Thesis Project Portfolio

Machine Learning in Cyber Security

(Technical Report)

Methods to Prevent Unfairness from Emerging in Machine Learning Algorithms

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Callie Hartzog

Spring, 2022

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

(Executive Summary)

Using Machine Learning as a Tool for Moral Good

Machine learning is a complex field that is constantly evolving and contributing solutions to all aspects of society. The automation of data analysis offers many benefits in streamlining technical systems. Specifically, machine learning algorithms and techniques can be used to improve current cyber security practices. However, with this automation comes great drawbacks. Automation takes judgment out of the hands of humans, who have the capability of recognizing ethical issues with data while computers cannot. With this, there exists a conflict between the efficiency of machine learning algorithms and their ethical standards. These algorithms need to be regulated in order to prevent inaccuracies and ethical issues.

The technical portion of my thesis focuses on the contributions machine learning can make towards improving cyber security. Machine learning algorithms have the capabilities of recognizing patterns in data that are not easily perceivable to the average human. This strength of machine learning can be used to analyze the transmission of data between machines to see when abnormal traffic patterns occur that may indicate some form of a cyber attack. This technique would potentially prevent new cyber attacks whose patterns may be unknown to current cyber defense systems.

In my STS research I look into common ethical issues with machine learning algorithms

in the fields of crime, finance, and medicine. Each ethical issue is connected to a specific type of bias in order to understand the specific ethical issues with these algorithms. Once the algorithms are categorized by bias type, it is easier to see where the ethical issues originate from. Some have issues stemming from improper data collection and usage, while others lack vital historical information. Overall, more human regulation and oversight with machine learning algorithms is needed to decrease unfairness.

The project as a whole demonstrates machine learning as a tool for societal improvement, but helps highlight that engineers cannot place blind faith in their creations. It is easy to see all the good machine learning does for society, from performing jobs humans are unable to do to helping increase the efficiency of technology. However, seeing only the good that algorithms do and refraining from investigating any negative consequences they could have creates serious problems for many minority groups. It is the duty of an engineer to ensure that a piece of technology does not infringe upon the rights of others in its implementation. Creating technology that perpetuates the social status quo is simple, but engineers should question the ethics of creating out of simplicity instead of creating out of a sense of moral justice.