Final Exam – Essay

Name: Bryan Orville Audric

NIM: 2602160750

1. This question asks about your personal opinion regarding the result of your paper:
2. Describe the weaknesses and limitations of your paper

The tittle of my project is “Detecting Phishing URLs using Machine Learning Models based on Different Feature Filtering Methods”

Here are some weaknesses and limitations of my paper

* Lack of phishing and malware link data, resulting in a low amount of training data for both labels (Weakness and Limitations)

The dataset contains 651191 URLs which are divided into 428103 benign or safe URLs, 96457 defacement URLs, 94111 phishing URLs and 32520 malware URLs. Looking at the number of URLs in other URL types such as defacement, phishing and especially malware, it is significantly lower compared to benign, which may severely impact the evaluation results of the model. It is clear to see that the lower value on precision, recall and f1 score especially on phishing and malware classification may be caused due to this issue. Hence, this imbalance of data can also be considered as limitation (insufficient number of defacement, phishing and malware URLs) and weakness.

* The comparison with articles/conferences that can be used to support the validity of our paper is too general. (Weakness)

It is apparent that the related works I cited was too general, in a way that they are still connected/related to the paper’s objective, but it was not specific enough. Such example would be the paper that I included is a paper that discusses the utilization of deep learning for phishing detection. It is still related to our project since we have the same exact goal. However, the methodology that we propose are slightly different, hence, it was not specific enough to be cited.

* The lack of discussion on computational efficiency and scalability of each method (Weakness)

The goal of our paper is to introduce a way to reduce the number of features using feature filtration methods, hence the model can train with less features, resulting in shorter time consumption and lower complexity. However, the impact of model training process with those subsets of features especially on computational efficiency was not deeply analysed and discussed.

* The framework of my research might not produce the same results in the coming years (Limitations)

The characteristics of phishing URLs will vary from one year to the next. As the culprit is getting better at replicating benign or safe URL, the framework that I proposed might not work if tested on the newest phishing tactics.

1. Explain how you are going to address the weaknesses if you have more time and how you are going to address the limitations for your future work.

* At the time of writing and conducting the research, I was still inexperienced hence I overlooked the potential problem that can be caused due to the imbalance of dataset. Ideally, I would have to try several datasets, models and methodology to see how it turns out before writing the paper. However, at the time of writing, there was not enough time to do all of that. Instead, I was forced to write the paper based on a single attempt of research. If I had more time, I would try several datasets, models, and methodologies as well as reading more research papers to get better understanding on the process before writing the paper. By doing this, I can improve the research process, write a paper that is more comprehensive and specific to further ensure the validity of the research. This would also help prevent the issue of overlooking such mistakes (Imbalance dataset) and would further solidify the research results.
* To address the limitations, I would either find an adequate dataset, combine several datasets or balance out the dataset if the data was imbalanced as mentioned previously. As mentioned previously, the phishing tactics especially with the use of URLs might invalidate the current framework as the culprit is getting better at replicating the benign or safe URL. If I choose the same objective or goal for my future work, I will shift from detecting phishing attempt by URL to detecting phishing attempt by analysing the entire web using machine learning models. This will ensure less false positives or negatives cases that can arise due to the culprit adaptability of creating fake benign or safe URL. If I choose a different topic for my future work, I will have to further analyse the impact of my research idea and comparing it to other that has done the same before conducting and writing the research paper, ensuring the results can be hugely beneficial to others.

1. This question asks about your personal opinion regarding the peer-review system:
2. Present your opinion regarding the absoluteness and the correctness of the result in a paper accepted by a peer-reviewed journal/conference.

In my perspective, the absoluteness and the correctness of the result in paper accepted by a peer-reviewed journal/conference is not guaranteed as the occurrence of these factors is possible. Such factors would be:

* Human error – Failure to realize or ensure that the paper’s research process, experimental design, data analysis, etc is properly documented
* Bias – The results of the research might be confirmed and accepted due to the bias of the peer reviewer
* Reproducibility issue – The results of the research are not able to be reproduced because the peer reviewer overlooked an unrealistic factor that contributed to the results

While having these possible issues during peer-review, the system is still necessary to further validify the integrity and the quality of a research paper.

1. Based on your understanding of the peer-review system, do you think peer-review system is needed while there is already a massive amount of unreviewed preprint articles? (read <https://doi.org/10.7554/eLife.83889> for more context)

Why?

What do you think are the true roles of Peer-review in this modern age? Explain your

answer!

As mentioned previously, I do believe peer-review system, especially in academic research, is still necessary to further validify the integrity and the quality of a research paper. Some reasons that support this statement are:

* Quality Control - to identify and correct research flaws, maintaining the integrity of and reliability of the scientific research
* Constructive Feedback – peer-reviewers provide valuable feedback that can improve the clarity, integrity and impact of the research
* Gatekeeping - similar to quality control, peer-review system is necessary to filter out low-quality or fraudulent research. This is why some unreviewed preprint article and especially news lacks integrity and are either low-quality or fraudulent.

In these modern ages, the true roles of peer-review are as follows:

* Facilitating Open Science preventing the need of gatekeeping

Modern peer review is adapting in this modern age to support open science initiatives. Platforms like eLife are promoting transparency by making peer reviews public, eliminating the existent of traditional accept/reject decisions. This openness helps to share the nuances of scientific evaluation more broadly

* Ensuring Reproducibility

As mentioned previously, the reproducibility issue that arises from fraudulent research has been a concern especially in this modern era where information spreads quickly across the internet. By evaluating whole research paper critically, it ensures the integrity, reliability and reproducibility of the research

* Enhancing Collaboration

Publicly available peer-reviews encourage more collaborative approach as it provides more transparent feedback that can be used to further improve the research work

* Supporting Career Development

Researchers that have the works properly validated through peer-review process, can benefit from their works being recognized and respected.