CIS 700 Machine Learning and Security Spring 2021

Theme : Adversarial text generation :Adversarial machine learning applications in Text Analysis

- **Our theme for the project this semester is related to a high evolving area called Adversarial machine learning. This is an area between cyber security and machine learning. We will talk more about the subject through some lectures.**
- **Rather than starting a code from scratch, in this project, you will select an AML code from one of the links below (Based on Python or R languages).**
- **Make sure that the code can compile with you with no problems before you confirm your selection. For Assignment 1, the assignment will focus on making a demo of your own of the code and explaining it. In future HWs, you will be asked to expand on that project.**
- **The selected code (GAN AML) should demo an algorithm or method for two main tasks/ (1) automatic text generation and (2) automatic text manipulation.**
- **Reserve your project selection in the Google Document as no two students can pick the same project. Feel free to pick any project from github.com, Kaggle, etc. as far as it is related to AML text.**

1. https://github.com/search?q=%22Adversarial+text+generation%22
2. https://paperswithcode.com/task/text-generation
3. https://github.com/williamSYSU/TextGAN-PyTorch
4. https://github.com/weilinie/RelGAN
5. https://github.com/ivokun/VGAN
6. https://qdata.github.io/deeplearning4discrete-web//Generate-Text/
7. https://becominghuman.ai/generative-adversarial-networks-for-text-generation-part-1-2b886c8cab10
8. https://www.topbots.com/ai-research-gan-vae-text-generation/
9. https://becominghuman.ai/generative-adversarial-networks-for-text-generation-part-2-rl-1bc18a2b8c60
10. https://becominghuman.ai/generative-adversarial-networks-for-text-generation-part-3-non-rl-methods-70d1be02350b?gi=ecd35a575d2c
11. https://www.nyit.edu/files/engineering/SOECS_REU2018_PosterPresentation_AdversarialTextGenerationForGooglePerspective.pdf