Risks and Ethical Concerns in Cyber Security with Advancements of Artificial Intelligence – A Systematic Review

Ayden Perez
Department of Multidisciplinary Engineering
Texas A&M University
College Station, USA
aydencperez1@gmail.com

Saira Anwar, IEEE Member
Department of Multidisciplinary Engineering
Texas A&M University
College Station, USA
sairaanwar@tamu.edu

Abstract—Contribution: This study offers an analysis of cybersecurity for continuing advancements in artificial intelligence (AI). Specifically, we synthesized the literature and highlighted the possible cybersecurity risks and ethical concerns associated with advancements in AI. Background: Recent advancements in AI have implicated various risks and ethical concerns regarding cybersecurity. Prior literature studies have highlighted a plethora of these issues. We have conducted a systematic review to analyze the issues presented in the prior literature. Analyzing the issues presented has allowed us to answer one research question. Research Question: Our study answered one research question: Given the continuous advancements in artificial intelligence, what are cybersecurity's potential risks and ethical concerns? Methodology: We utilized the IEEE Xplore database to answer the research question. After setting the search criteria to journal articles posted between 2019 and 2024, we found 67 articles relevant to our keywords. After screening, we finalized 16 articles to address our research question. The articles selected were analyzed using qualitative thematic analysis. Articles were then categorized into three different themes: (1) social engineering, (2) misinformation and fake news, and (3) hacking. Findings: Our findings indicate that researchers have informed us about the malicious use of AI in cybersecurity by classifying attacks into three themes. These themes indicate the manner of attack. Furthermore, we find that the major risks and ethical concerns regarding the application of AI in cybersecurity relate to the preservation of privacy. As the field of artificial intelligence continues to grow, we see that it is imperative to continue monitoring the safety of this technology. For researchers to serve the public, future work should aim to translate technical terminology into more digestible phrases for those not knowledgeable in the field.

Keywords—cybersecurity risk, ethical concerns, artificial intelligence, privacy, cyber attacks

I. Introduction

Artificial intelligence (AI) is a broad field of study encompassing computing areas such as automated reasoning, game theory, knowledge representation, logic, machine learning, mathematics, and natural language processing [1]. Continued advancements in these computing areas have prompted discussions regarding their effects on cybersecurity [2]. These effects can be broadly classified as risks and ethical concerns. Many of the issues presented to cybersecurity result from generative AI's capabilities to mimic human intelligence. The current status of issues suggests that further advancements in AI will present greater consequences to cybersecurity [3], [4].

Research has taken notice of the threats presented by AI in cybersecurity. Literature studies have highlighted the ability of AI to assist in malicious activity such as phishing attacks, deception, forgery, and various other unethical practices [1], [3], [4]. Research on the risks and ethical concerns regarding AI's advancement will allow cybersecurity experts to understand the field's future better. Due to the abundance of literature regarding AI in cybersecurity, a systematic review is needed to consolidate these varying ideas.

Our study answers one research question: Given the continuous advancements in artificial intelligence, what are cybersecurity's potential risks and ethical concerns?

Answering the research question allows this study to communicate the risks and ethical concerns presented to cybersecurity due to continued advancement in AI. This focus also provides an overview of how advancements in AI affect cybersecurity.

II. Research Methods

This study utilized a systematic literature review methodology to examine the existing literature and answer the research question. For this purpose, we utilized Borrego, Foster, and Froyd's [5] four complementary methods: search, selection, coding, and synthesis. Also, we followed the synthesis mechanism utilized in our previous research [6], [7].

A. Search Method

We searched the IEEE Xplore database literature for a repeatable, systematic review process. We finalized the IEEE Xplore database due to its relevance with various engineering disciplines, specifically cybersecurity and AI. Within the database, we searched for journal articles published from 2019 to 2024. We further narrowed the scope of studies by applying the search protocol depicted in Table I. The search was conducted in November 2023.

B. Selection Strategy

The 67 studies identified were analyzed based on our inclusion and exclusion criteria. The inclusion and exclusion criteria can be seen in Table II. Fifty-one (51) articles were excluded from our study based on our four exclusion principles. These four principles are: written in the English language with full-text availability; focus differs from AI or cybersecurity; nature of the articles; relevance to research. We excluded 1, 16, 21, and 13 articles for each exclusion criterion. Additional explanations of these exclusion principles can be seen in Table II. Based on the inclusion criteria, 16 studies were found relevant for our literature review. Figure 1 showcases our study's inclusion and exclusion flowchart based on the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) checklist for our research purposes [8].

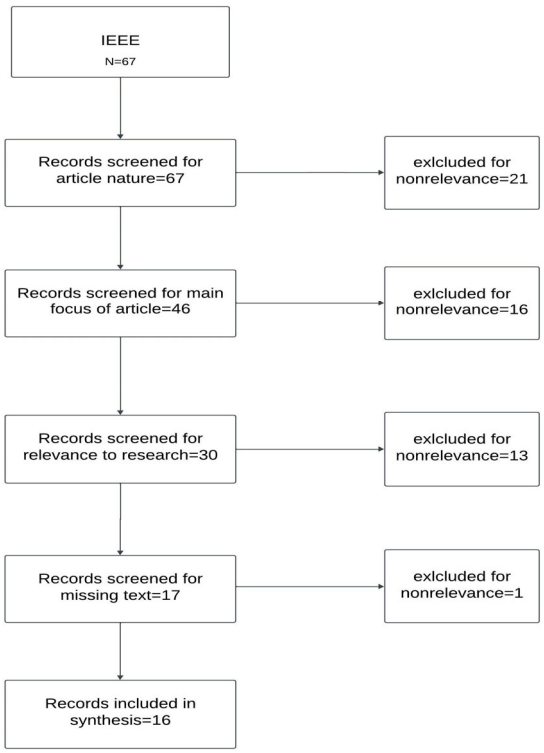

Fig. 1. Study Inclusion and Exclusion Flowchart Using PRISMA Flow [8]

TABLE I. THE SEARCH PROTOCOL FOR THE REVIEW

Database	Search Protocol
IEEE Xplore	Search String: ("Ethical Concerns" OR "Ethical Issues" OR Ethics) AND ("Artificial intelligence" OR AI) AND (cybersecurity) AND (Applications OR Software) AND (cryptography OR encryption OR "cyber security") Used advanced search Searched in Full Text Only

C. Coding and Synthesis

The articles meeting the inclusion criteria for our review were classified based on prevalent themes. These themes were identified using an article synthesis matrix. The matrix comprises the title, purpose, methodology, research design, research question, method, and results. Utilizing the article synthesis matrix allowed us to identify commonalities and differences in the included articles. This synthesis enabled us to devise a coding scheme for the articles that helped us answer our research question. Our method of coding and synthesis led to the identification of three themes in the articles: (1) social engineering, (2) misinformation and fake news, and (3) hacking.

Classifying the articles into three themes allowed us to answer our research question. It showcased the categories used in current literature when informing on cybersecurity threats presented by AI.

TABLE II. CRITERIA FOR EXCLUSION OF THE STUDIES

Exclusion Principle	Description
Written in English with no missing text	Articles must be complete and written in the English language.
Focus differs from AI or cybersecurity	Articles in this category do not focus on cybersecurity or AI. Many mention these topics but are not a core part of the article.
Nature of the Article	Articles in this category focused on ethics related to different areas utilizing AI or cybersecurity. Many of these refer to the use of AI in the medical field or cybersecurity failures that are irrelevant to the research.
Relevance	Articles in this category displayed no relevance to the research taking place. Possibly speaking on industry or other areas that benefit from AI but not in the context of this article.

III. FINDINGS

The risks and ethical concerns presented in the 16 selected articles were categorized into three themes: (1) social engineering, (2) misinformation and fake news, and (3) hacking. Classifying the articles into these themes has allowed us to answer our first research question. Further analysis of the themes allowed us to answer our second research question.

Classifying the risks and ethical concerns presented in the 16 selected articles has showcased how research informs on malicious AI-based applications in cybersecurity. We find that research points to three settings where malicious AI-based applications in cybersecurity are being used. These settings are for individual targeted attacks, mass-targeted attacks, and attacks that can cause physical harm.

Further analysis of the themes has allowed us to answer our second research question. Analyzing the risks and ethical concerns presented in the 16 selected articles allowed us to infer how further advancements in AI will affect cybersecurity.

A. Theme 1: Social Engineering

As described by Blauth and colleagues [3], social engineering uses deceptive techniques to manipulate human subjects into sharing sensitive or personal information. The authors suggest that such techniques (broadly classified as social engineering) can be classified into two categories: (1) phishing and (2) manipulation. Phishing refers to social engineering that elicits information from a target. Manipulation refers to using social engineering to influence a target's opinion.

In their paper, Blauth and colleagues [3] discuss how AI applications can threaten cybersecurity. The authors presented evidence that these techniques have been used since 2007. Specifically, the study discusses how AI can launch phishing attacks. For example, they discussed using a chatbot known as 'CyberLover.' With this chatbot, attackers could coerce their targets into disclosing sensitive information. Continued advancements in AI have enhanced the power of AI-assisted phishing. Furthermore, generative AI can create real-time deepfake media. This advancement has allowed users to impersonate well-known individuals, such as celebrities and politicians, on a live camera feed. These tools allow attackers to present themselves as trustworthy individuals when conversing with their targets [3].

Researchers have also noted the use of artificial intelligence for manipulation. For example, Jeong [4] states that attackers can release a large number of bots to manipulate public opinion. This kind of manipulation can be especially harmful for political elections. The author stated that these bots have been used to infiltrate political campaigns on online social networks. Furthermore, when large language models (LLMs) are combined with deepfakes, AI bots can be used for targeted attacks. For example, the voice of a family member may be used to gain a target's trust. The author suggests that if the target believes the voice is real, they may be more easily persuaded to fulfill the attacker's requests.

B. Theme 2: Misinformation and Fake News

The spread of misinformation and fake news is another notable risk and ethical concern presented in the selected studies. Spreading misinformation and fake news can affect a large volume of online users. For example, spreading fake news could alter the public opinion of political figures.

The spread of misinformation and fake news is especially detrimental to cybersecurity due to its reach. Malicious actors can utilize platforms like social media to launch misinformation and fake news campaigns. The volume of users on these platforms makes it difficult to slow the spread of fake news even after the source has been eliminated. For example, a user may read a fake news article before its detection and begin regurgitating the misinformation presented, spreading it to other users.

An excellent example of how misinformation can be used to cause economic damage is presented by Shahriar and colleagues [9]. The authors stated that misinformation can be used to cause damage to institutions and individuals alike. The spread of misinformation about institutions can greatly affect stock prices, leading to possible financial losses for investors. Misinformation can also be used to defame individuals or groups, making it difficult for them to succeed in the workforce.

Research specifically notes the capability of attackers to influence public opinion by publishing misinformation and fake news. For example, Shahriar and colleagues [9] stated that this malicious abuse of AI could especially damage politics. Attackers can leverage generative AI to produce misinformation and fake news. For this purpose, attackers can combine large language models and image-generating applications. Attackers can abuse this capability to influence the public opinion of candidates ahead of elections.

C. Theme 3: Hacking

The risks and ethical concerns presented in the third theme address the capability of AI models to assist in hacking. As defined by Gupta and colleagues [2], hacking is the exploitation of system vulnerabilities to gain unauthorized access or control of said systems. Gupta and colleagues highlighted how AI can assist hacking by showcasing several conversations with ChatGPT. These conversations involve users utilizing tactics such as reverse psychology to bypass safety features. After bypassing the safety measures put in place, the user made ChatGPT provide malicious code capable of gaining unauthorized control of a system.

The ability of AI to produce malicious code presents a major cybersecurity threat. Dunmore and colleagues [10] state that malicious code can be especially dangerous when considering the widespread use of computers in the military. For example, if malicious code is used to gain unauthorized access to a military system, this could result in the loss of a military-grade weapon. Unauthorized access to military-grade weapons systems presents a major threat to cybersecurity because it could lead to the loss of human lives.

Shahriar and colleagues [9] further emphasize the capability of hacking to cause real-world damage by discussing the use of autonomous vehicles. Autonomous vehicles integrate sensory technologies to make accurate, real-time decisions. If malicious code is injected into this system, it could result in the loss of life. For example, malicious code could be injected into one of these autonomous vehicles to disrupt the sensory technology. Disrupting the sensory technology of an autonomous system could result in a high-speed collision.

Hacking presents numerous threats to cybersecurity due to the real-world implications of gaining unauthorized access or control of certain systems. The threat of hacking is further emphasized when considering how this can be combined with other malicious tactics. For example, Gupta and colleagues [2] showcased examples of ChatGPT producing ransomware and malware. An attacker could attach this malicious code to a phishing email. If a user clicks this link, the attacker could access the system and bypass the need to obtain the user's trust.

IV. DISCUSSION

The articles included in the synthesis can be seen in Table III below.

TABLE III. TABLE III. STUDIES INCLUDED IN THE SYNTHESIS

S.No.	Studies included in the Synthesis
1	Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI. IEEE Access, 10, 77110-77122. https://doi.org/10.1109/ACCESS.2022.3191790
2	A. Dunmore, J. Jang-Jaccard, F. Sabrina, and J. Kwak, "A Comprehensive Survey of Generative Adversarial Networks (GANs) in Cybersecurity Intrusion Detection," IEEE Access, vol. 11, pp. 76071-76094, 2023. doi: 10.1109/ACCESS.2023.3296707.

3	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. 8021880245, 2023. doi: 10.1109/ACCESS.2023.3300381.
4	V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. HwaKim, "A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE," IEEE Access, vol. 11, pp. 37131-37148, 2023. doi: 10.1109/ACCESS.2023.3266979.
5	L. Hu, "Tech Ethics: Speaking Ethics to Power, or Power Speaking Ethics?," Journal of Social Computing, vol. 2, no. 3, pp. 238-248, 2021. doi: 10.23919/JSC.2021.0033.
6	D. Jeong, "Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues," IEEE Access, vol. 8, pp. 184560-184574, 2020. doi: 10.1109/ACCESS.2020.3029280.
7	K. B. Letaief, Y. Shi, J. Lu, and J. Lu, "Edge Artificial Intelligence for 6G: Vision, Enabling Technologies, and Applications," IEEE Journal on Selected Areas in Communications, vol. 40, no. 1, pp. 5-36, 2022. doi: 10.1109/JSAC.2021.3126076.
8	D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and The PRISMA Group, "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement," PLoS Medicine, vol. 6, no. 7, p. e1000097, 2009. doi: 10.1371/journal.pmed.1000097.
9	N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, "Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions," IEEE Communications Surveys & Tutorials, vol. 25, no. 3, pp. 1775-1807, 2023. doi: 10.1109/COMST.2023.3280465.
10	V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.D. Lin, "Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges," IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2384-2428, 2021. doi: 10.1109/COMST.2021.3108618.
11	A. Pawlicka, M. Pawlicki, R. Kozik, and M. Choras, "What' Will the Future of Cybersecurity Bring Us, and Will It Be Ethical? The Hunt for the Black Swans of Cybersecurity Ethics," IEEE Access, vol. 11, pp. 58796-58780, 2023. doi: 10.1109/ACCESS.2023.3287391.
12	S. Shahriar, S. Allana, S. M. Hazrati, and R. Dara, "A Survey of Privacy Risks and Mitigation Strategies in the Artificial Intelligence Life Cycle," IEEE Access, vol. 11, pp. 6182961854, 2023. doi: 10.1109/ACCESS.2023.3287195.
13	W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim, "Social Engineering Attacks Prevention: A Systematic Literature Review," IEEE Access, vol. 10, pp. 39325-39343, 2022. doi: 10.1109/ACCESS.2022.3162954.
14	L. N. Tidjon and F. Khomh, "The Different Faces of AI Ethics Across the World: A Principle-to-Practice Gap Analysis," IEEE Transactions on Artificial Intelligence, vol. 4, no. 4, pp. 820-839, 2023. doi: 10.1109/TAL.2022.3225132.
15	S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," IEEE Access, vol. 8, pp. 23817-23837, 2020. doi: 10.1109/ACCESS.2020.2968045.
16	Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," IEEE Access, vol. 10, pp. 93104-93139, 2022. doi: 10.1109/ACCESS.2022.3204051.

This study aims to determine the risks and ethical concerns for cybersecurity due to the continuous advancements in AI. We approached this goal by constructing one research question: (1) Given the continuous advancements in artificial intelligence, what are cybersecurity's potential risks and ethical concerns?

Our findings indicate that research informs on the malicious use of AI to threaten cybersecurity by classifying attacks into three categories: (1) social engineering, (2) misinformation and fake news, and (3) hacking. These categories were determined utilizing thematic qualitative analysis. Based on these categories, we can determine how further advancements in AI may affect cybersecurity. Specifically, it allows us to understand the risks and ethical concerns presented to cybersecurity due to future advancements in AI. We find that continued advancements in AI will increase the capability of attackers to threaten cybersecurity. Specifically, advancements in generative AI greatly threaten cybersecurity due to their ability to assist in social engineering, the production of misinformation and fake news, and hacking.

The results of this study indicated that social engineering is one of the most prominent threats to cybersecurity, with 38% of the selected studies indicating it as a threat. These findings align with existing research on AI, indicating that generative AI can impact a significant number of individuals more rapidly [11], [12]. Additionally, these findings align with the National Institute of Standards and Technology (NIST) assessment of an imminent threat [13], [14], [15]. While studies have examined the preventive measures to mitigate social engineering, enhancements in AI models have highlighted new techniques for attackers. These new techniques have presented challenges for implementing methods to detect and prevent these attacks [16].

With 50% of the selected studies indicating it as a threat, the results of this study indicate that misinformation and fake news campaigns can be enhanced with generative AI. These results align with previous attack patterns, such as those during the 2016 Presidential Election [1]. Detecting generative AI content poses a unique challenge due to how these models are trained. Generative adversarial networks (GANs) train generative AI models by providing feedback on whether or not the generated content was detected. This mechanism presents a paradoxical situation for detecting generated content. Given that the models are trained to be undetectable, utilizing GANs to detect misinformation and fake news may be an unreliable solution.

Analysis of the selected articles revealed AI-assisted hacking as a major concern for cybersecurity, with 75% of articles indicating it as a threat. These results align with previous literature, which states that the threat of hacking has long been a concern for cybersecurity [21]. Advancements in AI have increased this threat by presenting new technology susceptible to exploitation [10]. While AI streamlines tasks like driving, it simultaneously presents the opportunity for hacking. Given the consequences of successfully exploiting these systems, the use of autonomous vehicles and weapons systems poses a significant risk to cybersecurity. This risk forces the field of cybersecurity to determine what an acceptable amount of risk is to undertake in return for such systems. Furthermore, this challenges the sellers of such systems, forcing sellers to choose to sell a highly convenient product with high risk or a minimally convenient product with low risk.

Although we utilized a transparent mechanism for selection and inclusion, this study is still limited in several ways. First, our study only utilized one database with a small sample size of 16

studies. This number of included studies and the use of one database suggests that other risks and ethical concerns may not be covered in these studies. Furthermore, only journal articles were considered for our inclusion and exclusion review process. This review process could allow publication bias to be a key factor in the content reviewed. Our study was further limited by the time frame used. Our study only included articles published between 2019 and 2024. This choice or years could cause the possibility of earlier research denoting how these risks and ethical concerns can be prevented.

However, the limitations of this study present an opportunity for future research to be conducted. Future research could explore how these risks and ethical concerns can be mitigated. Future research can also be conducted to assess AI advancements and how cybersecurity responds to the new threats presented.

V. Conclusion

The advent of OpenAI's ChatGPT has led to abundant literature on artificial intelligence. By categorizing the risks and ethical concerns into three themes, this study provides a structured framework for understanding the implications of AI for cybersecurity. This paper not only helps in organizing existing knowledge but also serves as a foundation for future research. Additionally, it helps cybersecurity experts identify areas of concern so that they can mitigate and defend against these types of attacks. The synthesizing of various sources allows our study to present a holistic understanding of the challenges presented by AI applications in cybersecurity. Additionally, using theoretical examples helps illustrate how attackers can abuse AI for personal interests. This study further advances the literature by prompting readers to think critically about the evolving nature of cybersecurity and how AI can affect it.

Throughout our study, we highlighted various methods attackers can use to exploit AI and threaten cybersecurity maliciously. Notably, large language models and deepfakes pose a major risk to the security of online users. Large language models can produce text difficult to discern from human-generated responses. These capabilities can be combined for better attacks. Combining LLMs with deepfakes allows users to create online profiles that can entice victims to interact with them. Adding AI data collection could allow attackers to target certain psychological profiles for maximum effectiveness [3].

This study informs future researchers of the current risks and ethical concerns in cybersecurity due to recent advancements in AI while offering insight into how further enhancements will affect the field of cybersecurity. With the primary threat facing cybersecurity being the advent of advanced generative AI models, we can conclude that further refinement and enhancements in these models will only escalate the threat level presented to cybersecurity by these technologies. Additionally, our study allows cybersecurity practitioners to gain insight into how cybersecurity may change in the coming years. Providing this insight may allow practitioners to solve these issues before they get out of control.

VI. Acknowledgment

This study was funded with the support of Dr. George Ligler (Department of Multidisciplinary Engineering, Texas A&M University), and startup funding was provided to Dr. Anwar by the Texas A&M Experiment Station.

VII. References

[1] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," IEEE Access, vol. 8, pp. 23817–23837, 2020, https://doi.org/10.1109/ACCESS.2020.2968045.

[2] 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, https://doi.org/10.1109/ACCESS.2023.3300381.

[3] T. F. Blauth, O. J. Gstrein, and A. Zwitter, "Artificial intelligence crime: an overview of malicious use and abuse of AI," IEEE Access, vol. 10, pp. 77110–77122, 2022, https://doi.org/10.1109/ACCESS.2022.3191790.

[4] D. Jeong, "Artificial intelligence security threat, crime, and forensics: taxonomy and open issues," IEEE Access, vol. 8, pp. 184560–184574, 2020, doi: 10.1109/ACCESS.2020.3029280.

[5] M. Borrego, M. J. Foster, and J. E. Froyd, "What is the state of the Art of systematic review in engineering education? " Journal of Engineering Education, vol. 104, no. 2, pp. 212–242, 2015.

[6] S. Anwar, N. A. Bascou, M. Menekse, and A. Kardgar, "A systematic review of studies on educational robotics," J. of Pre-College Eng Educ. Research (J-PEER), vol. 9, no. 2, p. 2, 2019. https://doi.org/10.7771/2157-9288.1223

[7] S. Anwar and M. Menekse, "A systematic review of observation protocols used in postsecondary STEM classrooms," Review of Educ., vol. 9, no. 1, pp. 81–120, 2021. https://doi.org/10.1002/rev3.3235

[8] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and The PRISMA Group, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA Statement," PLoS Med, vol. 6, no. 7, Art. no. 7, Jul. 2009, https://doi.org/10.1371/journal.pmed.1000097.

[9] S. Shahriar, S. Allana, S. M. Hazratifard, and R. Dara, "A survey of privacy risks and mitigation strategies in the artificial intelligence life cycle," IEEE Access, vol. 11, pp. 61829–61854, 2023, https://doi.org/10.1109/ACCESS.2023.3287195.

[10] A. Dunmore, J. Jang-Jaccard, F. Sabrina, and J. Kwak, "A comprehensive survey of fenerative adversarial networks (GANs) in Cybersecurity intrusion detection," IEEE Access, vol. 11, pp. 76071–76094, 2023, https://doi.org/10.1109/ACCESS.2023.3296707.

[11] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim, "Social Engineering Attacks Prevention: A Systematic Literature Review," IEEE Access, vol. 10, pp. 39325–39343, 2022, https://doi.org/10.1109/ACCESS.2022.3162594.

[12] U. Farooq and S. Anwar, "ChatGPT Performance on Standardized Testing Exam--A Proposed Strategy for Learners," arXiv preprint arXiv:2309.14519, 2023.

[13] US Department of Commerce, "National Institute of Standards and Technology (NIST)," May 2024. [Online]. Available: https://www.nist.gov/

[14] G. B. White and N. Sjelin, "The NIST cybersecurity framework," in Research Anthology on Business Aspects of Cybersecurity, IGI Global, 2022, pp. 39–55.

[15] C. Brumfield, Cybersecurity risk management: Mastering the fundamentals using the NIST cybersecurity framework. John Wiley & Sons, 2021.

[16] C. Subbalakshmi, P. K. Pareek, and R. Sayal, "A study on social engineering attacks in cybersecurity," in Innovations in Computer Science and Engineering: Proceedings of the Ninth ICICSE, 2021, Springer, 2022, pp. 59–71.