

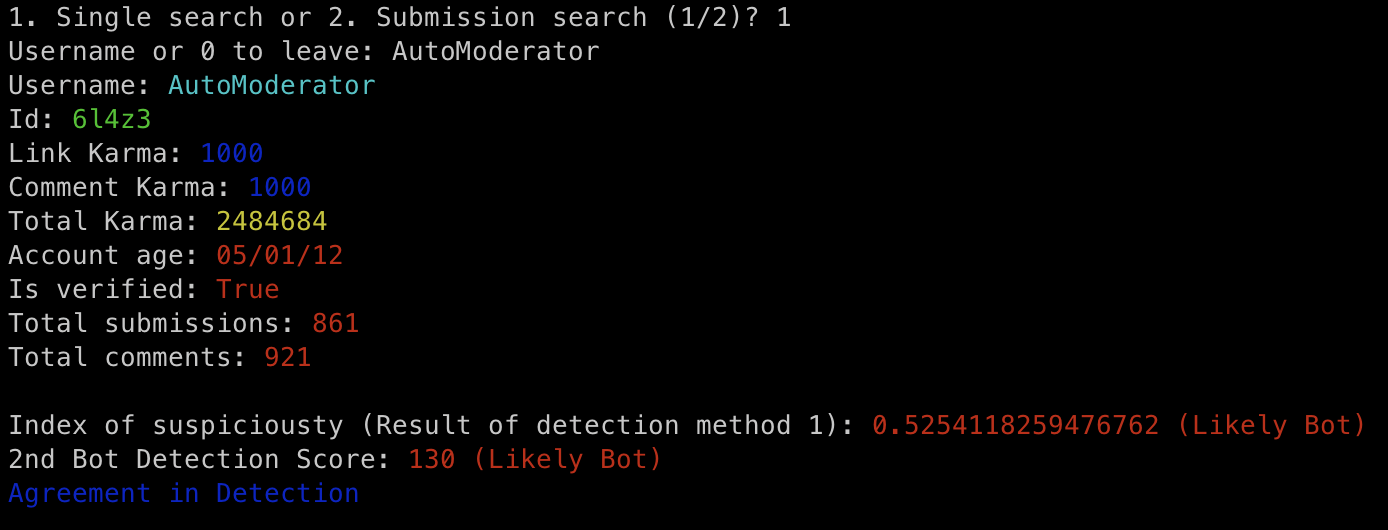
The user will be able to deploy the framework on Reddit using a specific subreddit (which is a collection of topics created by users). The user will also be able to select a specific user (by typing in the suspected users Reddit username). If the user wants to search a specific subreddit, the framework will scan through top posts, newest posts, or the posts that are most popular in a short timeframe. It then asks the user how many posts they would like to search for, and how deep in the posts (how many users) it would like to evaluate. When this is done, it will print out all of the users in the posts it grabbed and give a score based on the likelihood of them being a real human being, or a bot. The framework uses more than one method for detecting bots, and will tell you the results in an easy to understand, color coded result. If the results are unanimous, the framework will say as such, otherwise; it will allow the user to decide at their own discretion. The framework will also give the user insights on whether the given bot is a ‘good’ bot (one made to help) or a ‘bad’ bot (one made to harm).

**Evaluation:**

When designing this framework, accuracy was the key for our measurement of success. It doesn’t matter much if the results come quickly if they are wrong. To achieve this, we measure against a master list of known bots (which were scraped from several sources, GitHub and Reddit itself in particular). We were shooting for about an 80% accuracy method in detecting whether a user was a bot. When using our known bot list, and a list of known real human accounts, the accuracy rating was well within our desired output. Our timing desire was no more than about 10 seconds per account lookup, and this was unfortunately not really feasible within the context of how the program functioned. It really came down to speed or accuracy, and the team decided that accuracy was what we wanted to focus on.

**Major Challenges:**

There were a lot of challenges we encountered and overcame during the process of this project. Particularly detecting bots and distinguishing the good from the bad bots. This is still a widely researched topic in Computer Science, so we were working blind for a lot of this. We found that one detection algorithm alone was simply not sufficient for proper detection accuracy, and implemented a second detection algorithm to supplement the first. Realistically, the more detection algorithms that get added the better. For the future of this project, we should get as many as we can. The second and biggest challenge we faced was detecting the ‘nature’ of the bots we found. There is no real clear answer on this, so we had to work with the information we were given. One notable observation was the inclusion of links. We couldn’t find a good reason for bots to direct you outside of the Reddit platform, so it was immediately flagged as suspicious if they wanted you to leave the site and go somewhere else (especially if the outside link was obscured with a link shortener). There is no perfect science for this project, so it is something that needs to be built on more in the future.

****

**Figure 1: Searching a known bot by username**