ChatGPT and Cybersecurity Education: Exploring the Challenges and Promises of AI-Enabled Learning

Amer Samamah

Tafila Technical University

smamhamr014@gmail.com

Ahmad Mobarak

Tafila Technical University

ahmad101hamed@gmail.com

Hamzah Klaybat

Tafila Technical University

dreamhuntersa2000@yahoo.com

Osama Jaradat

Tafila Technical University

osojr2017@gmail.com

Osama Shawish

Tafila Technical University

shawishosama187@gmail.com

# Introduction

I

**n** recent years, cybersecurity has become an increasingly critical concern for individuals, businesses, and governments alike. According to Microsoft, nearly 80% of nation-state attackers targeted government agencies, thinks tanks and other non-government organizations [1] With the rise of digital technologies, cyber threats have become more sophisticated, widespread, and damaging. Despite the growing importance of cybersecurity, however, many people remain unaware of the risks they face and lack the knowledge and skills needed to protect themselves and their data. This has created a pressing need for effective cybersecurity education and learning programs. At the same time, recent advancements in artificial intelligence (AI) and natural language processing (NLP) have opened up new possibilities for education and learning. One such technology is ChatGPT a large language model developed by OpenAI. ChatGPT uses deep learning algorithms to generate human-like responses to text input making it a potentially powerful tool for personalized and interactive learning. While ChatGPT offers many benefits for cybersecurity education, there are also some limitations to consider. For example, ChatGPT is still a machine learning model and may not be able to handle all cybersecurity-related scenarios or provide a comprehensive understanding of all threats. Additionally, there is always a risk of cybersecurity breaches or attacks on the ChatGPT system itself, which could compromise the security of user data. One of the challenges of cybersecurity education is the constantly evolving nature of cyber threats. Hackers are always developing new techniques and tactics, which means that cybersecurity education must be continuously updated to keep up with the latest trends. ChatGPT can help address this challenge by providing real-time updates on emerging cyber threats, and offering personalized guidance on how to mitigate these risks.

In the following sections of this research paper, we will go deeper into the challenges and promises of using ChatGPT for cybersecurity education and learning. First, we will provide a detailed overview of ChatGPT, its architecture, and how it works. Next, we will explore the current state of cybersecurity education, including the challenges associated with it, and the need for innovative approaches to address these challenges.

In our next step, In the following sections, we will present a survey paper that focuses on the effectiveness of ChatGPT in teaching cybersecurity to students of the cybersecurity major. The survey aims to explore the potential of ChatGPT in facilitating personalized and interactive learning experiences, reducing teaching workload, and increasing access to information. Specifically, the survey will evaluate the quality of ChatGPT responses, its ability to provide real-time and personalized feedback, and its potential to improve students' learning outcomes. Additionally, we will discuss the ethical implications of using ChatGPT in education, including concerns about bias and discrimination, academic integrity, and declining high-order cognitive skills. Finally, we will offer recommendations for future research in this area and highlight the potential for ChatGPT to revolutionize cybersecurity education and learning. We will then analyze the potential benefits and limitations of using ChatGPT in cybersecurity education, drawing on real-world examples to illustrate its capabilities. Finally, we will discuss the future of AI-enabled education, including the potential impact of emerging technologies on cybersecurity education and learning, and the ethical considerations associated with using AI for educational purposes. By the end of this paper, readers will have gained a comprehensive understanding of the role that ChatGPT and other AI-enabled technologies can play in improving cybersecurity education and learning, as well as insights into the future of education in the age of AI.

# Related Work

There are many studies and research papers related to cyber security education and learning. Some of these studies have explored the challenges associated with teaching cyber security, such as the lack of resources and the difficulty of keeping up with constantly evolving threats. Other studies have looked at different approaches to cyber security education, such as using hands-on training or gamification

techniques. Some of the works focuses on the threats and vulnerability analysis using several techniques. natural language processing (NLP) techniques have been increasingly applied to the field of cybersecurity to enhance various security tasks such as intrusion detection, threat intelligence, and security assessment. Meanwhile, the emergence of large language models like ChatGPT has enabled new opportunities for learning cybersecurity via natural language conversations. In the area of NLP-based cybersecurity, various studies have

been conducted to investigate the application of machine learning and deep learning algorithms for detecting anomalies, identifying malicious patterns, and predicting attacks in network traffic data [2]. Furthermore, researchers have also explored the use of NLP techniques for analyzing text data from social media, dark web forums, and other sources to identify cyber threats and vulnerabilities [3]. More specifically, in the context of using ChatGPT for learning cybersecurity, there have been several recent studies that have shown promising results. For example, the paper [4] proposed a cybersecurity education framework that utilizes ChatGPT as a conversational agent to provide personalized and interactive learning experiences for novice learners. The study demonstrated that the ChatGPT-based system was effective in improving learners' knowledge and skills in various cybersecurity topics. Similarly, [5] developed a ChatGPT-based system that can generate natural language explanations for cybersecurity concepts and scenarios. The system was trained on a large corpus of cybersecurity-related texts and can answer questions and provide explanations in a conversational manner. The authors evaluated the system on a dataset of cybersecurity questions and found that it achieved high accuracy and naturalness in generating responses.

Overall, these studies demonstrate the potential of ChatGPT in enhancing cybersecurity education and training through personalized and interactive learning experiences. However, further research is needed to explore the effectiveness of ChatGPT in different learning contexts and to address challenges such as data privacy and security in NLP-based systems.

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref.no** | **Research Name** | **Methodology** | **Result** |
| 7. | A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem. | The paper proposes a machine learning-based approach to extract information from natural language documents available on the web to identify potential patterns of security issues.  Experiments were performed on news extracted from the Hacker News website and on Common Vulnerabilities and Exposures (CVE) vulnerability reports. | The study demonstrates the effectiveness of the approach in identifying potential patterns of security issues.  The paper highlights the challenges associated with the analysis of cyber threats and vulnerabilities in healthcare systems, which have increased due to the widespread adoption of digitization, electronic health records, and other connected medical devices. |
| 9. | Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime. | Review of the most significant practices and strategies in cybersecurity to prevent cybercrime and create a safe digital environment.  Discussion of the use of modern and advanced technologies in developing computer systems and protecting customer data.  Emphasis on the use of cybersecurity specialists to create a cyberspace free of gaps and the use of artificial intelligence techniques in designing the advantages of cyberspace.  Review of the characteristics of cyberspace and the three layers that make up its structure. | The use of cybersecurity practices is essential in protecting computer systems and data from cyber-attacks and making the digital environment safe and free of threats. |
| 11. | ChatGPT and Software Testing Education: Promises & Perils | Conducted a comprehensive empirical study to task ChatGPT with answering questions from five chapters of a popular software testing textbook.  Vetted the results across multiple dimensions.  Aimed to understand how often ChatGPT is correct in answering questions, how often it can fully and accurately explain its answers, how different ways of asking questions to ChatGPT can affect its ability to provide correct responses, and whether ChatGPT's expressed confidence provides bearing on the correctness of its answers. | ChatGPT is able to respond to 77.5% of the testing questions examined.  For the questions to which ChatGPT was able to respond, it provides correct or partially correct answers in 55.6% of cases, and provides correct or partially correct explanations in 53.0% of cases.  Prompting the model in a shared context, where similar questions are asked together, led to marginally better answers.  The tool's claimed confidence level seems to have little bearing on the correctness of the answers.  The paper discusses the potential promises and perils related to the use of ChatGPT in software testing courses. |
| 12. | Impact of Big Data Analytics and ChatGPT on Cybersecurity | Analyzing the need for smarter cybersecurity solutions due to the increasing sophistication of network attacks and cyber threats.  Discussing how Big Data analytics and Artificial Intelligence (AI) tools or platforms like ChatGPT can be used to prevent cybersecurity challenges.  Discussing the existing AI and data analytic technologies and how they can enhance cybersecurity.  Analyzing the shortcomings of incoming AI application in ChatGPT, focusing on its pros and cons in managing cyber threats.  Placing a strong emphasis on emphasizing security systems to respond to more preemptive and predictive reactions and monitoring, saving time when performing manual, repetitive security tasks.  Identifying the challenges curbing such adoptions and providing future directions to overcome the challenges. | The study reviewed the existing types of cybersecurity attacks and how to counter them through AI and Big Data analytics.  The study introduced AI methods and data analytics in computer security, detection, and intrusion systems developed to alter and detect possible attacks and deviating behavior.  The study found that Big Data analytics can produce the process of implementing cybersecurity operations and the essential training for the security analyst.  The study highlighted that the central aim of this research is to review the existing types of cybersecurity attacks and how to counter them through AI and Big Data analytics, thus giving the future direction of cybersecurity.  The study found that by introducing AI methods and data analytics in computer security, detection, and intrusion systems developed to alter and detect possible attacks and deviating behavior.  The study identified that the knowledge prioritization and upcoming threats are significant since the actors quickly alter and adapt their techniques and tactics. |

# Methodology

* Problem statement
* Research Question(s)
* Hypotheses
* Research Model
* Evaluation Measures

# References

1. John Lambert. (2021, Oct.). Microsoft Digital Defense Report shares new insights on nation-state attacks. Microsoft. Available: [Microsoft Digital Defense Report shares new insights on nation-state attacks - Microsoft Security Blog](https://www.microsoft.com/en-us/security/blog/2021/10/25/microsoft-digital-defense-report-shares-new-insights-on-nation-state-attacks/) Last accessed in : 20/April/2023.
2. [Dukka Reddy](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Reddy/Dukka+KarunKumar), [Himansu Behera](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Behera/Himansu+Sekhar), [Janmenjoy Nayak](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Nayak/Janmenjoy), [Pandi Vijayakumar](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Vijayakumar/Pandi), [Bighnaraj Naik](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Naik/Bighnaraj), [Pradeep Singh](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Singh/Pradeep+Kumar). (2020, Oct.). Deep neural network-based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. Wiley Online Library. Available:

<https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4121> Last accessed in 20/April/2023.

1. Murat Ertan Dogan, Tulay Goru Dogan, and Aras Bozkurt. (2022, Oct.) A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem. Available: <https://www.mdpi.com/1424-8220/23/2/651> Last accessed in 20/April/2023.
2. Mohammadreza Farrokhnia, Seyyed Kazem Banihashem, Omid Noroozi & Arjen Wals. (2023, Mar.)A SWOT analysis of ChatGPT Implications for educational practice and research Available: <https://www.tandfonline.com/doi/full/10.1080/14703297.2023.2195846> Last accessed in : 20/April/2023.
3. Fadel M. Megahed, Ying-Ju Chen, Joshua A. Ferris, Sven Knoth and L. Allison Jones-Farmer. (2023, Feb.) How Generative AI models such as ChatGPT (Mis)Used In SPC Practice, Education, And Research? An Exploratory Study. Available: [https://arxiv.org/abs/2302.10916 Last accessed in 20/April/2023](https://arxiv.org/abs/2302.10916%20Last%20accessed%20in%2020/April/2023).
4. [Dukka Reddy](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Reddy/Dukka+KarunKumar), [Himansu Behera](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Behera/Himansu+Sekhar), [Janmenjoy Nayak](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Nayak/Janmenjoy), [Pandi Vijayakumar](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Vijayakumar/Pandi), [Bighnaraj Naik](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Naik/Bighnaraj), [Pradeep Singh](https://onlinelibrary.wiley.com/authored-by/ContribAuthorRaw/Singh/Pradeep+Kumar). (2020, Oct.). Deep neural network-based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. Wiley Online Library. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4121> Last accessed in 20/April/2023.
5. Murat Ertan Dogan, Tulay Goru Dogan, and Aras Bozkurt. (2022, Oct.) A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem. Available: <https://www.mdpi.com/1424-8220/23/2/651> Last accessed in 20/April/2023.

[8] Maad M. Mijwil,Mohammad Aljanabi,Ahmed Hussein Ali,19

Mijwil..,Exploring the Role of Cybersecurity in the Protection of

Medical:Mesopotamian Journal of Cybersecurity Vol.2023, 18–21.

<https://mesopotamian.press/journals/index.php/CyberSecurity>.

[9] Author: Maad M. Mijwil,Mohammad Aljanabi,ChatGPT3..,Towards

Artificial Intelligence-Based Cybersecurity:The Practices and ChatGPT

Generated Ways to Combat Cybercrime,Available online January 2023

<https://doi.org/10.52866/ijcsm.2023.01.01.0019>

[10] Dr. Biswas Som Subhro Biswas, Role of ChatGPT in Cybersecurity

Affiliation:The University of Tennessee Health Science Center,

Memphis,Tennessee,

USA,https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=4403584.

[11] Sajed Jalil,Suzzana Rafi,Thomas D. LaToza,Kevin Moran,Wing

Lam,ChatGPT and Software Testing Education:

Promises & Perils,11 Mar 2023,

<https://arxiv.org/abs/2302.03287>

Pawankumar Sharma, Bibhu Dash, Impact of Big Data Analytics and

ChatGPT on Cybersecurity: Conference Paper · March 2023 .

https://www.researchgate.net/publication/369358499