Reflective Question 1

Yong Yu

Department of Electrical and Computer Engineering
University of Victoria)
Victoria, Canada
yongyu1@uvic.ca

I. Reflective Question 1

In recent days, machine learning and cybersecurity are both trending topics around the world. Large amount of data available to us can have a large impact on some of the security issues. Some of the traditional solutions may not work as well as it used to. In 2016, the large amount of user data in social media was used to generate fake news made a huge impact on the US residential election [1], and we being using the traditional voting system for many years. Our goal is find how will data science and machine learning can help avoid or solve some cybersecurity issues. In the research, we will focus on how data science or machine learning can help defence the malware attack nowadays. The research will give the introductions of malware attack and some data science knowledge includes some machine learning techniques, and introduce what are some of the traditional ways that used to handle the malware attacks. Explain why some of the solutions may be outdated due to the current state of technologies. Finally, the research goes on to explore the potential solutions for malware attacks that take the advantages of data science or machine learning [2] and explain the advantages or disadvantages of the data science/machine learning solutions over the tradition solutions and discuss some of the possible machine learning solution frameworks [2].

This topic is interesting to me and my partner because we both get to research on something we are not familiar with. The number of malware attacks are always growing every year. As the Internet gets more functionalities, we are able to store many critical information in the browser, such as our CRA information or the bank information etc. One way to access these private data is through malware attacking. As we can image, the malware attack can caused some serious problem. If we can adapt the trending technologies such as data analysis and machine learning to preserve or solve the critical security issues such as malware attack, it will be very important in the feature. The ability to adapt the trending technologies to solve the trending technical issues is also very helpful in my personal career life.

References

[1] H. Allcott and M. Gentzkow, "Social media and fake news in the 2016 election," *Journal of economic perspectives*, vol. 31, no. 2, pp. 211–36, 2017.

[2] I. H. Sarker, A. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big Data*, vol. 7, no. 1, pp. 1–29, 2020.