Defending our Cyberspace: A Study of the Effectiveness of Artificial Intelligence in Defensive Cyber Operations.

Project Objective

Our project's purpose is to identify the effectiveness in using artificial intelligence (AI) for cyber defense operations. By conducting surveys, case studies, and using statistical methods to analyze data, we aim to establish a correlation between AI integration and improve cybersecurity defenses. From our findings, we will publish a scholarly article explaining how effective AI will be at cyber defense operations. Our research will provide valuable insights for organizations considering AI adoption in cybersecurity frameworks.

Project Background and Significance

As AI's presence becomes more prominent in various aspects of our daily lives, it drives rapid changes in various sectors and industries. From detecting diseases years before symptoms emerge to automating repetitive daily tasks, AI is a tool that can be used in a variety of scenarios within our digital age. Specifically, among all these fields, AI's advancements in cybersecurity defense have increased tremendously. According to Akhtar and Tajbiul's (2024) research, AI-driven systems can process vast amounts of data at speeds far beyond human capability, identifying subtle patterns indicative of potential threats and enabling early detection and prevention.

As advancements are constantly being made in the technology world, the realm of cyberattacks also grows. Decades ago, cyberattacks operated mostly in the world of computers and phones, as digital systems weren't integrated into other parts of people's lives. However today, with everything becoming electronic and relying on computers, the risk of sabotage increases, from electric cars to the appliances and tools we use daily. With this increased risk and technology for cyberattack growth, new technologies in the field of cybersecurity must be explored and developed to handle these threats.

In fact, cybersecurity is no longer an "IT only" problem, as attacks have crossed the digital-physical barrier already in 2010. Modern cyberattacks can have physical consequences or be used as targeted military weapons, potentially more effective than traditional warfare, as showcased by a cybersecurity attack used to sabotage the Iranian nuclear program (Chomiak-Orsa, 2019). With such dangerous implications extending over just the internet, strong cyber defense mechanisms are needed to protect from any large-scale damage being done by these attacks.

AI is a tool that can do just this. With AI being one of the forefront technologies being researched and developed, the uses for it are constantly being expanded across a variety of fields. For example, applications in cybersecurity powered by AI have become increasingly crucial in the battle against online threats. This is because AI has been found to play an important role in modern security systems due to its ability to process vast amounts of data, identify trends, and even provide real-time threat detection. (Al-Mukhtar, 2024). With AI's role showing potential and establishment in the realm of cybersecurity, it is a tool worth exploring and utilizing in a crucial and expanding field like cybersecurity.

Taking into account the scale and impact of the growing cybersecurity field along with the emergence of a technology that could revolutionise the field, AI is a tool that must be studied and developed for cyberdefense systems. With basic research and findings, small advancements in AI for cybersecurity can grow every day, bringing impactful changes one step at a time.

Research Method

The project will be broken into two phases: data collection (surveys and case studies) and data analysis. The data collection phase will be conducted over the course of four weeks. The data analysis phase will be conducted over six weeks. The results will be utilized to provide a comprehensive understanding of AI's role in cybersecurity.

Data Collection:
Surveys
A survey will be conducted using Typeform and will be distributed to cybersecurity professionals at the SecureWorld conference. We will collect insight from analysts, engineers, and manager on AI-enhanced defensive strategies, detection accuracy, and response times. The survey questions will be broken down into four parts:

1. Participant background
2. AI implementation in cybersecurity
3. AI's impact on response and mitigation
4. Future of AI in cybersecurity

Responses from the surveys will be analyzed to identify trends, challenges, and benefits of AI integration.

Case Studies
The next phase involves conducting primary case studies by engaging directly with organizations that have integrated AI-driven cybersecurity measures. The organization we will be working with is Leidos. Interviews with cybersecurity teams, hands-on analysis of AI security tools, and direct observation of AI's effectiveness in real world cyber defense scenarios will be used. This will provide an understanding of the team's experiences with AI enhanced cybertools along with the

strengths and weaknesses of AI-driven detection and response. Real world cases (incident data) where AI played a crucial role in cyber threat mitigation will be recorded. These findings will be compared to one another to determine commonalities and differences in AI implementation success.

Data Analysis

The final phase involves the analysis of the data obtained. Descriptive and inferential statistics will be used to summarize survey responses and cybersecurity incident data to determine whether AI has a statistically significant impact on cybersecurity performance. Correlation and regression analysis will be used to measure the relationship between AI usage and cybersecurity performance. A time series analysis will be conducted to analyze AI's impact over time on cybersecurity defenses. These statistical methods will provide not only quantitative validation, but also predictive insights.

Expected Outcome

The aim and topic of our research is to adequately assess and understand the current and eventual progression of AI in defensive fields. From our findings we will publish a scholarly article. The purpose of this experiment is to identify the effectiveness of AI and how it will mitigate risk of possible cyber crimes. Interviews with cyber security professionals along with direct observation and hands-on analysis of cybersecurity tools will allow us to understand our findings and produce more quality data.

Taking a deeper dive into AI in cyberdefense within this experiment will allow us as well as others who are passionate about the field of research to advance the progression of defensive AI even further and allow precious data to be kept safe. This is applicable to many things in modern day life. Cyber threats are always looming, especially when there is a profit to be made such as selling information or even holding a ransom for valuable information. Finding the risk assessment of AI will be very valuable to keeping information safe such as medical information, client information, and even government classified information. This will directly benefit all communities, including the UCF community as sensitive information is held by the school which includes personal information of each student.

Our research will show the truth of the effectiveness of AI within cyber security spaces and the data will present whether implementation of AI is effective for defense against cyber attacks. The entire point of using AI for defensive purposes is that AI has an automated response to possible threats and that AI is always learning and progressing in complexity. On the contrary, methods used in cyber attacks are also always changing and adapting to the new defensive tactics that are preventing access to withheld information. This will cause a never ending battle as AI will have to constantly develop new strategies in mitigating risks of potential information breaches. We

hope from our research and testing that valid outcomes are recorded and can be used to produce an informational delve into AI enhancement in cyber security.

Literature Review

Akhtar, Z. B., & Tajbiul Rawol, A. (2024). Enhancing Cybersecurity through AI-Powered Security Mechanisms. *IT Journal Research and Development*, 9(1), 50–67. https://doi.org/10.25299/itjrd.2024.16852

Akin, E, Aslan, Ö, Beloev, I, Iliev, T, Kosunalp, S, Ozkan-Okay, M, Merve, & Stoyanov, I, . (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. *IEEE Access*, 12, https://doi.org/10.1109/ACCESS.2024.3355547

Al-Mukhtar, W. N. M. (2024). AI in cybersecurity: Transformative approaches to safeguarding information technology systems. *Turkish Journal of Computer and Mathematics Education*, 15(3), 391–412. https://doi.org/10.61841/turcomat.v15i3.14945

Sumari, A. D. W., Setiawan, A., & Syamsiana, I. N. (2020). Cognitive artificial intelligence application to cyber defense. *IOP Conference Series: Materials Science and Engineering*, 732, 012037. https://doi.org/10.1088/1757-899x/732/1/012037

Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. *Symmetry*, 12(3), 410. https://doi.org/10.3390/sym12030410

Chomiak-Orsa, I., Rot, A., Blaicke, B. (2019). Artificial Intelligence in Cybersecurity: The Use of AI Along the Cyber Kill Chain. *Computational Collective Intelligence. ICCCI 2019. Lecture Notes in Computer Science* (11684). https://doi.org/10.1007/978-3-030-28374-2_35

Preliminary Work and Experience

Briefly summarize any preliminary work accomplished for your project and/or the course work and other experience you have had that demonstrates your capacity to complete your project successfully (150-200 words).

All members are majoring in computer science or information technology giving us higher levels of understanding of AI and cyber security. Two members have taken security courses providing them further insight into defensive and offensive methods used in the digital world, which makes them further qualified in forming survey questions and understanding the information gathered. Other members have taken statistics which are important in understanding research and data that

will be obtained through the surveys. One member is also a member of HackUCF, the on campus cyber security club, allowing them to stay updated on current events and providing access to resources and further insight on what should be included on survey questions. All members are taking ENC3241, a technical writing class which provides all members with good understanding in ethics and abilities in analyzing information and data. This will allow us to conduct proper research as well as create surveys while following ethical guidelines.

IRB/IACUC statement

IRB approval will be required as human participants will be surveyed in AI programs on effectiveness. IACUC approval is not required as this research does not involve animals.

Budget

In our study all surveys will be created using the free software Typeform. To incentivize people to participate there will be a $5 gift card given to those who completed the survey. We are going to survey 100 people making a total of $500 in gift card rewards. There are also publishing costs for our finished research, publishing costs on more lower end journals can be around $200 dollars. We will also require an estimated $200 for travel costs for our group members in order to travel to and from the SecureWorld conference, this brings our total budget to $900.