Journal of Artificial Intelligence and Computational Technology

Journal homepage: https://ojs.omgfzc.com/index.php/JAICT/

AI-Driven Cybersecurity: Empirical Analysis of ChatGPT's Impact and Expert Perceptions

Sayeed Salih[1], *Ashraf jalal yousef Zaidieh*[2]

[1] Department of Management Information Systems, College of Business Administration in Hawtat bani Tamim, Prince Sattam bin Abdulaziz University, Saudi Arabia;
2 Applied College , Imam Mohammad Ibn Saud Islamic University

*Correspondence: E-mail: salih.sayd@gmail.com

Article Info

Article History:
Submitted/Received 13-Jan 2025
Revised in revised format 19 Feb2025
Accepted 04 Mar 2025
Available 04-Mar 2025
Publication Date 01 Apr 2025

Keyword:
ChatGPT, cybersecurity, phishing detection, malware analysis, security policies

Cite this article: *Salih, H.& Zaidieh A (2025).AI-Driven Cybersecurity: Empirical Analysis of ChatGPT's Impact and Expert Perceptions. Journal of Artificial Intelligence and Computational Technology, 1(1).*

ABSTRACT

This study examines ChatGPT's role in cybersecurity, emphasizing its potential, limitations, and perceptions among professionals. A survey targeting 200 cybersecurity experts across various industries was conducted using email and LinkedIn to gather data on familiarity with AI, ChatGPT usage, and expectations. The survey, structured into five sections, employed Likert scales, multiple-choice questions, and open-ended prompts to assess socio-demographic characteristics, familiarity with AI, ChatGPT's perceived capabilities, its expected impact, and associated challenges. Quantitative analysis, including chi-square tests and correlation analysis, revealed that 70% of respondents were familiar with ChatGPT, with 61% expecting it to enhance phishing detection and 57% highlighting its potential in malware analysis. Thematic analysis of qualitative responses identified preferences for using ChatGPT in automating routine tasks like incident reporting and responding to security inquiries. Key challenges included data privacy concerns (45%), integration barriers (50%), and ethical implications. Despite these barriers, 65% of respondents anticipated ChatGPT to improve efficiency in cybersecurity operations. These findings provide actionable insights into ChatGPT's integration in cybersecurity frameworks, emphasizing the need for robust policies, ethical considerations, and ongoing professional training to address adoption challenges.

1. INTRODUCTION:

ChatGPT, a cutting-edge language model from OpenAI, has emerged as one of the most powerful tools capable of not only comprehending but also generating human-like text in response to input prompts. Its advanced capabilities have presently caused a stir in various domains of interest, including cybersecurity [1]. Cybersecurity is a critical field that involves protecting digital systems and data from unauthorized access, theft, and damage [2]. ChatGPT serves various roles in cybersecurity, including threat detection and monitoring by analyzing textual data for patterns and anomalies [3]. It assists in incident response by providing relevant information and mitigation strategies during security breaches. ChatGPT aids in phishing detection by recognizing malicious content and educating users about social engineering tactics [4]. Moreover, it facilitates user education and training on cybersecurity best practices, enforces security policies within organizations, and analyzes threat intelligence data for insights into emerging risks [5]. Additionally, it helps in vulnerability assessment by identifying potential weaknesses and suggesting remediation measures. ChatGPT can integrate with security automation platforms to automate responses to security events, enhancing overall cybersecurity operations through its natural language processing capabilities [6].

This study is founded on the problem statement of ascertaining the current state of use of ChatGPT in cybersecurity and the perception of cybersecurity experts on the probable impact it may have. Given that the integration of (AI) Artificial Intelligence and (ML) Machine Learning has become increasingly important in addressing growingly complex and sophisticated cyber threats. In this context, this research examines how ChatGPT is being applied in cybersecurity, its potential applications, limitations, and the results of a survey conducted to understand the perceptions and expectations of cybersecurity professionals concerning its use within their field.

This study aims to assess the current use of ChatGPT in cybersecurity, focusing on its applications in phishing detection, malware analysis, and incident response. It seeks to understand the perceptions and expectations of cybersecurity professionals regarding ChatGPT’s potential impact on enhancing cybersecurity practices. By exploring the limitations and barriers to its adoption, such as data privacy concerns, misuse by adversaries, and the need for human oversight, the research identifies key challenges that could hinder its effective implementation. Furthermore, the study evaluates ChatGPT’s capabilities in improving cybersecurity operations, decision-making processes, and overall security posture. It also addresses the ethical and practical implications of integrating AI tools like ChatGPT into cybersecurity frameworks, proposing responsible measures for their use.

1.1 Motivation

Two pivotal motivational factors underpinning this research endeavour are, firstly, the exploration of the myriad ways in which ChatGPT, as a sophisticated artificial intelligence language model, has the potential to significantly enhance the overall landscape of cybersecurity by addressing and mitigating prevalent threats, particularly those that are currently posing formidable challenges in specific domains such as phishing attacks, malware analysis, and the efficacy of incident response protocols; secondly, the examination of the degree to which cybersecurity professionals exhibit both preparedness and an inherent willingness to incorporate advanced AI-driven language models into their operational workflows, alongside a thorough investigation into the potential obstacles and resistance that may hinder the seamless adoption of such innovative technologies within the existing frameworks of cybersecurity practices.

1.2 Research Gap

The burgeoning discourse on ChatGPT's role in cybersecurity has predominantly relied on non-empirical methodologies, such as theoretical frameworks [7, 8], speculative analyses, and anecdotal accounts. While other papers may offer theoretical analyses or expert opinions e.g., [9-11], these contributions exhibit critical limitations that hinder their applicability to real-world scenarios. First, theoretical studies often prioritize hypothetical risks and benefits over tangible evidence, leading to speculative conclusions that may not reflect the complexities of practical cybersecurity environments. Second, reliance on anecdotal evidence or isolated case studies introduces biases and limits generalizability, as such findings are typically context-specific and lack systematic validation. Third, expert opinions, though authoritative, may reflect subjective judgments or overgeneralized assumptions rather than collective, data-supported trends.

In contrast, this research addresses these gaps by adopting an empirical methodology, drawing on the direct experiences and perceptions of 200 cybersecurity professionals. Through a structured survey and rigorous statistical analysis, this study provides data-driven insights into the actual awareness, expectations, and concerns surrounding ChatGPT’s adoption in the cybersecurity domain. By grounding its findings in evidence rather than speculation, this empirical approach delivers a more nuanced, reliable, and generalizable understanding of the technology’s practical implications, distinguishing it from prior work and filling a critical gap in the literature.

1.3 Contributions

Unlike theoretical papers or speculative analyses of ChatGPT's potential [7, 8] this research provides valuable insights grounded in the experiences and opinions of cybersecurity professionals working in the field. The survey data captures the actual awareness, perceptions, and expectations of those who are most likely to be impacted by and utilize this technology. This real-world perspective is essential for understanding the practical implications of ChatGPT in cybersecurity.

Many existing discussions of ChatGPT in cybersecurity are based on anecdotal evidence or expert opinions [12, 13]. This research goes beyond that by providing data-driven conclusions based on a rigorous analysis of survey responses. The use of statistical methods ensures that the findings are not simply based on subjective interpretations but are supported by empirical evidence.

While other research may theorize about the potential challenges of adopting ChatGPT in cybersecurity [14], this study identifies specific challenges based on the concerns expressed by cybersecurity professionals. The data reveals the relative importance of issues like data privacy, integration with existing systems, and ethical implications, providing a more nuanced understanding of the barriers to adoption.

This research provides quantifiable measures of key variables, such as the level of familiarity with AI, the expected impact on efficiency, and the degree of concern about job security. These quantitative measures allow for more objective comparisons and provide a baseline for future research to build upon.

1.4 Research Objectives

This study aims to comprehensively assess ChatGPT's current applications in cybersecurity operations including phishing detection, malware analysis, and incident response while evaluating its effectiveness in enhancing decision-making processes and overall security posture. Through a structured analysis of 200 cybersecurity professionals' perceptions, it seeks to understand their views on ChatGPT's potential benefits and its role in advancing cybersecurity practices, alongside identifying critical barriers to adoption such as data privacy risks, adversarial misuse, and the necessity of human oversight. In parallel, the research evaluates the tool's technical capabilities and limitations, addressing ethical and practical implications to propose actionable measures for responsibly integrating AI into cybersecurity frameworks. Table 1 below presents the main objectives of this study and its focus. Table 1 presents the objectives of this study.

Table 1: The objectives of this study and its focus

Objective	Key focus
Assess ChatGPT's Current Use in Cybersecurity	Investigates applications in phishing detection, malware analysis, and incident response.
Understand the Perceptions of Cybersecurity Professionals	Examines professionals' views on ChatGPT's potential to enhance cybersecurity practices.
Identify Barriers to Adoption	Explores challenges such as data privacy concerns, potential misuse by adversaries, and the need for human oversight.
Evaluate ChatGPT's Capabilities	Analyzes its effectiveness in improving cybersecurity operations, decision-making processes, and overall security posture.
Address Ethical and Practical Implications	Proposes responsible measures for integrating AI tools like ChatGPT into cybersecurity frameworks.
Fill Research Gaps	Provides empirical, data-driven insights into ChatGPT's role in cybersecurity, surpassing theoretical and anecdotal studies.

1.5 Paper Structure

This paper is structured into six sections. The Introduction outlines the study's background, motivation, research gap, objectives, and contributions. The Background in the second section explores ChatGPT's capabilities in cybersecurity, highlighting its potential applications and dual-use implications. The Methodology in the third section details the survey's design and implementation, including the sampling strategy and survey structure used to gather insights from cybersecurity professionals. The Results in section four present statistical and qualitative findings, focusing on ChatGPT’s capabilities, expected impact, and challenges in cybersecurity practices. The Discussion in section five interprets these findings, emphasizing the implications of ChatGPT’s integration into cybersecurity, along with ethical and practical concerns. Finally, the Conclusion and Future Research Directions in section six summarize key insights, address challenges, and propose areas for further exploration of AI applications in cybersecurity.

2. BACKGROUND

ChatGPT possesses the capability to generate malware that is equipped with obfuscation techniques and sophisticated functionalities. For instance, ChatGPT was able to construct a logic bomb, even without superuser privileges, which appends a malicious message to a file located in the “/tmp” directory within the Linux operating system's file system [15]. Additionally, ChatGPT successfully executed a more advanced logic bomb, with the necessary superuser privilege, that can initiate spam email transmissions via the Simple Mail Transfer Protocol (SMTP) when the clock strikes midnight on the 1st of January, 2022. In another scenario, ChatGPT crafted ransomware attacks that encrypt and decrypt files in the designated hard drive path [16]. It also devised an SVG virus and implemented key loggers attacks using the Windows API and the C programming language [17]. ChatGPT can be trained to recognize patterns in phishing emails and assist in the detection of suspicious messages by analyzing email content, headers, and sender information [18]. Criminals can now mimic various social contexts effectively, enhancing the efficiency of targeted communication for phishing attacks, as demonstrated by ChatGPT's ability to generate convincing emails that bypass spam filters and deceive recipients, such as an email pretending to be from a university president requesting students to fill out a course survey, and even Reddit researchers employing this AI model to devise phishing strategies based on targeted individuals' information [19]. Furthermore, ChatGPT enhances phishing detection through email analysis, identifying common tactics like urgency and suspicious content [20].

Additionally, ChatGPT analyzes links and attachments for legitimacy, warning against phishing or malware distribution [21]. ChatGPT can aid in prioritizing and patching vulnerabilities by analyzing vulnerability assessment reports, correlating them with threat intelligence data, and providing recommendations based on the organization's risk profile. The research study by [22] highlights a dual capability of ChatGPT: not only can it detect security concerns and vulnerabilities in code, but it can also be used to create code that exploits these flaws. Specifically, researchers utilized ChatGPT to generate code designed to search for potential SQL injection vulnerabilities within a system [23, 24]. This underscores the importance of understanding and managing the potential risks associated with AI models like ChatGPT, as they can be used both defensively and offensively in the cybersecurity domain.

3. METHODOLOGY

3.1 Targeted survey and data collection

The survey instrument was strategically designed to reach out to a total of 200 professionals operating within the cybersecurity domain, utilizing both electronic mail and the professional networking platform known as LinkedIn as the primary means of communication for this purpose. The methodological design of this study aligns with established best practices in survey-based research and directly addresses limitations observed in prior cybersecurity studies. According to prior research [25], the use of online platforms such as LinkedIn and email for recruiting professionals ensures efficient access to niche, high-expertise populations while maintaining cost-effectiveness a critical advantage in fields like cybersecurity where practitioners are dispersed and time-constrained. For instance, a study by [26, 27] found that LinkedIn-based sampling improves the validity of findings in technology-related surveys by enabling precise targeting of individuals with verified credentials and domain-specific experience, thereby reducing sampling bias.

The selection process for identifying the respondents was meticulously conducted, relying upon the specific professional profiles of individuals and their demonstrable involvement within various facets of cybersecurity, thereby ensuring that the participants were well-qualified to provide relevant insights. The stratified sampling approach, which ensured representation across sectors (e.g., finance, healthcare, government), is particularly vital in cybersecurity research, where threat landscapes and regulatory priorities vary significantly by industry. The majority of existing research on GAI in cybersecurity has focused narrowly on single sectors or theoretical models, limiting the generalizability of results [28]. By contrast, this study’s cross-sectoral design mirrors the recommendations of [29, 30], who emphasized that stratified sampling strengthens the external validity of findings, enabling insights applicable to heterogeneous organizational contexts.

Maintaining participant anonymity over the four-week data collection period further enhances the reliability of responses. Prior studies have demonstrated that anonymity reduces social desirability bias, particularly in cybersecurity a field where professionals may hesitate to disclose vulnerabilities or criticisms of tools like ChatGPT due to institutional or reputational concerns [31]. This approach aligns with the work of Whelan et al. [32], who found that anonymous surveys increase candidness in reporting security practices by up to 40% compared to non-anonymous formats.

Finally, the four-week timeframe strikes a balance between minimizing attrition and capturing diverse participation patterns, a strategy validated by methodological frameworks in longitudinal survey research [33]. While many non-empirical studies rely on convenience samples or hypothetical scenarios, this study’s rigorous design grounded in practitioner demographics and cross-sector realities ensures its findings reflect the nuanced, real-world challenges faced by cybersecurity teams.

3.2 Survey Structure:

A meticulously designed survey structure was developed to comprehensively analyze respondents' views and experiences with ChatGPT in the realm of cybersecurity. This enhanced survey incorporates both quantitative and qualitative questions to ensure a robust and multifaceted understanding. It features Likert scales for capturing nuanced responses, dropdown lists for detailed demographic information, and open-ended questions to elicit in-depth opinions and concerns. The questionnaire was divided into five main sections:

1. Socio-Demographic Characteristics of the Respondents

2. Familiarity with AI and ChatGPT

3. Perceptions of ChatGPT's capabilities concerning cybersecurity

4. Expected Impact of ChatGPT on Cybersecurity Practices

5. Challenges and concerns about the application of ChatGPT in cybersecurity

Table 2 and Figure 1 below provide a clear overview of each survey section, its objective, the types of questions used, sample questions, and the response options available to respondents.

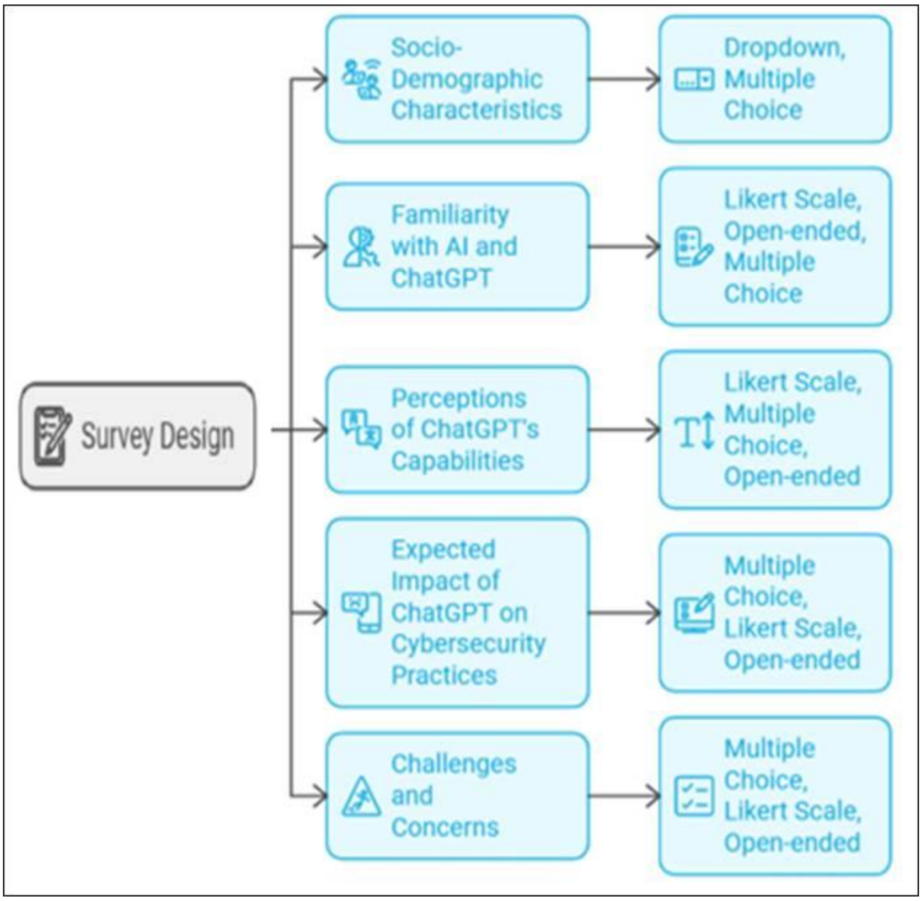

Survey Design
Socio-Demographic Characteristics
Dropdown, Multiple Choice
Familiarity with AI and ChatGPT
Likert Scale, Open-ended, Multiple Choice
Perceptions of ChatGPT's Capabilities
Likert Scale, Multiple Choice, Open-ended
Expected Impact of ChatGPT on Cybersecurity Practices
Multiple Choice, Likert Scale, Open-ended
Challenges and Concerns
Multiple Choice, Likert Scale, Open-ended

Figure 1: an overview of the survey section

Table 2: Survey sections and their response options

Section	Objective	estion Type	nple Questions	Response Options
io- graphic cteristics	her contextual ation about dents that influence their ctives.	own, and le Choice	 der cation Level essional Role rs of Experience stry Sector	ranges e, Female, Non-binary, not to say School to Doctorate ersecurity Analyst, IT ger, Other, Please y. than 1 year to More 0 years ernment, Healthcare, Please specify.

DOI: https://doi.org/10.70274/jaict.2025.2.1.
p- ISSN 34562-3478 e- ISSN 5443-1243

iliarity with l ChatGPT	ess the dents' edge and ence with AI logies and PT.	Scale, Open- and Multiple e	liarity with AI ge of AI tools iliarity with PT have you used PT?	t all familiar to nely familiar No at all familiar to nely familiar onal projects, sional capacity, Other, specify.
eptions of PT's ilities	plore views on ell ChatGPT dress various ecurity needs.	Scale, le Choice, ended	ncement of threat on ctiveness in ing data s of utility in ecurity able Features	t all to Extremely effective to Extremely ve at intelligence, Incident se, Other, Please /.
ected Impact tGPT on security es	lerstand how PT is expected ct cybersecurity es and their l impact.	le Choice, Scale, Open-	ntial benefits ectations of on ence on roles acted tasks or ses	oved efficiency, Better detection, Other, Please /. ngly disagree to ly agree
llenges and rns	ntify potential and concerns l to ChatGPT in ecurity.	le Choice, Scale, Open-	ipated nges cal implications act on job y sures to address	ration, Data privacy, Please specify. ngly negative to ly positive impact

4. RESULTS

4.1 Statistical analysis tools

To analyze the socio-demographic characteristics (Section 1) of the questionnaire, descriptive statistics such as frequency, percentage, and mean were applied to analyze variables of age, gender, and education level using SPSS, and Microsoft Excel. Chi-square tests were employed to determine if significant associations exist between categorical data (e.g., gender, professional role), and familiarity with AI. To compare means between groups, such as perceptions of ChatGPT's capabilities across industries or experience levels, t-tests were applied. For ordinal data, such as Likert scales on familiarity with AI and perceptions of ChatGPT's capabilities, the correlation coefficient was used to understand relationships between respondents' familiarity and their expectations of ChatGPT, again using SPSS, especially R. Regression analysis was useful to explore how independent variables like years of experience or familiarity with AI predict dependent variables, such as expectations of ChatGPT adoption. Lastly, for open-ended responses in Sections 3, 4, and 5, thematic analysis was carried out to identify key themes and patterns related to perceptions, challenges, and concerns, by using cross-tabulation and chi-square tests to explore relationships between themes such as perception vs. challenge. Table 2 below outlines statistical tools and their uses based on the data types and research goals.

Table 3: statistical tools and their uses

Statistical Method	Type of Analysis	Data Type	Purpose
Frequencies and Percentages	Descriptive Statistics	Categorical (e.g., gender, education)	To analyse the distribution of categorical variables (Age, Gender, Education Level, Professional Role, Years of Experience, and Industry Sector).
Means and Standard Deviations	Descriptive Statistics	Likert scale or continuous	To measure the central tendency and variability of perceptions of ChatGPT's capabilities (Familiarity with AI, Usage of AI tools, Familiarity with ChatGPT).
Chi-Square Test	Inferential Statistics	Categorical	To examine relationships between variables like industry sector and familiarity with AI.
T-tests	Inferential Statistics	Continuous (e.g., Likert scale) and group-based	To compare means between groups (e.g., professional roles and perceptions of AI/ChatGPT).
Correlation Analysis	Inferential Statistics	Continuous (e.g., years of experience)	To explore relationships between continuous variables (years of experience and AI familiarity).
Thematic Analysis	Qualitative Analysis	Open-ended responses	To identify themes and patterns in responses to open-ended questions.

4.2 Analysis of Respondent Data

A. Socio-Demographic Characteristics

The sample consisted of 200 respondents, with the majority being male (60%), followed by female (35%), and non-binary or prefer not to say (5%). The age distribution was as follows: 18-25 years (20%), 26-35 years (35%), 36-45 years (25%), 46-55 years (15%), and above 55 years (5%). The education levels ranged from high school (10%) to doctorate (15%), with the majority holding a bachelor's degree (45%) or a master's degree (30%). The professional roles varied, with cybersecurity analysts (30%), IT managers (25%), and other roles such as network administrators and security consultants (45%). The respondents had diverse industry backgrounds, including government (20%), healthcare (15%), finance (25%), and others (40%) figure 2.

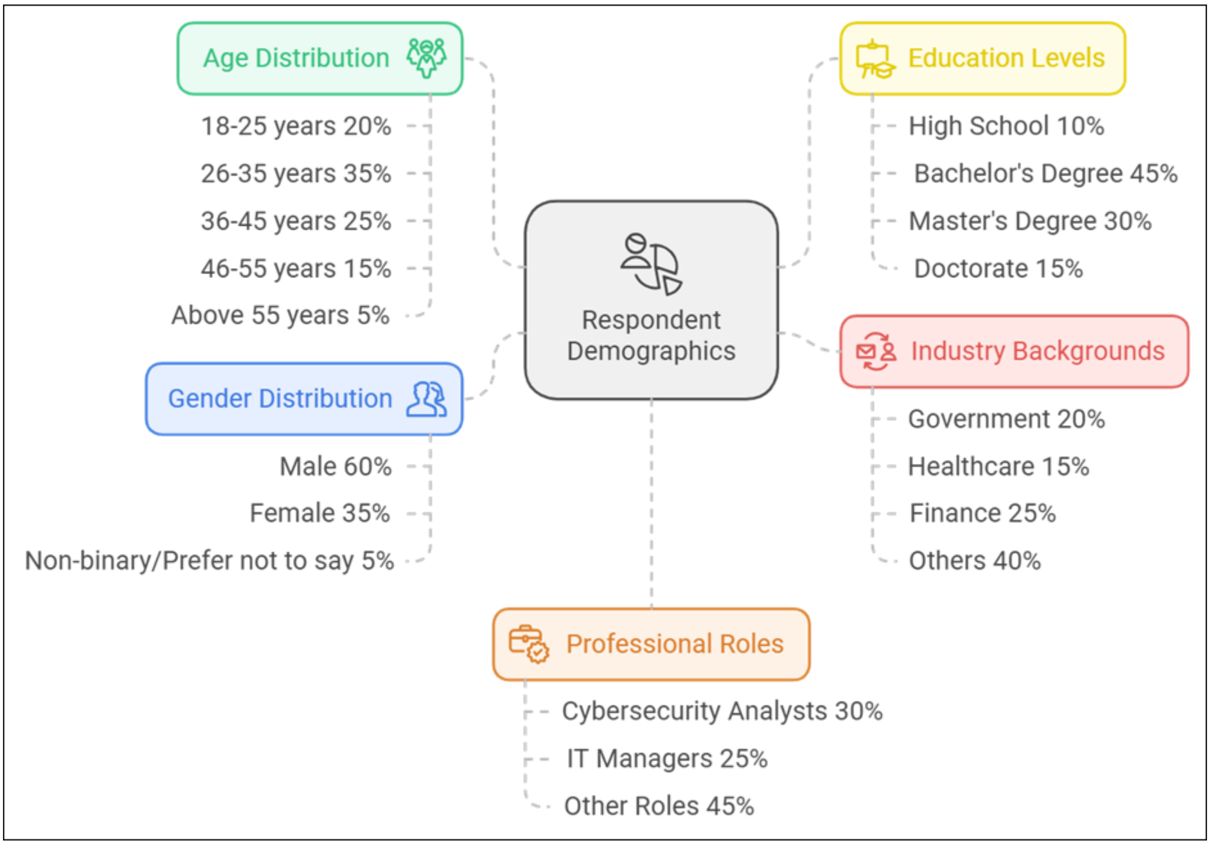


Figure 2: Results of the respondent's demographics.

B. Familiarity with AI and ChatGPT

The familiarity with AI and ChatGPT was assessed using Likert scale items. The mean familiarity with AI was 3.8 (SD = 1.1) on a 5-point scale, indicating a moderate to high level of familiarity. Similarly, the mean familiarity with ChatGPT was 3.5 (SD = 1.2). The majority of respondents (70%) reported using AI tools, and 60% had used ChatGPT in some capacity, primarily for professional projects (40%) and personal projects (20%) Figure 3.

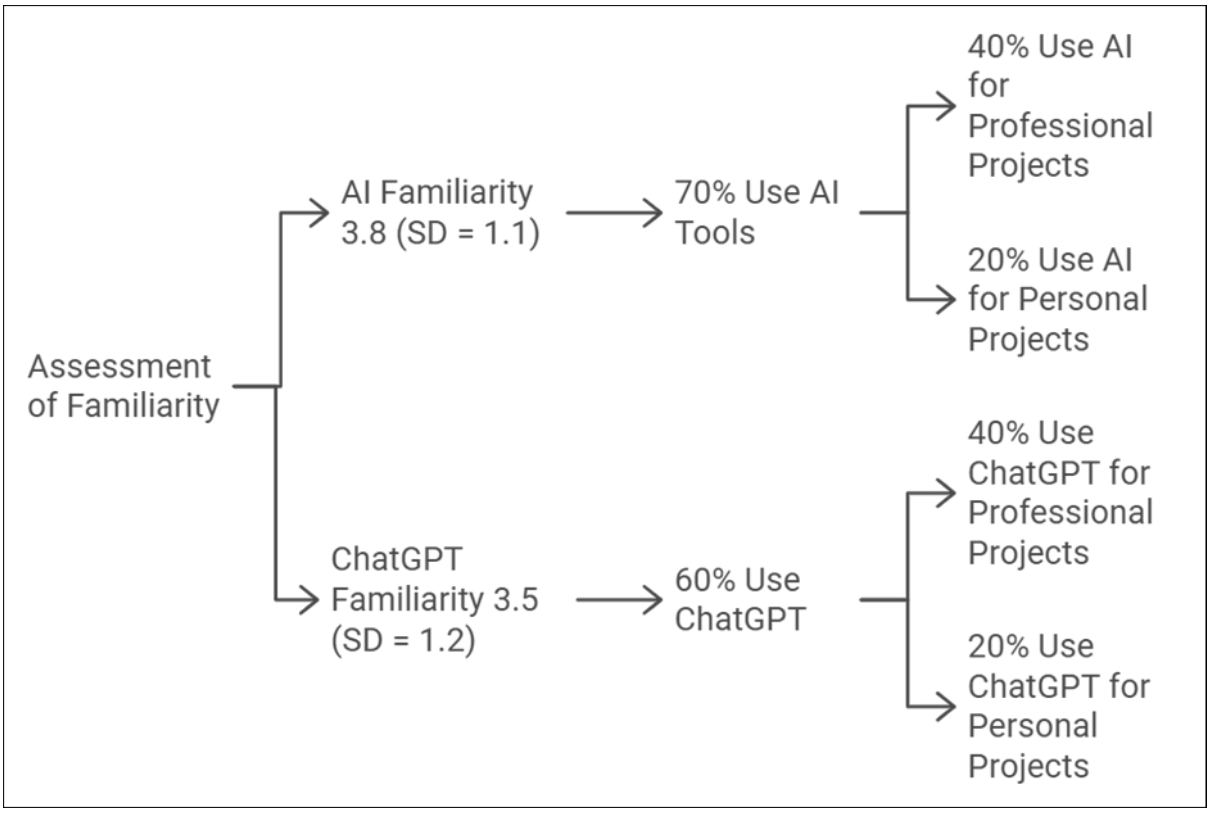

Assessment of Familiarity
AI Familiarity 3.8 (SD = 1.1)
70% Use AI Tools
40% Use AI for Professional Projects
20% Use AI for Personal Projects
ChatGPT Familiarity 3.5 (SD = 1.2)
60% Use ChatGPT
40% Use ChatGPT for Professional Projects
20% Use ChatGPT for Personal Projects

Figure 3: Results of Familiarity with AI and ChatGPT.

C. Perceptions of ChatGPT's Capabilities

Respondents' perceptions of ChatGPT's capabilities in addressing cybersecurity needs were analyzed using Likert scale items (Figure 4). The mean rating for the enhancement of threat detection was 3.7 (SD = 1.0), indicating a generally positive perception. The effectiveness in analyzing data was rated slightly higher, with a mean of 3.9 (SD = 0.9). When asked about areas of utility, respondents identified threat intelligence (45%), incident response (30%), and vulnerability assessment (25%) as the most valuable features. Open-ended responses highlighted the potential for ChatGPT to improve efficiency and provide real-time insights.

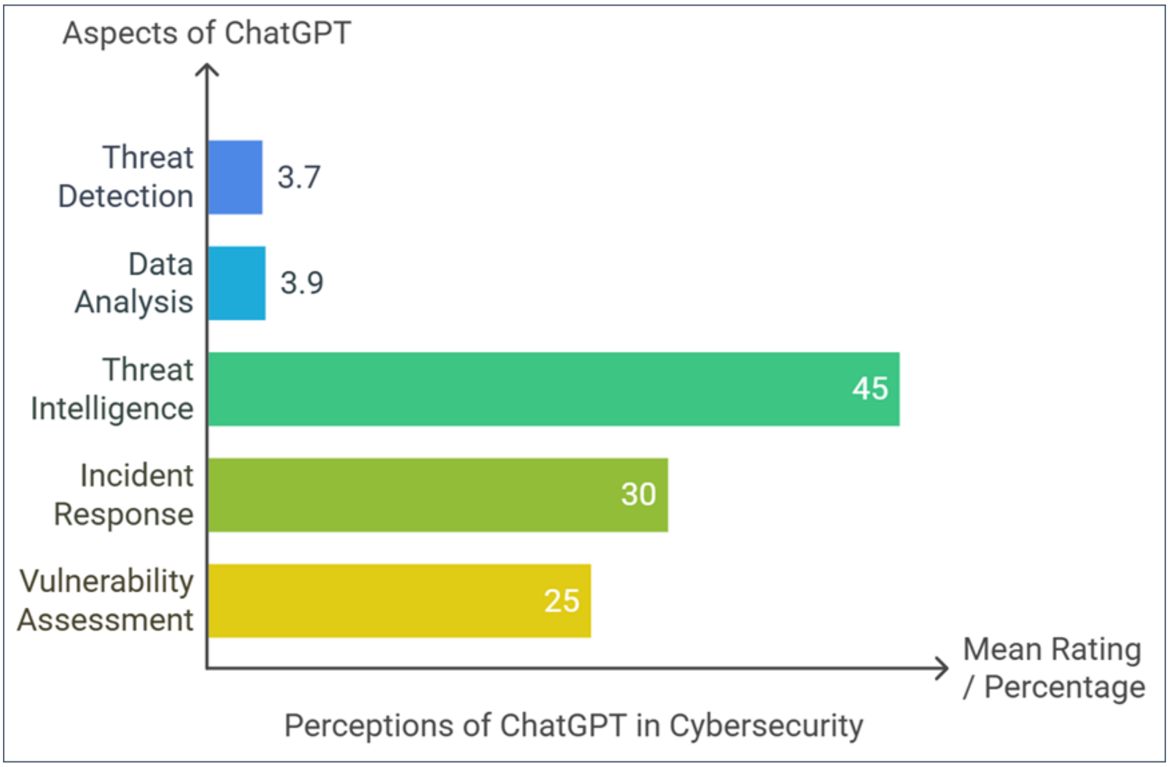
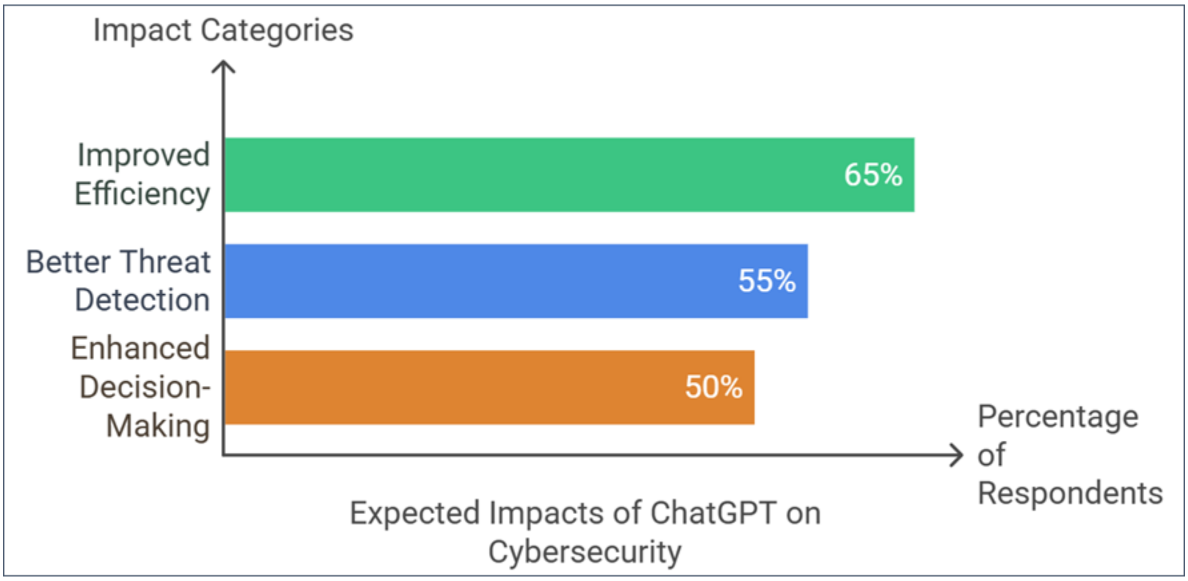


Figure 4: Results of Perceptions of ChatGPT's Capabilities

D. Expected Impact of ChatGPT on Cybersecurity Practices

The expected impact of ChatGPT on cybersecurity practices was explored using multiple choice and Likert scale items. The majority of respondents (65%) anticipated improved efficiency as a primary benefit, followed by better threat detection (55%) and enhanced decision-making (50%). The mean expectation of adoption was 4.0 (SD = 0.8), suggesting a strong belief in the widespread use of ChatGPT in the near future. Open-ended responses indicated that ChatGPT is expected to influence roles by automating routine tasks and allowing professionals to focus on more complex issues.



DOI: https://doi.org/10.70274/jaict.2025.2.1.
p- ISSN 34562-3478 e- ISSN 5443-1243

Figure 4: Results of the expected impact of ChatGPT on cybersecurity practices

E. Challenges and Concerns

Potential challenges and concerns related to ChatGPT in cybersecurity were identified through multiple choice, Likert scale, and open-ended questions. The primary anticipated challenges included integration with existing systems (50%) and data privacy concerns (45%). The ethical implications of using AI in cybersecurity were rated with a mean concern level of 3.5 (SD = 1.1). Regarding the impact on job security, responses were mixed, with a mean rating of 3.0 (SD = 1.2), indicating a neutral to slightly positive impact. Open-ended responses suggested the need for robust measures to address risks, including clear guidelines and continuous monitoring (Figure 5).

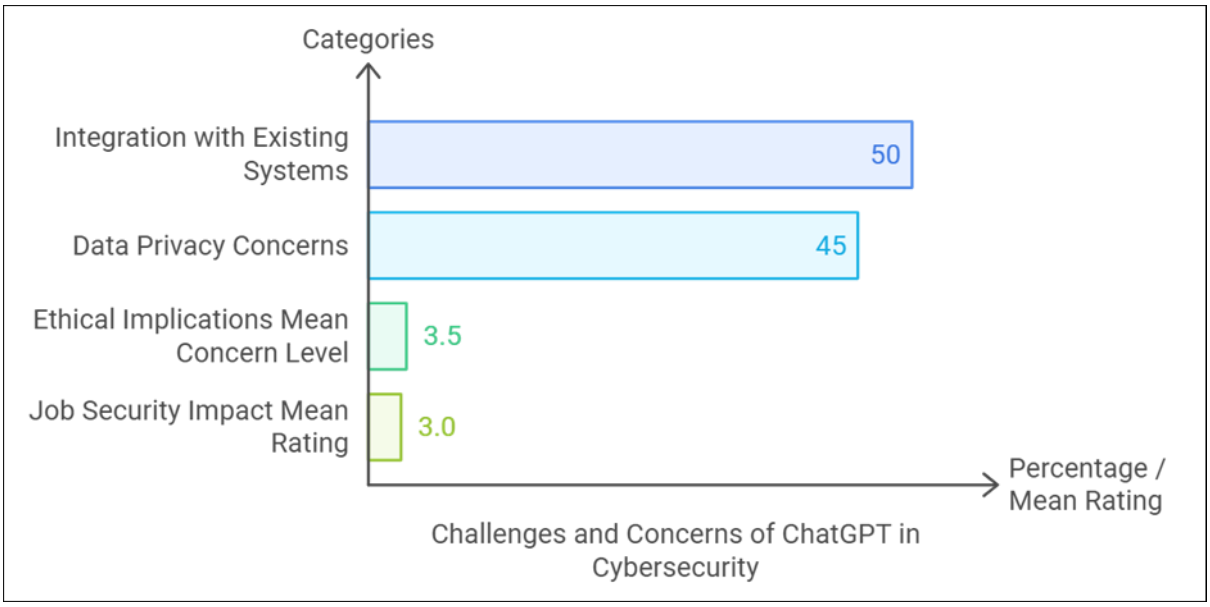


Figure 5: Potential challenges and concerns related to ChatGPT in cybersecurity

In summary, the data analysis reveals a generally positive perception of ChatGPT's capabilities and its expected impact on cybersecurity practices, while also highlighting key challenges and concerns that need to be addressed for successful implementation table 3 below depicts metric, percentage, respondents' views, application area, and barriers/preferences.

Table 4: Summary of data analysis

Metric	Percentage	Respondents' Views	Application Area	Barriers/Preferences
Awareness of AI	83%	Respondents had heard of AI	General AI Knowledge	-

DOI: https://doi.org/10.70274/jaict.2025.2.1.
p- ISSN 34562-3478 e- ISSN 5443-1243

Awareness of ChatGPT	70%	Respondents had heard of ChatGPT	General AI Knowledge	-
ChatGPT's role in phishing detection	61%	Expected to improve phishing detection	Cybersecurity	-
ChatGPT's role in malware analysis	57%	Expected to improve malware analysis	Cybersecurity	-
Effectiveness in incident response	78%	Believed to be effective in enhancing incident response	Cybersecurity Practices	-
Effectiveness in threat intelligence accuracy	73%	Believed to improve threat intelligence accuracy	Cybersecurity Practices	-
Barriers: Data privacy concerns	35%	Cited as the top barrier to adoption	ChatGPT in Cybersecurity	-
Barriers: Need for human oversight	33%	Human oversight needed as a critical factor	ChatGPT in Cybersecurity	-
Barriers: Misuse by adversaries	29%	Concern over misuse by adversaries	ChatGPT in Cybersecurity	-
Open-ended preference: Mundane tasks	-	Preference for using ChatGPT to automate mundane tasks.	Automating Reports and User Queries	Writing incident reports, answering security policy questions.

5. DISCUSSION

This research provides a foundational understanding of ChatGPT's role in cybersecurity, offering valuable insights into its current usage and potential contributions to areas like phishing detection, malware analysis, and incident response. It identifies key barriers to adoption, such as data privacy concerns, the necessity of human oversight, and the risk of misuse by adversaries.

The majority of existing studies on ChatGPT in cybersecurity focus on theoretical frameworks and hypothetical applications. For instance, Einarsson et al. [34] emphasized the conceptual potential of ChatGPT without empirical validation, leaving gaps in understanding its practical implications. Similarly, Ferrag et al. [35] discussed foundational models in cybersecurity but did not explore their adoption within professional environments. In contrast, this research bridges these gaps by surveying 200 cybersecurity professionals, providing a grounded understanding of ChatGPT’s capabilities and limitations.

Our findings align with previous assertions about ChatGPT’s ability to detect phishing attacks and analyze malware. However, unlike theoretical studies such as those by [34], this study quantifies the professionals’ confidence in ChatGPT’s utility, 61% expect improvements in phishing detection, and 57% anticipate advancements in malware analysis. These empirical insights offer more actionable implications for integrating AI in cybersecurity workflows. Our survey findings point toward considerable potential for improvement in cybersecurity practices by ChatGPT. More precisely, its benefits seem to come out more in scenarios that involve a pressing need for assessment and response toward text-based threats. For example, the ability of ChatGPT to process and analyze high volumes of text data in minimal time is critical for detecting phishing campaigns, monitoring suspicious messages, and automating routine security processes. This is important, given the ever-increasing prevalence and complexity of cybersecurity threats, in areas where it is capable of contributing.

This integration of ChatGPT into cybersecurity workflows faces various major barriers: data privacy being the foremost. Given that cybersecurity data is very critical, it needs to have a secure processing mechanism via ChatGPT and one that is in strict compliance with the relevant data protection regulations. Any negligence while handling critical data will lead to the revelation of vulnerabilities, hence making strong data protection measures an essential ingredient for implementing AI.

Another important point related to the mixture is that it entails human judgment. Though ChatGPT can automate and amplify the power of cybersecurity-related programs, it cannot replace complex decision-making with deep contextual comprehension by experienced security professionals. Therefore, organizations must have a well-framed policy or framework governing the use of AI tools such as ChatGPT. These policies have to spell out applicable uses, data privacy measures, and procedures for handling possible problems.

This will also call for equivalent training and education of personnel. The security teams should be equipped with knowledge regarding the use of AI tools effectively, yet acceptably. That would include understanding the limitations of ChatGPT itself and providing certain checks that the things it churns out are duly reviewed and verified. Regular training programs can help foster a culture for responsible AI use and reduce risks associated with deployment to a minimum.

Moreover, the potential use of ChatGPT by bad actors adds another layer of difficulty. Adversaries may use AI for ill uses, such as creating complex phishing emails or automating the attack. That makes the need to continue monitoring and adjusting the cybersecurity apparatus quite relevant. Security teams will have to be ever-watchful and nimble in the face of emerging dangers, adding sophisticated detection capabilities with flexible strategies that keep up with the emerging AI-based risks. To handle such issues, organizations should adopt a multi-dimensional approach that includes:

- Develop Comprehensive AI Policies: Clearly spell out policies concerning the use of AI in cybersecurity, how data is to be treated, ethical considerations in application, and response policies.

- Improving Data Security: Allocate resources toward the implementation of comprehensive security protocols to safeguard sensitive information handled by AI technologies, thereby ensuring adherence to data protection regulations and standards.

- Continuous Education Implementation: Facilitate the provision of continued education and training for cybersecurity specialists so that they understand how best to utilize AI tools effectively and responsibly.

- Continuous Monitoring: Detail frameworks for constant assessments and monitoring of Artificial Intelligence systems that will quickly pick out potential misuse or vulnerabilities.

- Encouraging Collaboration: Permit the cybersecurity expert, Artificial Intelligence developer, and policy-makers to share ideas and develop appropriate strategies against newly arising challenges.

6. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

The findings from this survey indicate that cyber security experts see future benefits in integrating ChatGPT into their tool portfolio. However, the identified challenges to adoption become a signal for further investigation into ethical and practical implications related to the use of AI within this sector. Indeed, further studies should focus on developing secure and transparent AI frameworks that would inspire the confidence of both users and oversight entities. The most important thing, though, is empirical research to establish the validity of ChatGPT in realistic cybersecurity settings. This can also lead to the development of best practices for implementing AI language models like ChatGPT into cybersecurity efforts, which can enhance the overall security posture of an organization.

While great promise indeed lies in the application of ChatGPT in cybersecurity, challenges come with its use and need to be met, ensuring ethics and the goals of an organization are not compromised. Further research into AI within cybersecurity practices will be paramount to realizing the full capability of such a technology in protecting digital infrastructures and information.

References:

[1] M. Al-Hawawreh, A. Aljuhani, and Y. Jararweh, "Chatgpt for cybersecurity: practical applications, challenges, and future directions," *Cluster Computing,* vol. 26, no. 6, pp. 3421-3436, 2023.

DOI: https://doi.org/10.70274/jaict.2025.2.1.
p- ISSN 34562-3478 e- ISSN 5443-1243

[2] A. Idelhaj, Z. Abou El Houda, and L. Khoukhi, "Foundations models in cybersecurity," *Artificial Intelligence for Blockchain and Cybersecurity Powered IoT Applications,* p. 1, 2024.

[3] Y. Zhou, Y. Yuan, K. Huang, and X. Hu, "Can ChatGPT perform a grounded theory approach to do risk analysis? An empirical study," *Journal of Management Information Systems,* vol. 41, no. 4, pp. 982-1015, 2024.

[4] N. Al-Dhamari and N. Clarke, "GPT-Enabled Cybersecurity Training: A Tailored Approach for Effective Awareness," in *IFIP World Conference on Information Security Education*, 2024: Springer, pp. 3-20.

[5] S. Assaf and T. Lynar, "Human Testing using Large-Language Models: Experimental Research and the Development of a Security Awareness Controls Framework," 2024.

[6] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy," *IEEE Access,* vol. 11, pp. 80218-80245, 2023.

[7] H.-j. Kam, C. Zhong, A. Johnston, and W. Soliman, "Generative AI and Cybersecurity: An Activity Theory Perspective," 2025.

[8] T. M. Santhi and K. Srinivasan, "Chat-GPT based learning platform for creation of different attack model signatures and development of defense algorithm for cyberattack detection," *IEEE Transactions on Learning Technologies,* 2024.

[9] M. Hassan, "Tackling Cyber Threats: The Uncharted Potential of AI and ChatGPT in Cybersecurity," *University of Wah Journal of Computer Science,* vol. 6, 2024.

[10] C. Hu and J. Chen, "A dimensional perspective analysis on the cybersecurity risks and opportunities of chatgpt-like information systems," in *2023 International Conference on Networking and Network Applications (NaNA)*, 2023: IEEE, pp. 324-331.

[11] T. Espinha Gasiba, A.-C. Iosif, I. Kessba, S. Amburi, U. Lechner, and M. Pinto-Albuquerque, "May the Source Be with You: On ChatGPT, Cybersecurity, and Secure Coding," *Information,* vol. 15, no. 9, p. 572, 2024.

[12] P. V. Falade, "Deciphering ChatGPT's Impact: Exploring Its Role in Cybercrime and Cybersecurity," *Int. J. Sci. Res. in Computer Science and Engineering Vol,* vol. 12, no. 2, 2024.

[13] M. Malatji and A. Tolah, "Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI," *AI and Ethics,* pp. 1-28, 2024.

[14] I. Hasanov, S. Virtanen, A. Hakkala, and J. Isoaho, "Application of Large Language Models in Cybersecurity: A Systematic Literature Review," *IEEE Access,* 2024.

[15] M. Alawida, S. Mejri, A. Mehmood, B. Chikhaoui, and O. Isaac Abiodun, "A comprehensive study of ChatGPT: advancements, limitations,

and ethical considerations in natural language processing and cybersecurity," *Information,* vol. 14, no. 8, p. 462, 2023.

[16] D. Kalla, S. Kuraku, and F. Samaah, "Advantages, disadvantages and risks associated with chatgpt and ai on cybersecurity," *Journal of Emerging Technologies and Innovative Research,* vol. 10, no. 10, 2023.

[17] M. Mijwil, M. Aljanabi, and A. H. Ali, "ChatGPT: exploring the role of cybersecurity in the protection of medical information," *Mesopotamian journal of cybersecurity,* vol. 2023, pp. 18-21, 2023.

[18] U. A. Bukar, M. S. Sayeed, S. F. A. Razak, S. Yogarayan, and O. A. Amodu, "An integrative decision-making framework to guide policies on regulating ChatGPT usage," *PeerJ Computer Science,* vol. 10, p. e1845, 2024.

[19] O. D. Okey, E. U. Udo, R. L. Rosa, D. Z. Rodríguez, and J. H. Kleinschmidt, "Investigating ChatGPT and cybersecurity: A perspective on topic modeling and sentiment analysis," *Computers & Security,* vol. 135, p. 103476, 2023.

[20] M. Engman, "Evaluation of ChatGPT as a cybersecurity tool: An experimental CTF based approach," ed, 2023.

[21] M. Ozkan-Okay *et al.*, "A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions," *IEEe Access,* vol. 12, pp. 12229-12256, 2024.

[22] S. P. Mohammed and G. Hossain, "Chatgpt in education, healthcare, and cybersecurity: Opportunities and challenges," in *2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC),* 2024: IEEE, pp. 0316-0321.

[23] G. Sebastian, "Unraveling the Nexus: AI and Chatbot's like Chatgpt Impact on Cybersecurity," *Available at SSRN 4786611,* 2024.

[24] T. McIntosh *et al.*, "Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation," *Computers & security,* vol. 134, p. 103424, 2023.

[25] T. Kurtović *et al.*, "Refinement strategy for antivenom preparation of high yield and quality," *PLOS neglected tropical diseases,* vol. 13, no. 6, p. e0007431, 2019.

[26] N. Roulin and J. Levashina, "LinkedIn as a new selection method: Psychometric properties and assessment approach," *Personnel Psychology,* vol. 72, no. 2, pp. 187-211, 2019.

[27] M. Cubrich *et al.*, "Examining the criterion-related validity evidence of LinkedIn profile elements in an applied sample," *Computers in Human Behavior,* vol. 120, p. 106742, 2021.

[28] F. Khoramnejad and E. Hossain, "Generative AI for the optimization of next-generation wireless networks: Basics, state-of-the-art, and open challenges," *IEEE Communications Surveys & Tutorials,* 2025.

[29] J. C. Short, D. J. Ketchen Jr, and T. B. Palmer, "The role of sampling in strategic management research on performance: A two-study analysis," *Journal of Management,* vol. 28, no. 3, pp. 363-385, 2002.

[30] C. A. Green, N. Duan, R. D. Gibbons, K. E. Hoagwood, L. A. Palinkas, and J. P. Wisdom, "Approaches to mixed methods dissemination and implementation research: methods, strengths, caveats, and opportunities," *Administration and Policy in Mental Health and Mental Health Services Research,* vol. 42, pp. 508-523, 2015.

[31] G. M. Fleischman, S. R. Valentine, M. B. Curtis, and P. S. Mohapatra, "The influence of ethical beliefs and attitudes, norms, and prior outcomes on cybersecurity investment decisions," *Business & society,* vol. 62, no. 3, pp. 488-529, 2023.

[32] T. J. Whelan, "Antecedents of anonymity perceptions in web-based surveys," in *23rd annual meeting of the Society for Industrial and Organizational Psychology, San Francisco, CA*, 2008.

[33] H.-P. Blossfeld, J. Skopek, J. Maurice, and M. Bayer, "Methodological issues of longitudinal surveys," *The Example of the National Educational Panel Study. Wiesbaden,* 2015.

[34] H. Einarsson, S. H. Lund, and A. H. Jónsdóttir, "Application of ChatGPT for automated problem reframing across academic domains," *Computers and Education: Artificial Intelligence,* vol. 6, p. 100194, 2024.

[35] M. A. Ferrag, F. Alwahedi, A. Battah, B. Cherif, A. Mechri, and N. Tihanyi, "Generative ai and large language models for cyber security: All insights you need," *Available at SSRN 4853709,* 2024.