Published in the Workshop Proceedings of the IEEE TPS 2024:
Inclusive AI for Cybersecurity Workshop in Conjunction with The Sixth IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications

Design Challenges for Scam Prevention Tools to Protect Neurodiverse and Older Adult Populations

Pragathi Tummala
George Mason University
Fairfax, United States
ptummal2@gmu.edu

Hannah Choi
George Mason University
Fairfax, United States
hchoi37@gmu.edu

Anuridhi Gupta
George Mason University
Fairfax, United States
agupta29@gmu.edu

Tomas A Lapnas
George Mason University
Fairfax, United States
tlapnas@gmu.edu

Yoo Sun Chung
George Mason University
Fairfax, United States
ychung3@gmu.edu

Matthew Peterson
George Mason University
Fairfax, United States
mpeters2@gmu.edu

Geraldine Walther
George Mason University
Fairfax, United States
gwalthe@gmu.edu

Hemant Purohit
George Mason University
Fairfax, United States
hpurohit@gmu.edu

***Abstract*—Scams through various communication mediums whether online social media, emails, search ads, or offline via phone calls and short messages (SMS) have dramatically increased after the pandemic. Prior technical research has leveraged artificial intelligence (AI) algorithms for scam detection tasks, such as spam and phishing detection, to design systems for preventing users from scams. However, due to the heavy data-dependence on AI techniques, in particular machine learning, the training datasets for classification models could be non-representative in capturing different nuances and evolution of social engineering attacks that aim to target vulnerable populations like the elderly or neuro-diverse individuals. For such populations, biases in the resulting models, in turn, lead to vulnerabilities in associated cybersecurity tools. Further, a one-size-fits-all approach to create interaction mechanisms in such tools reduces their value to protect individuals with neuro-diverse profiles and older adults with varying cognitive abilities. In this paper, we synthesize the existing literature with the goal of identifying the sources of inclusive design challenges for scam filtering and prevention tools through a critical analysis of literature on both current solutions explored in cybersecurity research and the needs of individuals with diverse disability profiles. We present an Inclusive AI-driven Cybersecurity (IAC) Framework for designing effective and accessible tools to protect all populations. The findings of this research can inform effective designs of scam prevention tools across different communication media with the inclusive goal of ultimately protecting all populations.**

***Index Terms*—Fraud, Spam, Phishing, Inclusive AI, Inclusive Cybersecurity**

I. Introduction

Social engineering attacks are one of the key challenges of cybersecurity. Attackers deceive the public through a variety of scamming tactics including spam messaging on phones, click baits, and phishing URLs in online social media, emails, and advertising, etc. [1]–[4] These tactics rely upon deceptive messaging with the social context of distressed relatives such as grandchildren, false romance claims, misleading investment opportunities, etc. The impact of such attacks is devastating for our society; for instance, they accounted for nearly $10 Billion in losses last year alone according to the Consumer Sentinel Network Data Book of 2023 [5]. It is, therefore, essential to prevent such scams by effectively designing scam-prevention tools that protect vulnerable populations.

Individuals with diverse types of disabilities are especially susceptible to falling victim to scams because of the way they interact in digital environments [6], [7]. For instance, neuro-diverse individuals may face challenges when attempting to recognize certain social nuances employed by social engineering attackers. Such individuals need more specific forms of assistance. Similarly, existing work shows that nearly 70% of older adults report difficulties in adapting to new digital technologies and many face cognitive and physical limitations that hinder their ability to use digital tools effectively [8], leading to greater risks of falling prey to social engineering attacks. Given the ever-growing reliance on online services and social interaction, designing assistive, accessible, and inclusive tools for scam prevention to protect such vulnerable populations is increasingly critical.

The inclusive design needs to involve the creation of cybersecurity tools that are *accessible* to all users and *effective* in protecting all users. Recent research [9] shows that 70% of cybersecurity professionals in a survey lacked awareness of best accessibility practices, highlighting the key risk of designing non-inclusive cybersecurity tools that do not effectively protect all populations, specifically do not protect the most vulnerable ones. Further, due to the growing use of machine learning algorithms for scam detection tasks by cybersecurity professionals, such as browser plugins/extensions for phishing detection, there is a lack of understanding of how non-representative data is used for training scam detection models could lead to ineffective protection across non-standard populations. For instance, if the training data does not capture different social nuances that lead to scamming certain vulnerable user groups, the resulting model would be biased and fail to protect those groups. Therefore, there is an increasing need to understand and address bias and fairness issues underlying model behaviors [10], [11] when designing cybersecurity tools.

In this paper, we aim to analyze the needs of critically diverse populations to inform the design of an inclusive cybersecurity framework, which can guide the development of scam prevention tools to protect all populations in our society from social engineering attacks. The scope of our analysis is focused on assistive tools for scam prevention involving AI techniques such as LLM-based assistive machine learning for the task of information processing.

Our paper is organized as follows. We first summarize the challenges faced by individuals with diverse disabilities, examples of assistive technologies, and current cybersecurity research. We then present a framework for designing inclusive scam prevention solutions using modern AI techniques.

II. Related Work

This section summarizes existing literature across three relevant domains.

A. Relevant Challenges for Individuals with Disabilities

Individuals with disabilities face a variety of unique challenges that can significantly impact their ability to engage with security systems effectively. Disabilities are diverse and can be broadly categorized into physical, sensory, cognitive, communicative, and neurodiverse types. Each category presents distinct challenges for interacting with digital environments, particularly regarding compliance with established security protocols [12]. Understanding these challenges is crucial for creating inclusive cybersecurity measures that accommodate a wide range of user needs.

1) ***Types of disabilities****:*

a) Physical disabilities: They impact about 15% of the global population [13]; they include conditions such as paralysis, amputation, and muscular dystrophy. In the U.S. alone, over 2.2 million people use wheelchairs, underscoring the need for inclusiveness of technology design in various deployments such as secure door access that accommodates mobility impairments [12].

b) Sensory disabilities: Approximately 2.2 billion people worldwide experience some form of visual impairment, where 39 million were classified as blind, and 466 million suffered from auditory impairments. These conditions significantly impact access to visual and aural content online, particularly among older adults, where 18% face vision impairment and 33% experience hearing loss, in the U.S. [14]. The prevalence of these impairments underscore the need for inclusive design and accessibility measures in digital environments.

c) Cognitive disabilities: They affect about 1 in 7 people globally, which is about 14% of the population. Similarly, about 12.8% of the adults in the U.S. experience cognitive disabilities, including learning disabilities and intellectual disabilities, impacting memory, problem-solving, and attention [15].

d) Neurodiversity: It encompasses conditions such as autism spectrum disorder (ASD) and Attention Deficit Hyperactivity Disorder (ADHD), affecting 15-20% of the world population [16], and around 2% of the U.S. population. These conditions influence how individuals process information and interact with technology, highlighting the need for adaptable digital solutions.

e) Communication disabilities: They can include speech and language disorders, and affect an estimated 5% to 10% of people in the U.S. [9]. Also, around 28–49% of the people with disabilities globally have a communication impairment as a component of their disability [17].

2) ***Challenges with diverse disabilities****:* Individuals with disabilities face significant challenges when interacting with technology, many of which stem from accessibility barriers. Research indicates that approximately 98% of websites are not fully accessible to individuals with disabilities, with fewer than 10% adhering to the Web Content Accessibility Guidelines (WCAG) [12]. Among individuals with cognitive disabilities, about 60% require customizable interfaces to use technology effectively. Systems that do not offer options for text size adjustment, simplified navigation, or alternative input methods can be particularly challenging for such users [15]. Sensory barriers are also significant; approximately 15% of individuals with hearing impairments report difficulties using standard digital tools, which often rely on auditory alerts. Moreover, many digital systems lack integration with assistive technologies, with less than 20% of software applications being compatible with tools like screen readers and adaptive input devices [12]. This lack of integration limits usability and accessibility for individuals who depend on these technologies. Similarly, the technical, psychological, and cultural challenges may prevent individuals, particularly older adults, from effectively navigating digital tools. As a consequence, it is critical to point out that the design of scam prevention tools such as browser plugins for spam and phishing detection needs to be inclusive. We summarize the challenges for users with diverse types of disabilities to inform the need for inclusive AI-based cybersecurity solutions in Table I.

B. Illustrative Designs for Assistive Technologies

There has been greater emphasis on exploring assistive tools and inclusive designs within the field of Education. Researchers have focused on designing tools with better accessible learning objects [18]. In the process of developing learning objects for individuals with disabilities, researchers found that understanding the nature of mobility and cognitive limitations is necessary to accommodate the corresponding populations. When information is not always easily understood, the way it is presented has the potential to affect memorability.

Similarly, research has shown that students with a learning disability have lower reading skills than students who do not. Students' learning experiences and methods can be positively impacted by assistive technologies [19]. Researchers have investigated how supportive such assistive technologies have become in augmenting user experience [20]. The existence of such tools has created pathways for people with sensory impairments to conduct tasks at home, work, school, and more. They can better communicate, be independent, learn,

TABLE I: Challenges and needs for cybersecurity solutions for individuals with diverse types of disabilities

Types of Disabilities	Conditions/Diagnoses	Primary Challenges	Needs for Inclusive AI for Cybersecurity
Physical Disabilities	Spinal cord injuries, muscular dystrophy, cerebral palsy	Mobility limitations; need for adaptive input devices	Robust machine learning models with adaptability to diverse inputs and assurance for usability across diverse assistive devices.
Sensory Disabilities	Visual impairments (blindness, low vision), auditory impairments (deafness, hearing loss)	Barriers to visual and auditory content; difficulties in accessing digital interfaces	Machine learning-enhanced screen readers and haptic feedback systems to convey security information through touch.
Cognitive Disabilities/Learning	Memory disorders, Dyslexia	Difficulties with memory, problem-solving, and navigation	Adaptive authentication systems using reinforcement learning to personalize security solutions based on cognitive/learning abilities.
Neurodiversity	Autism spectrum disorders, ADHD	Challenges with processing information, focusing, and managing sensory overload	Unbiased machine learning models with responsive to neurodiverse user needs and offering customized security measures.
Communication Disabilities	Speech and language disorder	Difficulty in understanding security instructions or interacting with text-heavy security systems.	Natural Language Processing (NLP) models to simplify security communication; text-to-speech and speech-to-text systems for interaction.

and have better control of their environment. Examples of some of these assistive technologies are screen readers, image expansion tools on a computer screen, Braille equipment, and text recognition applications. Such assistive technologies impact all learning styles differently. It can play a large role in factors affecting learning including cognitive, emotional, voluntary, attitudinal, and more. Based on the learning style, the information processed presents its results. With the vision to develop better inclusive designs in educational tools, assistive technologies are focusing on both the information processed and the interaction mechanisms.

The above illustrations of design approaches in other application domains guide how assistive tools for scam prevention can be designed to protect vulnerable population groups from social engineering attacks.

C. Exploration in Cybersecurity for Inclusion

The field of cybersecurity has extensively explored inclusion challenges when considering user privacy, but has paid limited attention to security questions. Given the associated risks, researchers need to increase their focus on inclusion to address the diverse needs of individuals, particularly those with disabilities. Research shows that 70% of cybersecurity professionals in a recent survey study lacked awareness of accessibility best practices, underscoring the need for greater attention to this design aspect and enhanced training in this area [21].

Further, approximately 30% of users with disabilities report difficulties using cybersecurity tools due to compatibility issues with assistive technologies such as screen readers and speech-to-text software [22]. Recent research has highlighted efforts to address these challenges. For example, Joakim et al. [23] developed a cybersecurity training tool designed for users with cognitive disabilities. This tool, which incorporates AI technologies, provides context-sensitive warnings and training on security issues like phishing and password management. Its features, such as text-to-speech functionality, help minimize cognitive load and improve accessibility. However, further research is needed to assess its impact across diverse user groups.

AI-driven cybersecurity solutions have been shown to advance data protection and threat management while addressing the needs of individuals with sensory disabilities. AI-enhanced systems offer accessible interfaces for those with visual impairments through screen readers and voice recognition, and provide text-based alerts for individuals with hearing impairments. In addition, these solutions, offer alternative input methods like speech-to-text for those with motor impairments [24]. Moreover, these solutions tailor interfaces for individuals with cognitive impairments, simplifying navigation and enhancing usability. Prior research has shown the diverse use-cases of integrating advanced AI techniques into cybersecurity [25]–[27]. These methodologies include deep learning for real-time threat detection, natural language processing (NLP) for filtering malicious content, and artificial neural networks (ANNs) for identifying network attacks. Additionally, AI technologies automate response mechanisms, such as dynamic adjustment of security policies and automated incident response, enhancing overall system resilience. However, these studies also suggest that current AI methods may be limited by human biases in training data. This calls for further research into training programs and enhanced AI techniques to better address such challenges.

By prioritizing inclusive design and integrating AI technologies, the cybersecurity field can create accessible and effective security solutions, ensuring that all users, regardless of their abilities, will be able to engage with and benefit from cybersecurity measures.

III. Inclusive AI-driven Cybersecurity Framework

This section describes our framework for designing inclusive cybersecurity solutions using AI technologies while accounting for the diverse needs of the neuro-diverse and older adult populations.

The Inclusive AI-driven Cybersecurity (IAC) Framework, as shown in Fig. 1, is designed to address the diverse needs of all users, including those who are neuro-diverse and have disabilities, by integrating AI technologies into cybersecurity solutions. This design is primarily shown with a focus on mitigating phishing attacks which are one of the most popular

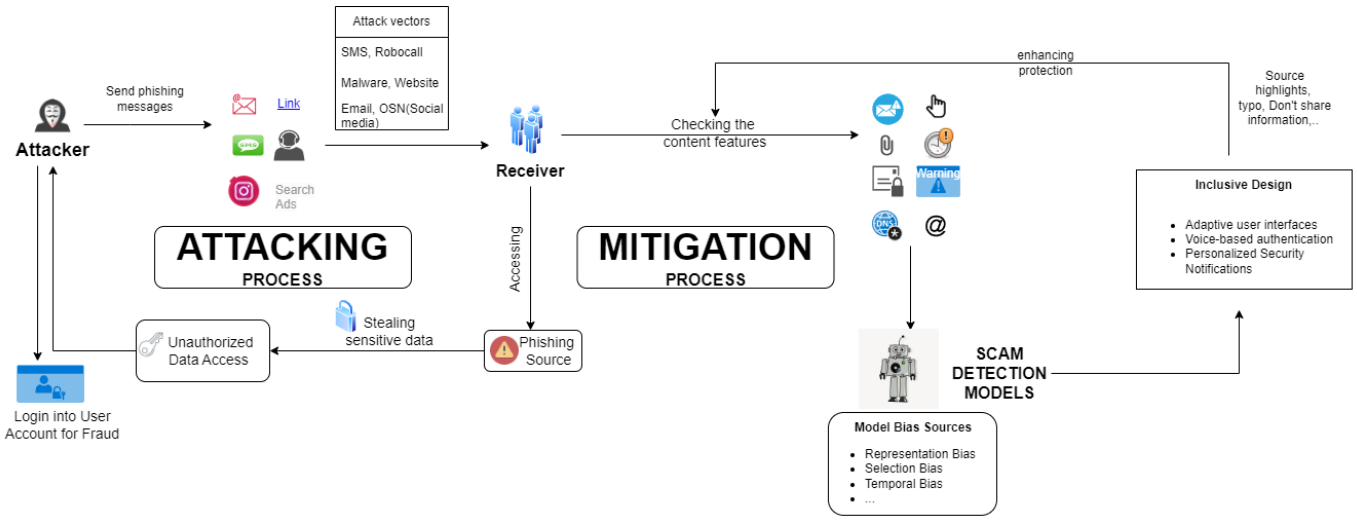

Fig. 1: Inclusive AI-driven Cybersecurity Framework for designing scam prevention tools

social engineering attacks and are common and significant threats in the digital landscape. The framework is structured around three core components: the attacking process, the mitigation process, and inclusive design, all interconnected by feedback loops aimed at improving the system's overall effectiveness and inclusivity.

In the attack phase, the framework begins with the attacker, who initiates phishing attacks through various channels, including SMS, robocalls, malware, websites, emails, and social media platforms. The receiver, typically the unsuspecting target of the attack interacts with the phishing content. If the receiver is deceived by the phishing attempt, the attacker gains unauthorized access to sensitive data, which can subsequently be used to commit fraud, such as logging into the user's accounts. This process highlights the vulnerability of users to sophisticated phishing tactics and the need for robust protective measures.

The mitigation process is where the system intervenes to prevent successful phishing attempts. It starts with analyzing the content features of the received messages and checking for signs of phishing, such as suspicious links, attachments, or other warning signals. AI-powered scam detection models play a crucial role in this process by identifying potential threats. However, these models are not without flaws; they can suffer from biases such as representation bias, selection bias, and temporal bias, which can impact their accuracy and fairness. The mitigation process also includes enhancing user protection by providing feedback that highlights potential threats, such as identifying the source of the message, pointing out typos, and advising users against sharing sensitive information.

Inclusive design is a critical aspect of the framework, aimed at ensuring that the cybersecurity solution is accessible and effective for all users, particularly more vulnerable users, such as neuro-diverse users. The design includes adaptive user interfaces that adjust to meet the specific needs of neuro-diverse users, making the system more user-friendly and accessible. Voice-based authentication is another feature that provides an alternative to traditional methods, catering to users who may find voice interactions more intuitive. Additionally, personalized security notifications ensure that the advice and warnings provided by the system are tailored to the user's cognitive preferences, enhancing understanding and compliance.

The framework is sustained by feedback loops that continuously improve the scam detection models and the overall system. These loops ensure that the system learns from each interaction, reducing biases in AI models, and enhancing the inclusivity and accessibility of the design. By integrating these elements, the framework aims to create a cybersecurity solution that not only effectively combats phishing attacks but also accommodates the diverse needs of all users, with a particular emphasis on neuro-diversity. This approach ensures that the digital environment remains safe, equitable, and accessible.

IV. Conclusion and Future Work

This paper presents an inclusive approach to cybersecurity by critically examining existing scam detection solutions and identifying their limitations regarding vulnerable populations such as older adults and neurodiverse individuals. We introduced the Inclusive AI-driven Cybersecurity (IAC) Framework, which lays a foundational approach for designing cybersecurity tools that integrate inclusivity into both AI model development and user interaction mechanisms. This framework highlights the need for adaptive, bias-aware AI techniques that accommodate the unique needs of diverse user groups and evolve with emerging threats.

Future research should focus on further refining and validating the IAC framework through practical implementation and comprehensive evaluation. This includes designing and testing personalized cybersecurity solutions that go beyond scam pre-

vention, addressing a broader range of threats faced by diverse user populations. Additionally, researchers should investigate methods to mitigate biases inherent in AI models for scam detection by developing inclusive AI techniques that leverage more representative datasets and de-biasing strategies. Case studies and real-world trials with vulnerable populations will also be essential to assess the framework's effectiveness and ensure its scalability and adaptability in different cybersecurity contexts.

ACKNOWLEDGMENT

Authors thank the U.S. National Science Foundation for grant # 2210107 and the Commonwealth Cyber Initiative for grant # HN-4Q24-057 to partially support this research.

REFERENCES

[1] S. Rao, A. K. Verma, and T. Bhatia, "A review on social spam detection: Challenges, open issues, and future directions," *Expert Systems with Applications*, vol. 186, p. 115742, 2021.

[2] İ. Yurtseven, S. Bagriyanik, and S. Ayvaz, "A review of spam detection in social media," in *2021 6th International Conference on Computer Science and Engineering (UBMK)*. IEEE, 2021, pp. 383–388.

[3] A. Das, S. Baki, A. El Aassal, R. Verma, and A. Dunbar, "Sok: a comprehensive reexamination of phishing research from the security perspective," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 671–708, 2019.

[4] O. Abayomi-Alli, S. Misra, A. Abayomi-Alli, and M. Odusami, "A review of soft techniques for sms spam classification: Methods, approaches and applications," *Engineering Applications of Artificial Intelligence*, vol. 86, pp. 197–212, 2019.

[5] U.S. Federal Trade Commission, "Consumer sentinel network data book 2023," accessed: September 1, 2024. [Online]. Available: https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf.

[6] R. Montañez, A. Atyabi, and S. Xu, "Social engineering attacks and defenses in the physical world vs. cyberspace: a contrast study," in *Cybersecurity and Cognitive Science*. Elsevier, 2022, pp. 3–41.

[7] L. Yu, G. Mottola, C. N. Kieffer, R. Mascio, O. Valdes, D. A. Bennett, and P. A. Boyle, "Vulnerability of older adults to government impersonation scams," *JAMA Network Open*, vol. 6, no. 9, pp. e2 335 319–e2 335 319, 2023.

[8] K. Zhang, "Digital disability: A new risk to older people in digital societies," *International Journal of Public Health*, vol. 69, p. 1607303, 2024.

[9] B. Naqvi, J. Kävrestad, and A. K. M. N. Islam, "Ensuring usable cybersecurity for all: Examining cognitive disabilities from research to industry," 2024, available at SSRN 4609555. [Online]. Available: https://ssrn.com/abstract=4609555

[10] S. Caton and C. Haas, "Fairness in machine learning: A survey," *ACM Computing Surveys*, vol. 56, no. 7, pp. 1–38, 2024.

[11] A. Atabek, E. Eralp, and M. E. Gursoy, "Trust, privacy and security aspects of bias and fairness in machine learning," in *2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE, 2023, pp. 111–121.

[12] K. Renaud and L. Coles-Kemp, "Accessible and inclusive cyber security: A nuanced and complex challenge," *SN Computer Science*, vol. 3, no. 5, p. 346, 2022.

[13] World Health Organization, "Disability and health," World Health Organization: WHO, 2023, accessed on 2024-09-03. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/disability-and-health

[14] C. Correia, K. J. Lopez, K. E. Wroblewski, M. Huisingh-Scheetz, D. W. Kern, R. C. Chen, L. P. Schumm, W. Dale, M. K. McClintock, and J. M. Pinto, "Global sensory impairment among older adults in the united states," *Journal of the American Geriatrics Society*, vol. 64, no. 2, pp. 306–313, February 2016.

[15] US Department of Health and Human Services, "Quick statistics about voice, speech, language," National Institute of Deafness and Other Communication Disorders, 2016, retrieved April 12, 2022. [Online]. Available: https://www.nidcd.nih.gov/health/statistics/quick-statistics-voice-speech-language

[16] U.S. NIH Division of Cancer Epidemiology and Genetics (DCEG) Staff, "Neurodiversity," April 2022, accessed: 2024-09-23. [Online]. Available: https://dceg.cancer.gov/about/diversity-inclusion/inclusivity-minute/2022/neurodiversity

[17] C. Jagoe, C. McDonald, M. Rivas, and N. Groce, "Direct participation of people with communication disabilities in research on poverty and disabilities in low and middle income countries: A critical review," *PLoS One*, vol. 16, no. 10, p. e0258575, 2021. [Online]. Available: https://doi.org/10.1371/journal.pone.0258575

[18] E. McCarty and C. Morress, "Establishing access to technology: an evaluation and intervention model to increase the participation of children with cerebral palsy." *Physical Medicine and Rehabilitation Clinics of North America*, vol. 20, no. 3, pp. 523–534, 2009.

[19] J. M. Willman and M. T. Marino, "Universal design for learning and assistive technology: Leadership considerations for promoting inclusive education in today's secondary schools," *NASSP Bulletin*, vol. 94, no. 1, pp. 5–16, 2010.

[20] M. Sterian and M. Mocanu, "The role of assistive technologies in the learning process for people with sensory impairments," *Euromentor Journal*, vol. 6, no. 3, pp. 70–80, 2015.

[21] B. Naqvi, J. Kävrestad, and A. N. Islam, "Inclusive and accessible cybersecurity: Challenges and future directions," *IEEE Computer*, vol. 57, no. 6, pp. 73–81, 2024.

[22] F. A. Inan *et al.*, "Internet use and cybersecurity concerns of individuals with visual impairments," *Journal of Educational Technology & Society*, vol. 19, no. 1, pp. 28–40, 2016.

[23] J. Kävrestad, J. Rambusch, and M. Nohlberg, "Design principles for cognitively accessible cybersecurity training," *Computers & Security*, vol. 137, p. 103630, 2024.

[24] C. Gupta and A. Khang, "Designing artificial intelligence-enabled training approaches and models for physical disabilities individuals," in *AI-Oriented Competency Framework for Talent Management in the Digital Economy*. CRC Press, 2023, pp. 388–415.

[25] N. Şen and T. Akbay, "Artificial intelligence and innovative applications in special education," *Instructional Technology and Lifelong Learning*, vol. 4, no. 2, 2023.

[26] S. DİLEK, H. ÇAKIR, and M. Aydın, "Applications of artificial intelligence techniques to combating cyber crimes: A review," *International Journal of Artificial Intelligence Applications (IJAIA)*, vol. 6, no. 1, 2015.

[27] C. Arisoy, A. Mandal, and N. Saxena, "Human brains can't detect fake news: A neuro-cognitive study of textual disinformation susceptibility," in *2022 19th Annual International Conference on Privacy, Security Trust (PST)*. IEEE, 2022, pp. 1–10.