Thesis Project Portfolio

The Application of Artificial Intelligence on Cybersecurity

(Technical Report)

Applying Explainable Artificial Intelligence in the Field of Cybersecurity

(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

Jacqueline Ellen Lainhart

Spring, 2024

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Introduction

Cybersecurity is an important aspect of computer science and helps protect the data and identities of individuals as well as organizations. The scope of the internet and technology widens everyday while also widening the potential threats and attacks that can occur. People have their whole lives—social security numbers, banking information, interests—stored online. There exists a trust to protect that data. The motivation was to discover aspects of cybersecurity where there can be improvement. In both the technical and STS research paper, the focus was on how artificial intelligence (AI) can help make cybersecurity tools more effective. The technical paper mentions using quantum computing. The STS research paper had a slightly diverging focus with explainable artificial intelligence.

Technical Research

The technical portion of my research produced a comprehensive exploration of the current and potential use of AI in relation to cybersecurity. Through the utilization of AI, algorithms that provide real-time detection can be developed. This is done with extensive model training with data about user behavior, their network logs, and previous attacks. The proposed solution to improve current AI tools further would be by using quantum computing. However, using quantum computing for cybersecurity poses a threat to encryption keys. Therefore, proactive measures were explored such as regulations and quality assessments. By producing proactive measures for a post-quantum world, we further improve our current AI tools while mitigating the great harm that implementing quantum computing can do for AI in cybersecurity.

STS Research

For the STS research paper, I delved into the implementation of explainable artificial intelligence (XAI) for cybersecurity to ensure transparency and accountability for AI tools and lessen the flaws that AI can have. This research looked at the different XAI methodologies that would be best applied for cybersecurity. XAI can help address current issues with AI by making its inherently black box nature become more white box. By making the decisions that an AI system makes understandable, it allows AI to reach a larger audience and gain trust in cybersecurity systems. This lets even non-AI experts be able to utilize AI tools and conclude whether their outputs are valid.

Conclusion

Both the technical and STS research papers explored the same topic but had different ways to improve it. Combining AI and cybersecurity with a focus on quantum computing or XAI can see significant changes in the cybersecurity field. Having done both papers, a vision for the future of AI and the nearer future of AI starts to unfold. With more research into these specific areas, the existing AI can only become better making everyone and their information safer.