My robot wants to buy a pet

Student: Cassie Qing Tang (if20281@bristol.ac.uk), Project Type: Research
Supervisor: Dr. Matthew Edwards
University of Bristol, Department of Computer Science

1. Project Introduction

This project targets the growing threat of online pet scams by creating an automated system to waste scammers' time and resources, aiding in scam identification and prevention. Following extensive development and testing, a four-week experimental deployment against pet scammers unveiled and refined effective scam-baiting tactics.

2. Methods

The whole system was developed in Python and based on an19352's GitHub repo [1], comprises four crawlers and an email autoresponder, customized for pet scam site detection and response:

1. petscam_crawl: Crawls petscam.com [2] for the latest scam webs listings using requests and bs4 Library.

2. contactpage_crawl: Extracts contact forms from scam sites via heuristics.

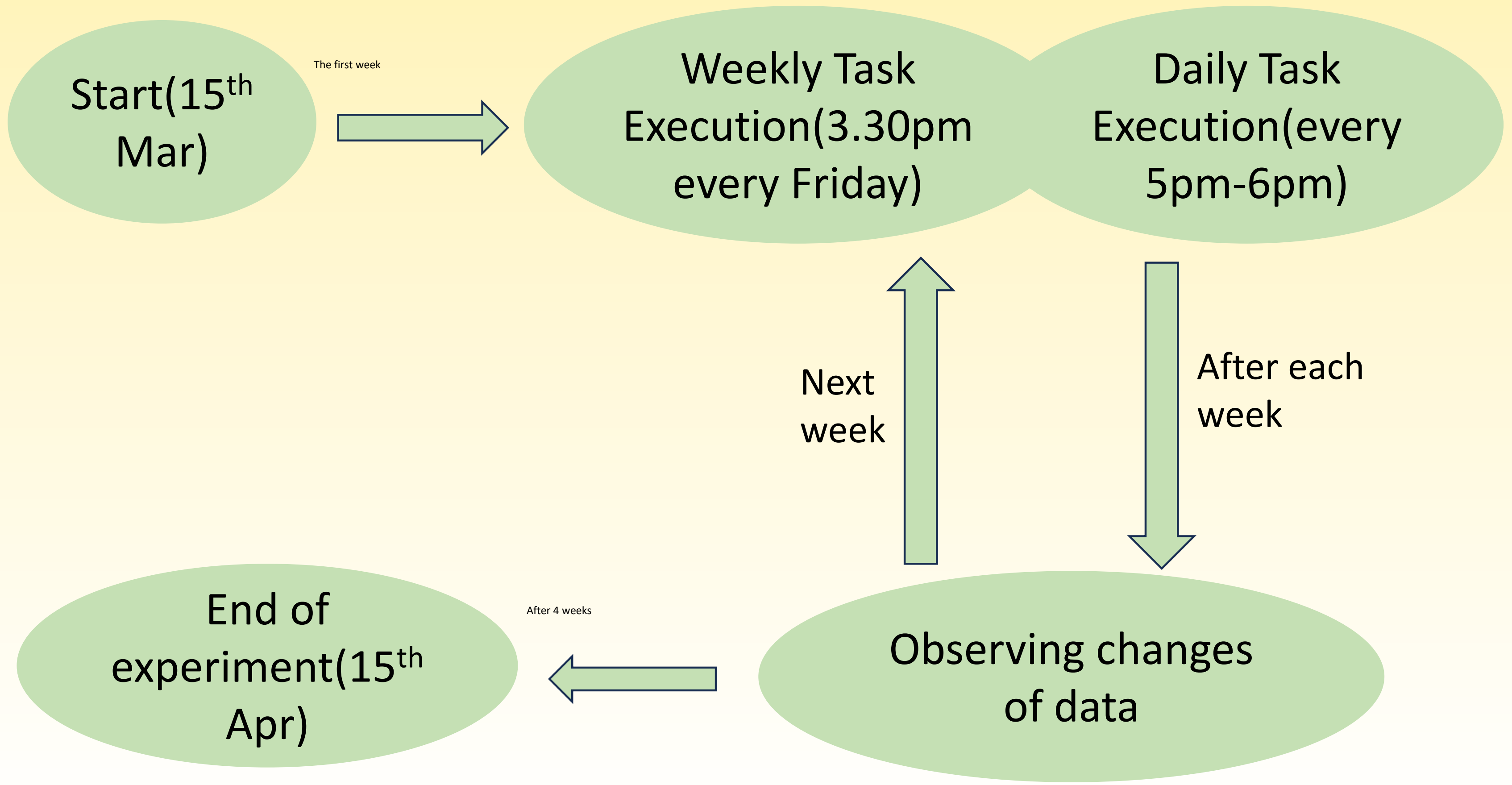
3. formfill_crawl: Uses Selenium WebDriver for simulating human browser interaction, filling, and submitting forms on scam sites with complex structures.

4. email_crawl: Retrieves and crawl the inbound scammer emails from the Mailgun mail server under my own domain management.

5. corn.py: Integrates with gpt-4-0125-preview API, using four reply strategies to auto-respond to scammers, including newbies, bargainers, curious investigators, and impatient enthusiasts.

3. Experiment Execution

The experiment lasted for 4 weeks (15th Mar – 15th Apr). Weekly tasks included obtaining and filling out the contact pages of the most recently listed pet-scam websites. Meanwhile, daily tasks involved crawling and automatically replying to emails from scammers.

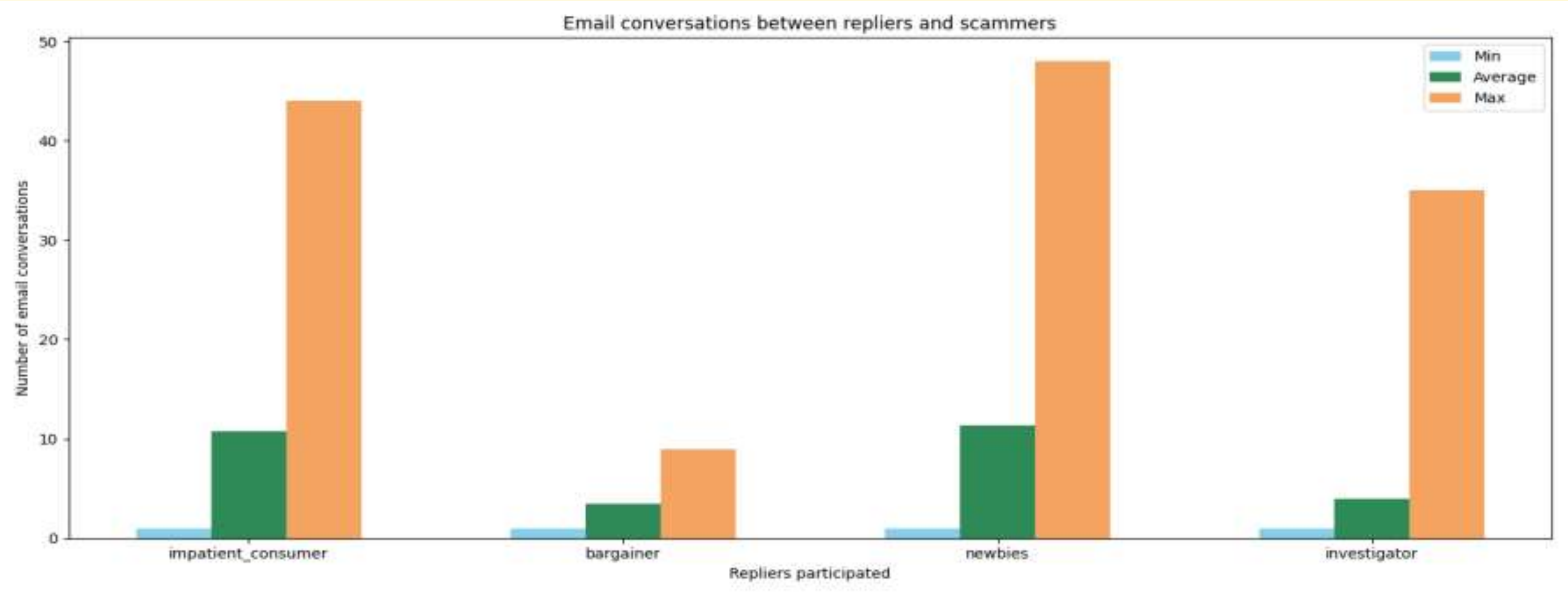

Start(15th Mar)
The first week
Weekly Task Execution(3.30pm every Friday)
Daily Task Execution(every 5pm-6pm)
After each week
Observing changes of data
Next week
After 4 weeks
End of experiment(15th Apr)

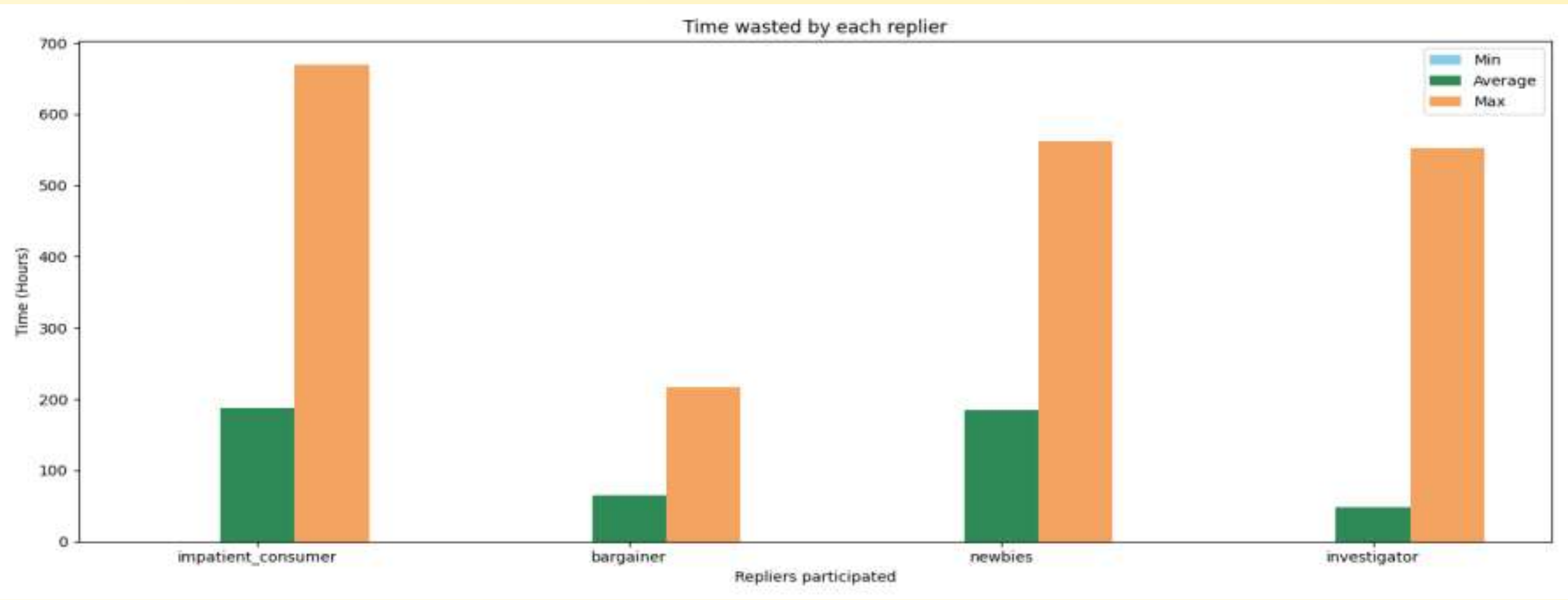
4. Results & Findings

After a one-month scam-baiting experiment, AI repliers with the 'investigator' personality interacted with 13 scammers, 'newbies' with 17, 'bargainers' with 16, and 'impatient consumers' with 18. Analysis of the email volume and the time scammers spent in conversations resulted in two bar graphs, involving the extremes and averages.

The graphs reveal that 'newbies' and 'impatient consumers' exhibit high engagement, with 'newbies' sending up to 48 emails in some dialogues. 'Impatient consumers' consistently spent more time in bait scams. Relatively, the interaction time of 'newbies' was a bit lower. 'Investigators' showed variability, occasionally leading to lengthy exchanges. However, 'bargainers' demonstrated a generally mediocre performance across metrics.

Ultimately, the 'impatient consumer' strategy proves most effective, frequently engaging and significantly wasting scammers' time, with 'investigators' potentially excelling in certain strategic encounters.





5. Conclusions & Future Directions

In conclusion, this project effectively combats the rise of online pet scams by employing an automated system designed to deplete scammers' resources and deter fraudulent activities. Over a four-week experimental phase, four robotic responders consistently engaged scammers, wasting at least a month of their time. Dozens of scammers continued to interact with the system even after the experiment concluded. This not only aids in scam prevention but also refines scam-baiting strategies, contributing valuable insights into the fight against non-delivery fraud and advance fee fraud.

The future direction of this project may focus on integrating the script for filling non-delivery fraud websites with other systems that can classify fraudulent advertisements or websites. This could include the code for automatic detection of pet scam websites [3].

References

[1] https://github.com/an19352/scambaiter_back
[2] https://petscams.com/
[3] https://github.com/Ronel-Mehmedov/dissertation2021

University of Bristol