Responsible AI Integration in Cyber Education: A Model for K-9 to K-12 Instruction

Md Al Samiul Amin Rishat [1,*], Gahangir Hossain [2], M A Shariful Amin [3], and Pretom Roy Ovi [2]

[1] Department of Information Science Concentration in Data Science, University of North Texas, Denton, Texas, USA
[2] Department of Data Science, University of North Texas, Denton, Texas, USA
[3] Department of Marketing and Computer Information Systems, Tarleton State University, Texas, USA
Email: MdAlSamiulAminRishat@my.unt.edu (M.A.S.A.R.); Gahangir.Hossain@unt.edu (G.H.); MAMIN@tarleton.edu (M.A.S.A.); Pretomroy.Ovi@unt.edu (P.R.O.)
*Corresponding author

Manuscript received December 26, 2025; revised February 12, 2026; accepted April 14, 2026; published August 12, 2026

***Abstract*—The rapid expansion of technology-driven education has increased teenagers' exposure to cyber threats, emphasizing the need for timely and developmentally appropriate cyber awareness programs across K-9 to K-12 settings. Although adolescents demonstrate confidence in using digital devices, many lack the critical skills required to recognize and evaluate online risks, leaving them vulnerable to disinformation, cyberbullying, and harmful digital behaviors. This study proposes a structured model for integrating ChatGPT into cyber awareness education using a conceptual mixed-methods approach informed by Strengths, Weakness, Opportunities, Threats (SWOT) and Fishbone analyses. The model leverages ChatGPT's interactive capabilities to support just-in-time learning while addressing concerns related to ethical use, misinformation, and regulatory compliance. Insights from K-9 to K-12 students' considerations and expert consultation informed the development of the proposed governance framework for responsible Artificial Intelligence (AI) adoption and dynamic content verification. The study suggests that ChatGPT-enhanced interventions have the potential to support increased student engagement, enhance inclusivity, and contribute to strengthening K-9 to K-12 students' resilience to online threats, provided that they are integrated responsibly with appropriate supervision. When used responsibly under appropriate supervision, ChatGPT may serve as an effective complement to traditional cyber-safety curricula by promoting critical thinking about online interactions and encouraging proactive digital defense behaviors. However, the study is limited to theoretical models and stakeholder perceptions, without direct implementation in real classroom environments. Future research should prioritize longitudinal investigations in authentic, technology-enhanced instructional settings to evaluate long-term learning outcomes, ethical considerations, and policy implications of AI-supported cyber awareness programs.**

***Keywords*—adolescent cyber awareness education; ChatGPT integration; conversational Artificial Intelligence (AI) in K-12; ethical AI governance; Strengths, Weakness, Opportunities, Threats (SWOT) and fishbone analysis**

I. Introduction

Artificial Intelligence (AI) is rapidly becoming a disruptive technology in many subjects such as medical, finance and education. According to the parlance, AI is interpreted as the ability of a machine to simulate human intelligence by learning, reasoning and making decisions [1, 2], which allows achieving high volumes of data processing along with adaptation to changing environments within these systems. Advances in natural language processing have further expanded AI capabilities by enabling chatbots and virtual assistants that can understand and generate human-like text [3]. AI tools have supported personalized learning, adaptive assessments and virtual tutoring in education [4]. ARCS based evaluation of an AI tutor (PTA), shows that its Attention, Relevance, Confidence and Satisfaction factors prodigiously enhance student's problem-solving skills [5]. One of the recent achievements of AI is Natural Language Processing (NLP) based models such as chatbots and virtual assistants that can comprehend and generate human-like text [6]. Recent work also shows strong interest in educational chatbots, with Rokaya *et al.* [7] using a merged Technology Acceptance Model-Emotional Intelligence (TAM-EI) framework to model students' adoption of chatbot applications. Building on these advances, a prominent NLP-driven AI is the release of Chat Generative Pre-Trained Transformer (ChatGPT) by OpenAI. Released in November 2022, ChatGPT's global popularity grew rapidly with more than 1M users after the first week. Using deep learning and transformer architectures, ChatGPT is a context-aware, coherent, and interactive human-like response model learned from massive textual datasets [8, 9]. On the one hand, its user-friendly interface combined with its capability to produce coherent utterances has led to its wide use as a tool for education, content production and technical support.

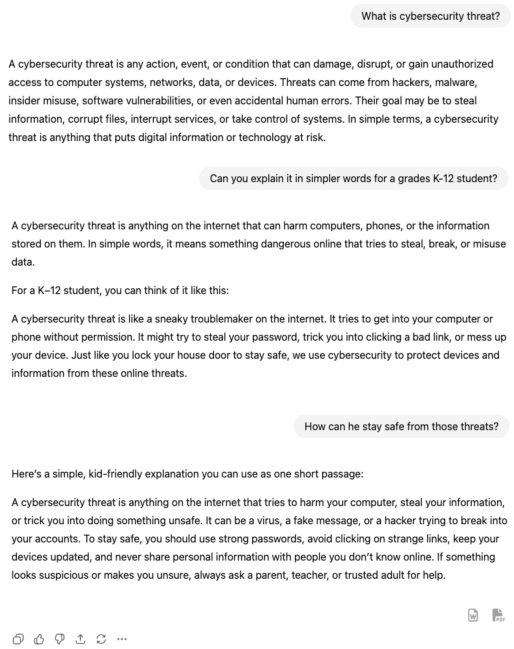

Fig. 1. Demonstration of ChatGPT's capability to retain context over conversation turns, enabling follow-up questions to be answered with continuity and coherence.

Aside from its ability to generate human-like text, ChatGPT also offers several advanced features that distinguish it from basic chatbots. For example, ChatGPT can retain the context of a conversation within the same interaction [10]. This ability allows it to respond to follow-up questions without the need for users to repeat previous information, enhancing continuity in interactions [11], as shown in Fig. 1.

An additional feature is ChatGPT's multimodal functionality, which allows it to process user-provided images and documents and generate responses accordingly [12]. For example, a student could upload an image of a chart, graph, or handwritten notes, and ChatGPT would be able to interpret and analyze the content. This capability is particularly valuable in educational settings where students interact with both text and visual materials, as demonstrated in Fig. 2, showcasing ChatGPT's ability to understand and respond to visual inputs.

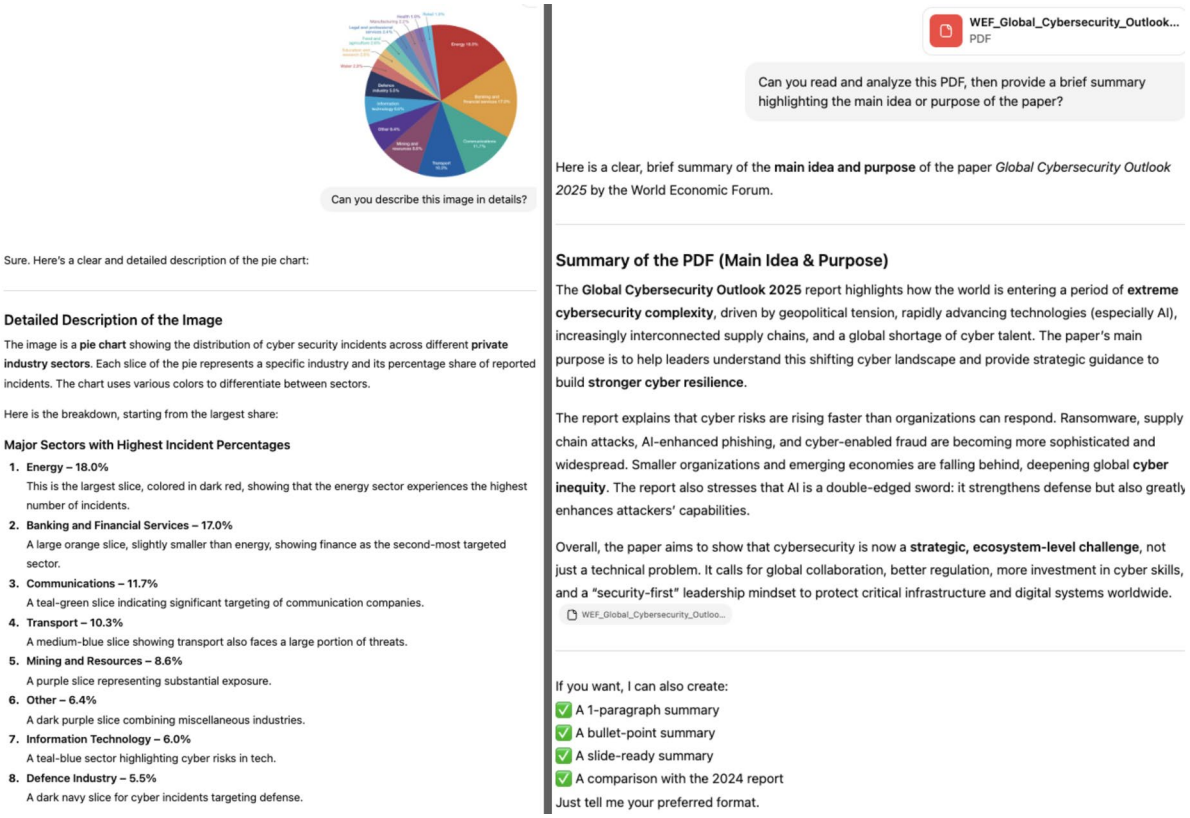

Fig. 2. Showcasing the multimodal ability of ChatGPT to understand and generate responses to visual inputs.

ChatGPT doesn't have real-time access to the internet by default. Which means it cannot check news or stocks, and it can't visit websites (unless you have a version that has specific browse-the-web feature [1]). When browsing is activated, ChatGPT can go on the web and can even cite where some of the information was obtained from further enhancing its utility with academic knowledge [13], as illustrated in Fig. 3 that demonstrates ChatGPT being capable of browsing for real-time information and citing a source.

ChatGPT can even both produce and edit images according to user prompts [14]. A user could describe a scene, and ChatGPT would make an image for it or edit an image to the ask, like in Fig. 4. This creative tool isn't just for artists but can also be used by teachers and students who wish to visualize ideas or create educational content.

With this kind of functionality, such as text discussion, document understanding, picture exchange, and even optional web browsing, ChatGPT has become a versatile learning assistant. It's a tool that scaffolds students, with writing, with reading content and problem solving (even studying visually), in one handy place.

Born in the era of the internet, K-9 to K-12 children experience a time of great openness to digital technology, with portable screens and networked devices increasingly embedded into their lives [15]. This is a generation that many describe as "digital natives", and they are looking not only for learning, but play, social interactions and self-expression on tech. But it's hard to sustain such an intense level of near-constant connection. Screen addiction. Some kids get addicted to screen exposure and as a result, lose their attention span; they tend to have poor sleep hygiene and physical inactivity is increased [16]. Furthermore, their overuse of social platforms and applications, gaming sites and chatting apps puts them at risk to various kinds of cyber threats [17]. This includes cyber harassment, exposure to inappropriate content and online grooming by predators, along with other hazards like identity theft, phishing scams and influence wielded through a disinformation campaign or fake news. The comprehension achievement in elementary, middle and high school students from K-9 to K-12 is on the rise and becomes vulnerable to these menaces as they have not developed their digital literacy or e-safety skills needed for internet threats whereas adult can interact with on-line threat effectively with their rational thinking and cyber security awareness [1, 18]. Without guidance, supervision and education, the digital lives of young people can lead to harmful outcomes for their safety, welfare and ongoing capacity in their digital life. With such security threats, it

becomes much more crucial to be cyber aware in K-9 and K-12 education [1, 19]. However, access to cybersecurity education remains uneven across K-12 contexts. While ChatGPT offers promising interactive and personalized learning experiences, its integration into education aligns with key educational theories. Constructivism, as described by Piaget and Vygotsky, emphasizes the role of active learning and interaction with the environment in constructing knowledge. ChatGPT facilitates self-regulated learning, enabling students to engage in autonomous, adaptive learning processes, while its use can be framed within digital citizenship to promote responsible and ethical engagement with digital content. Survey evidence and teacher-focused studies report that many schools, especially in resource-limited settings, lack dedicated cybersecurity instruction due to gaps in teacher preparation and limited availability of age-appropriate curriculum materials [20, 21]. While having the potential for delivering personal, interactive cyber-awareness training, these platforms (e.g., ChatGPT) also introduce new threats such as misinformation risk, content hallucination, bias and insufficient control [22], thereby themselves becoming part of the problems they have been created to solve [23, 24]. These are mirrored by the technological and ethical concerns common in decentralized digital systems, including financial industries, where transparency, responsivity and applying securely to rapidly developing digital economies is important The effective deployment of ChatGPT in this space therefore requires a careful trade-off between celebrating its positive achievements we don't want children's safety to limit creativity but at the same time being cautious not to create emergent threats from the safeguarding of young learners' well-being and resilience against digital harm. The literature is still scarce concerning how to include ChatGPT into solutions, "Resuming Cyber Awareness Programs" for K-9–K-12 students [1, 19].

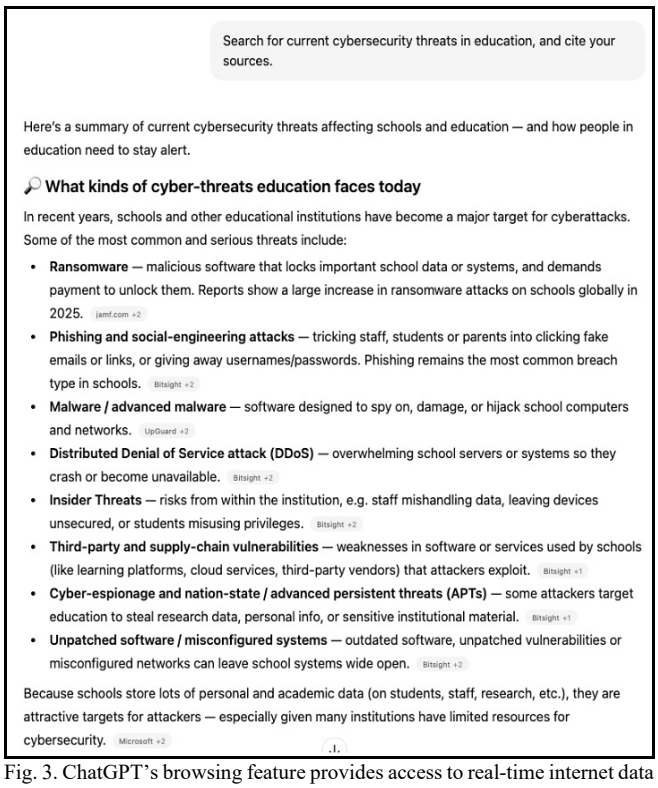

Fig. 3. ChatGPT's browsing feature provides access to real-time internet data and source citations, available in only its browsing-enabled models.

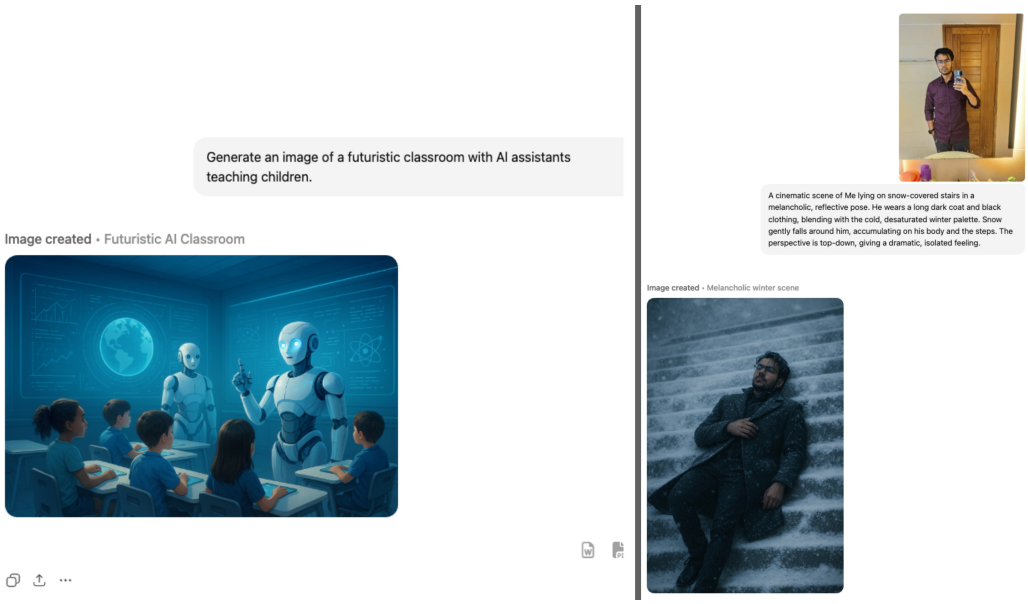

Fig. 4. ChatGPT supports creative and educational uses with its capabilities of image creation and modification on users' prompts texts.

To fill this gap, we propose a conceptual framework for the integration of ChatGPT in K-12 cybersecurity education, using a qualitative approach informed by SWOT analysis and Fishbone diagrams. This framework leverages prompt-generated ChatGPT outputs in educational contexts. By identifying internal and external factors affecting cyber education practices, we outline the likely sources of key risks and opportunities, while conceptually illustrating how these factors may interact over time. This framework is designed to provide strategic insights rather than empirical intervention outcomes. The study is structured as follows:

- We start by gaining a better understanding of the internal strengths and weaknesses, and external opportunities and threats that come with ChatGPT in search for K-9 to K-12 student cyber awareness. This comprises an analysis of challenges like engagement, misinformation and

accessibility, as well as ethical AI considerations.

- Fishbone Diagram (Root Cause Analysis) uses the prompt-generated corpus and prior literature to identify and group root causes underlying high-priority risks and barriers.
- Governance Framework Design In light of the findings, we recommend a governance-based approach that prioritizes ethical AI deployment, real-time content validation, human-in-the-loop oversight and scales across multiple educational settings.

The rest of the paper is organized as follows: Related Work: Section II discusses existing literature in cybersecurity awareness at K-9 to K-12 levels. Section III presents the proposed multimethod framework. In Section IV, we apply Fishbone analysis and SWOT to evaluate ChatGPT-enabled interventions. Section V describes the significance of these strategies and early cybersecurity education. Section VI is the conclusion, with findings and future work.

II. Literature Review

AI is a game changer in multiple industries, such as health care, where AI's four-dimensional depth estimation technique has already increased three-dimensional approaches to perception [25], business, where analytics and predictive modeling powered by AI are informing strategic decision making [26] and education, where pre-service early-childhood teachers' metaphorical conceptions of AI shape curriculum design [27]. In the education field, AI has proven attractive with respect to its transformative potential for teaching and learning in adaptive personalized learning environments, intelligent tutoring systems and personalization of content delivery [28, 29]. The advancement of Natural Language Processing (NLP) technologies has particularly resulted in the development of conversational agents or chatbots that are able to emulate human conversation and perform educational tasks [30]. ChatGPT, from OpenAI, is one of those developments and employs huge transformer architectures to provide context awareness and human-like responses. Since its release in November 2022, ChatGPT garnered quick adoption historically in educational settings, where it has been used to help students construct content, develop ideas and refine digital literacy [31, 32]. Previous studies have highlighted the role of AI in enhancing learning, particularly through its capacity for providing personalized feedback and promoting engagement. This aligns with constructivist theories which argue that learning is most effective when students are actively involved in the process, engaging with material and applying it to real-world contexts. Similarly, ChatGPT supports self-regulated learning, allowing students to navigate content independently and take control of their educational journeys. Moreover, the use of ChatGPT in cybersecurity education can be framed within digital citizenship, fostering responsible digital behavior, critical thinking, and ethical decision-making in an increasingly digital world.

Though the use of ChatGPT in education is promising, there are also some major risks. Researchers have also observed that ChatGPT's function of generating convincing, yet possibly false information can undermine educational integrity and propagate disinformation [33, 34]. Additionally, other problems have been pointed out such as its adverse effects on students' critical thinking and creativity as well as the risk of it being used to cheat in exams [35–37]. Nonetheless, advocates for its use think that proper scaffolding and implementation would enable ChatGPT to help in promoting educational equity, such as by enabling students from marginalized groups access to explanations and support around the clock [38, 39]. However, there is little work available that considers the pedagogical implications generally or the ethical dilemmas of applying it specifically to developing cyber awareness in students.

Cyber awareness, particularly for K-9 to K-12 children [40], is invaluable in the digital era, during which youth are increasingly exposed to deceitful content, online bullying, privacy threats, and addiction to digital technology. AI empowered IoT systems are subject to similar privacy leaks, where personal information can be deduced, disclosed or abused by algorithms in decision-making process, indicating the necessity of protective model and contextual protection [41]. According to Altarawneh *et al.* [42], adolescents seem to lack important cyber security skills especially pertaining to protecting passwords, the safe use of social media and are accordingly at risk from online harms. The authors point out that cybersecurity education for K-9 to K-12 children must be formalized, theoretical and under the guidance of interactive means such as expert lead workshops. Gamified learning environments, peer-based models and scaffolded digital ethics training have been put forward as a solution by some researchers [43, 44]. Nonetheless, the incorporation of AI-powered tools such as ChatGPT in these models is at an early phase and needs to be systematically assessed.

Some researchers have tried to gauge the potential of ChatGPT in education with what-if analysis models like SWOT. According to Farrokhnia *et al.* [45], a SWOT analysis was conducted to explore the strengths, weaknesses, opportunities and threats of ChatGPT in education which identified strengths namely its capacity for personalized on-the-spot feedback production & support for complex learning activities as well as the threats such as academic integrity undermining, taking the conversation out of context and erosion of higher order thinking skills. Similarly, Taktak *et al.* [46] used a SWOT analysis to examine the integration of ChatGPT in K-12 education, with a focus on practical and ethical considerations from teachers' and school leaders' perspectives, and detection emerged as an implementation challenge rather than a pedagogical design issue [47]. SWOT analysis as a tool helps for the systematic identification of internal strengths and weaknesses, and external opportunities and threats, and has been well employed in educational planning and institutional evaluation [45, 48]. Yet, such analyses are typically descriptive and don't dig deep to diagnose root causes or predict how the system will behave over time.

In response to these concerns, educational researchers have employed the Fishbone Diagram [49], the Ishikawa diagram, as a tool to investigate root causes of complex problems. In the school technology integration context, for instance, Fishbone diagrams have been applied to differentiate the source of contributing factors by broad areas, including pedagogy, technological infrastructure, student

engagement and administrative support [47, 48]. For instance, Shinde *et al.* [50] employed Fishbone analysis, a structured approach to identify the root causes of challenges in the education system to systematically categorize issues such as personnel, academics, resources and institutional support that can drive targeted improvement efforts regarding educational quality and infrastructure. Although informative, very limited research has shed light on AI-driven educational systems such as ChatGPT, especially in cybersecurity training.

Taken together, literature reveals two important tensions. First, studies on ChatGPT in education highlight its value for personalized feedback, learner engagement, and self-directed learning, while also raising concerns about misinformation, academic misuse, and reduced critical thinking. This tension becomes even more important in cybersecurity education, where inaccurate or unsafe guidance may directly influence students' digital behavior. Second, existing analytical approaches remain fragmented. SWOT-based studies provide a strategic overview of strengths, weaknesses, opportunities, and threats, whereas Fishbone-based analyses are more useful for tracing underlying causes of implementation challenges. However, these approaches are rarely connected within a single framework. As a result, prior work provides useful descriptive insight, but offers limited synthesis on how pedagogical benefits, ethical risks, and implementation barriers should be jointly evaluated for K-9 to K-12 cyber awareness contexts.

To address these gaps, our work proposes an integrated solution that leverages SWOT analysis, and Fishbone diagrams to have a more comprehensive assessment of zero-cost adaptation for ChatGPT in the cyber awareness education audience for teenagers (ZACEPT). Rather than applying these tools in isolation, the framework links high-level strategic assessment with root-cause diagnosis, enabling a more structured evaluation of both opportunities and risks. In this way, the study advances prior work beyond descriptive discussion toward a more synthesized assessment of pedagogical value, ethical concerns, and implementation challenges in AI-assisted cybersecurity education. This integrated perspective supports the design of more ethical, scalable, and context-sensitive educational strategies for young learners. To investigate this possibility, we articulate the following research questions:

RQ1: How do the internal strengths and weaknesses of ChatGPT, when applied to K-9 to K-12 cybersecurity education, interact with external opportunities and threats to impact the design of a cyber awareness curriculum?

RQ2: What mitigation strategies can be employed to counter misinformation and other high-priority threats in ChatGPT-driven cyber awareness programs for K-12 students, and how can the platform's weaknesses be leveraged to enhance cyber resilience?

RQ3: How can ChatGPT's use in K-12 cybersecurity education be ethically scaled to ensure access to AI-driven digital services for young learners, while avoiding risks such as malicious exploitation (e.g., hacking tutorials using hallucinated content)?

III. The Multi-method Framework

To explore the potential role of ChatGPT in supporting cybersecurity awareness for K-9 to K-12 learners, this study employed a qualitative, conceptual framework that combines SWOT analysis and fishbone-inspired cause-effect mapping. SWOT was used to identify and organize the key internal and external factors, while the cause-effect mapping was used to illustrate how selected factors may influence cyber-awareness outcomes and intervention needs. The primary data source consisted of ChatGPT-generated outputs, produced using a fixed prompt set with the ChatGPT 5.1 model. We began by reviewing prior studies that applied SWOT analysis to ChatGPT in educational contexts, using these studies to guide the structure of our own analysis and adapt the SWOT workflow to our framework [51]. The prompts used in this study focused on classroom-relevant scenarios (e.g., plain-text queries, document-reading prompts, and instructional use cases), with the generated responses captured as a qualitative corpus. Stakeholder perspectives, where considered, functioned as supplementary interpretive and design-oriented inputs to refine the practical framing of the analysis and proposed safeguards. They were not treated as a separate formal qualitative dataset and were not independently coded or analyzed. Next, we applied SWOT analysis to identify internal strengths and weaknesses, as well as external opportunities and threats, based on themes extracted from the data generated. This analysis was further supported by comparisons with existing peer-reviewed literature to ensure the validity of the identified factors, while stakeholder-informed considerations were used only to refine interpretation and practical relevance rather than to serve as standalone evidence. In addition, we used a Fishbone (Ishikawa) diagram to analyze and map the root causes of a single focal issue, the ineffective or unsafe use of ChatGPT in the classroom. This process allowed us to organize causal factors and provided the foundation for the proposed governance framework, which emphasizes ethical AI deployment, validation practices, and teacher-in-the-loop oversight.

A. SWOT Analysis

As outlined by Mas'adi *et al.* [52], SWOT has traditionally been employed as a strategic planning instrument to evaluate internal strengths and weaknesses, and external opportunities and threats. This model provides a systematic structure to implement an improvement strategy that maximizes benefits and minimizes risk. In this study, SWOT was used to consolidate recurring themes extracted from the prompt-generated outputs into a structured strategic view, consistent with prior education-focused SWOT analyses of ChatGPT that synthesize evidence and implications.

SWOT analysis was employed in this study to compare internal and external factors and develop improvement strategies. The importance of each factor was assigned using a heuristic approach based on expert judgment, prior literature, and the factor's relevance to the study's goals. The importance levels were defined as follows: 4 = Critical Importance, 3 = High Importance, 2 = Moderate Importance, and 1 = Low Importance. This prioritization helps focus on the most strategically significant factors in implementing ChatGPT for K-12 cybersecurity education. The analysis incorporates IFAS and EFAS matrices as outlined by Arda *et al.* [53].

B. Fishbone Diagram

The Fishbone Diagram was employed to analyze the root causes of major problems and opportunities with the application of ChatGPT in K-9 to K-12 students' cyber awareness education. Adopting the process proposed by Mujayyin *et al.* [54], the process involved:

(1) Preparing relevant data,
(2) Identifying core problems,
(3) Categorizing causes,
(4) Validating findings, and
(5) Reaching consensus on primary causes.

IV. Analytics and Use-Cases

This study adopts a novel SWOT-based analysis model to assess the contributions of ChatGPT to the improvement of cyber awareness in K-9 to K-12 school students [55]. The discussion starts out by highlighting the most important strengths, e.g., real-time simulations, fair access, adaptive feedback and contextualization in the context of teaching online safety. These capabilities showcase ChatGPT's potential for offering tailored, scalable and interactive learning experiences. Weaknesses reveal important considerations concerning misinformation, lack of real-time threat intelligence updates, hallucination and supervision content that directly constrain the reliability of its use in sensitive educational settings.

The identified opportunities include support for gamified and multilingual learning, teacher collaboration, real-time feedback, and early legal literacy for children in using digital environments among the resource-deprived schools [44]. On the other hand, there are threats to data privacy violations, student addiction and reliance on it for bad purposes and legal issues. These insights ground the central study research questions and inquiry into the interplay of ChatGPT capabilities and external educational risks (RQ1), co-designed strategies for risk mitigation (RQ2), and governance frameworks for responsible, ethical deployment (RQ3).

A. Strengths of ChatGPT

Our literature review has identified the following strengths for ChatGPT.

Interactive cyber threat simulation: ChatGPT can simulate phishing, scams, password theft, and other common cyber risks in a safe and age-appropriate way, helping students practice how to respond before facing such threats in real life.

Personalized and contextualized learning: ChatGPT can adjust its explanations based on student age, prior knowledge, and everyday digital contexts such as gaming, messaging, and school devices, making cybersecurity concepts easier to understand and more relevant.

Accessible and scalable support: As a low-cost and widely available tool, ChatGPT can expand access to cybersecurity education, especially in schools with limited specialist staff or curriculum resources. Its multilingual capabilities can also support diverse student populations.

Just-in-time guidance: ChatGPT can provide immediate support when students face online uncertainty, such as suspicious messages or websites, offering timely explanations and preventive guidance.

Support for reflective thinking: Beyond giving answers, ChatGPT can encourage students to explain their reasoning, compare choices, and reflect on safe online behavior, thereby supporting critical thinking and digital citizenship.

B. Weaknesses of ChatGPT

Even though ChatGPT has many novel capabilities, it should also be noted that ChatGPT carries some weaknesses as illustrated below.

Risk of inaccurate or outdated information: ChatGPT may generate incorrect, oversimplified, or outdated cybersecurity advice, which can mislead young learners who may lack strong fact-checking skills.

Lack of real-time awareness: Because it does not always reflect current cyber threats or newly emerging online scams, its guidance may not fully prepare students for rapidly changing digital risks.

Dependence on human supervision: ChatGPT cannot replace teacher or expert judgment, particularly in sensitive, ethical, or emotionally complex situations. Safe and pedagogical sound use still requires monitoring and guidance.

Limited hands-on learning: While useful for explanation and simulation, ChatGPT cannot fully replace practical activities, demonstrations, or real-world exercises that help students build deeper cybersecurity skills.

Infrastructure and access constraints: Effective use depends on internet connectivity, devices, and digital literacy, which may be limited in under-resourced schools and communities.

C. Opportunities for Education

ChatGPT could potentially offer a wealth of opportunities for K-9 to K-12 students and educators. Some of the key opportunities for ChatGPT in education are as follows.

Early cyber awareness and digital citizenship: ChatGPT can help introduce safe online behavior, privacy awareness, and responsible digital communication from an early age, supporting long-term cyber habits.

Teacher support and curriculum integration: Teachers can use ChatGPT to generate examples, classroom scenarios, lesson materials, and guided discussions, even when they do not have deep cybersecurity expertise.

Gamified and adaptive learning: ChatGPT can support quizzes, role-playing, storytelling, and game-like cyber awareness activities that may improve engagement, retention, and motivation among younger learners.

Real-time feedback and reinforcement: Students can receive immediate explanations and feedback on their responses, which can strengthen understanding and correct misconceptions during learning.

Inclusive and multilingual learning: ChatGPT can make cybersecurity instruction more accessible for English language learners, international students, and learners in underserved settings by offering flexible and multilingual support.

Ethical and legal awareness: ChatGPT can also help explain the consequences of harmful online behavior, including cyberbullying, hacking, and privacy violations, in age-appropriate language.

D. Threats to Education

Although the strengths of ChatGPT result in different

types of educational opportunities, its weaknesses also imply some unclear threats, which I highlight below.

Privacy and data protection risks: Students may unintentionally share sensitive personal information while interacting with ChatGPT, raising concerns about privacy, consent, and compliance with child protection regulations.

Overreliance and reduced critical thinking: Excessive dependence on ChatGPT may discourage students from developing independent judgment, skepticism, and problem-solving skills that are essential for safe online behavior.

Misinformation and unsafe guidance: If students trust inaccurate or hallucinated outputs, they may adopt unsafe cybersecurity practices or misunderstand important online risks.

Malicious misuse: Some students may try to use ChatGPT to obtain hacking-related guidance, bypass restrictions, or explore harmful digital behavior, which could undermine the educational purpose of the tool.

Bias, resistance, and unequal adoption: Ethical concerns, bias in AI outputs, teacher or parent resistance, and unequal school resources may limit consistent and fair implementation across educational settings.

Reduced collaborative learning: Since ChatGPT mainly supports one-to-one interaction, excessive use may weaken peer discussion, group problem-solving, and other social learning experiences important in K-12 classrooms.

Security and data breach concerns: When integrated with third-party classroom systems or school platforms, ChatGPT-based tools may introduce additional risks related to data storage, misuse, or unauthorized access.

A detailed SWOT analysis of adopting ChatGPT as a cyber awareness tool for K-9 to K-12 children is illustrated in Fig. 5. This analysis gap can separate internal and external factors (strengths-weaknesses, opportunities-threats) which further contribute to the overall strategic assessment.

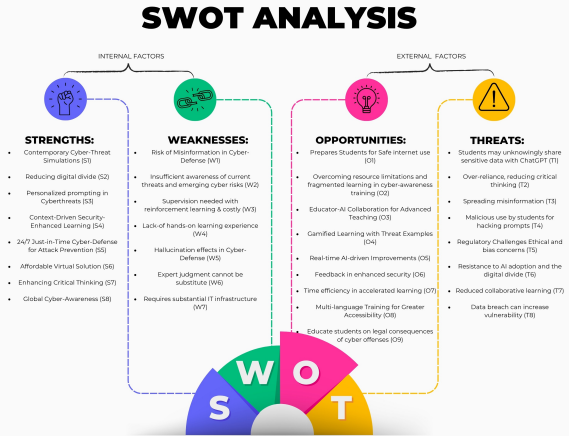

Fig. 5. SWOT analysis for using ChatGPT to promote cyber awareness education amongst young learners.

E. SWOT Analysis Interpretation and ChatGPT Driven Insights

SWOT analysis is an attempt to understand what influence an AI tool, ChatGPT, can have on the cyber-awareness of young learners. Major significant strength-opportunity (S-O), Strength-Threat (S-T), Weakness-Opportunity (W-O), and Weakness-Threat (W-T) pairings were derived from literature and K-9 to K-12 student-focused workshops, which mapped and prioritized the S-O W-T intersections using a cross-impact matrix Table 1 and final prioritization Table 2.

Table 1. The relationship between the strengths & weaknesses (rows) and the opportunities/ threats, as mapped under SWOT Interaction Matrix

SWOT	O									T								
	O1	O2	O3	O4	O5	O6	O7	O8	O9	T1	T2	T3	T4	T5	T6	T7	T8	
S	S1	1	0	1	1	1	1	0	0	1	1	0	1	1	0	0	0	0
	S2	1	1	1	1	0	1	1	1	0	0	1	1	0	0	1	1	0
	S3	1	0	1	1	0	1	1	0	0	0	1	0	1	1	0	0	0
	S4	0	1	1	1	1	1	0	0	1	0	0	1	0	1	1	0	1
	S5	1	1	0	0	1	1	1	1	0	0	1	1	1	0	1	0	1
	S6	1	1	1	0	0	1	1	0	0	0	1	1	1	0	0	1	0
	S7	0	1	1	1	0	0	1	1	1	1	1	1	0	0	0	1	1
	S8	1	0	1	0	1	1	0	0	0	1	0	1	1	0	0	0	0
W	W1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	0	1	1
	W2	1	1	0	1	1	1	1	1	1	1	0	1	0	1	1	1	0
	W3	0	0	1	1	1	1	0	1	0	0	0	0	1	0	0	0	1
	W4	0	1	1	1	0	1	0	1	0	1	1	1	0	1	0	1	1
	W5	0	1	0	0	0	1	0	1	1	1	0	1	1	0	1	0	1
	W6	1	0	1	1	0	1	0	1	0	0	0	1	0	0	0	0	1
	W7	1	0	1	0	0	0	0	1	0	0	1	0	1	0	1	1	1

The cross-impact matrix showing the relation among the identified SWOT is depicted in Table 1. The quadrants in the matrix correspond to SWOT categories: external positive factors (Opportunities), internal negative factors (Weaknesses clause 1) and external negative factors (Threats) and so on; while a cell contains information about the presence of interaction or its absence. Operationally, this matrix is an adjacency matrix of a graph representing directions between SWOT factors. The SWOT analysis in this study uses Table 1, a cross-impact matrix, to show how the SWOT factors (Strengths, Weaknesses, Opportunities, Threats) interact with each other. A cell marked with "1" indicates an interaction between two factors, helping identify key leverage points. Table 2 prioritizes these interactions into Top Priority, High Risk, High Impact, and Growth categories, guiding the development of targeted interventions and strategies for responsible AI deployment in K-12 cybersecurity education.

The filled-in intersections (i.e., cells with value 1) indicate a critical cross-influence like S2 → O2, S3 → T2, W1 → T3, of strategic importance in understanding the impact of ChatGPT on cyber awareness-hyper-awareness among young learners. These interactions can be examined to identify dominant pathways, key leverage points, and high-risk links. In addition, the SWOT matrix can be used to derive four strategy types by pairing internal and external

factors: Strengths-Opportunities (S-O), Strengths–Threats (S-T), Weaknesses-Opportunities (W-O), and Weaknesses–Threats (W-T).

S-O Intercrossing: This intersection-intercross marked where ChatGPT's internal strengths can possibly be used to take advantage of external opportunities in K-9 through K-12 cyber awareness education. Through the intersection of these points, to specific capacities of AI with context of learning environments, such intersections illuminate not only how strengths are leveraged by opportunities but may serve to scale, to customize and support digital safety training.

- S1O1: The strength of using cyber-threat simulations to increase students' propensity for safe internet usage is consistent with the possibility of increasing digital safety through experiential learning.
- S2O2: ChatGPT's opportunity to narrow down the digital divide is definitely a strong point /supportive of this strength) for the opportunity to address resource constraints, particularly in underprivileged/rural educational settings.
- S4O3: Learning based on context, where content is customized to the learner and the situation, enables us to create a possibility of productive collaboration among educators.
- S5O5: The persistent availability of AI for cyber defense training (24/7 access) enhances the potential for real-time, AI-enabled updates to the cyber-awareness content materials to maintain more useful and immediate response-focused information.
- S7O7: It is a strength of the methodology to be able to foster critical thinking in students, and this is opportune for time efficiency during learning when using AI tools such as ChatGPT.

S-T Intercrossing: S-T intercrossing demonstrates how ChatGPT's advantages may attenuate external rises in education. These strengths contribute to safety and responsible use for digital learning as K-9–K-12 students are exposed more exclusively to critical thinking, ongoing access, and structured uses of AI.

- S1T3: Malpractices are pre-prepared and cyber-threat simulations can be a pro-active strength to raise awareness among the younger generation to get patched to what's wrong while consuming malicious files. This may help to mitigate the exposure to fake news depending on how teachers address online information literacy skills with students.
- S2T6: By reducing the digital divide, more people are comfortable with technology, which means that there is less resistance to AI-based educational platforms. Through more organized exposure of learners to AI, apprehensions and reticence can be most effectively countered.
- S5T4: AI cyber defense tools are always on, giving users 24/7/365 monitoring and response. This ongoing defense helps mitigate the danger of AI being used for negative purposes, like illicit hacking.
- S7T2: Encouraging students to be critical and circumspect of AI-generated content. This mitigates against over-assimilation of AI, by prompting users to question, verify and contextualize information rather than unquestionably taking them at their word.

W-O Intercrossing: W-O intercrossing highlights how shortcomings in ChatGPT's potential for use in cybersecurity education can be mitigated with strategic opportunities, such as instantaneous feedback, gamified learning, and teacher partnerships to improve its effectiveness in K-9 to K-12 applications.

- W1O6: Another weakness is the wide range of disinformation in AI cyber-defense tools. This may be scaled with the help of built-in real-time security systems' feedback loops. Feedback loops allow the system to learn from user reports and expert validations, which increases response accuracy and reliability.
- W2O1: Younger generations have no basic knowledge of cybersecurity. This gap can be filled with initiatives that encourage responsible online behaviors like national digital literacy programs, curriculum adoption, or interactive methods for teaching digital hygiene in an engaging manner.
- W4O4: The obvious deficiency in the current cyber awareness training is the absence of hands-on, experiential learning. This could be addressed using a gamified learning environment. It's the tangible application of abstract cybersecurity concepts that makes gamified modules more interesting and easier to learn.
- W6O3: AI tools can help learning, but they should not be used to substitute expert human judgment. This challenge provides a moment in which we can build inclusive educators and AI systems. Through permitting teachers to curate, moderate and provide context for AI outputs, learners can access the scalability of an automated online tutor while being under expert supervision.

W-T Intercrossing: The overview of W-T intercrossing also reveals how vulnerabilities already present in ChatGPT may exacerbate externally imposed harms, such as those in educational settings. When misinformation, low awareness and hallucinations are left unchecked, they exacerbate risks such as unsafe behavior, regulatory hurdles and misuses of AI by students.

- W1T3: One of the biggest issues with current AI-enabled educational systems are misinformation. Uncontrolled, that susceptibility adds directly to the greater menace of misinformation contagion in online spaces, especially for less experienced digital denizens such as youthful learners who may not always recognize credible sources.
- W2T5: Insufficient cyber security awareness in youth, causing them to be prone to internet threats This vulnerability doesn't just endanger students; it also confuses the heck out of broader efforts to protect K-9 to K-12 children online. This raises the problem of enforcing compliance or ensuring safe digital spaces when AI is embedded in learning platforms.
- W5T4: The hallucination problem of AI producing fake or faulty information is a serious risk. And if these effects are fabricated technical content (e.g., fake hacking tutorials), then it allows a bad actor to weaponize them. This vulnerability also increases the risk of AI abuse for malicious or illegal purposes: thus, it stands as a high-priority threat that requires mitigation.

The SWOT interaction matrix clearly articulates crucial strength-opportunity and weakness-threat linkages, which

directly answer RQ1. It outlines how ChatGPT's characteristics interact with external elements to predict K-9 to K-12 students' cyber awareness performance.

- S2 → O2 (High Impact): The potential of ChatGPT in mitigating the digital gap (S2) matches the prospect of overcoming cyber-awareness shortcomings (O2). This shows that AI tools can serve as scalable, always-on tutors and help close access gaps in rural or under-resourced communities.
- S1 → T3: (High Risk): While cyber-terrorism exercises serve to make their content realistic (S1), they have the side effect that misinformation can self-replicate if not carefully vetted and validated. This indeed substantiates the two-sided face of ChatGPT: an enabler and a risk to enable speech.
- W1 → T3 (High) (Misinformation Threat → Misinformation ChatGPT): Misinformation in ChatGPT responses (W1) can be directly connected to a threat such as the proliferation of misinformation (T3). This combination represents the single most harmful interaction, revealing a fundamental weakness in how unsupervised AI is used by K-9 to K-12 learners.
- W4 → O4 (Growth): The problems of no hands-on learning (W4) are resolved in gamified ChatGPT interactions (O4), making active learning happen. When it comes to learning, what young people enjoy is playing around which we can use for decidedly unfun purposes.

Table 2. Matrix of priorities showing how to act in relation to what is happening. Each line contains priority, interacting SWOTs, the category of these and what reaction is suggested

Priority	Intercrossing	Category	Action Required
Top Priority	W1 → T3 (Misinformation → Spreading Misinformation)	Weakness-Threat (W-T)	Immediate AI validation, security training
High Risk	S1 → T3 (Cyber-Threat Simulations →Spreading Misinformation)	Strength–Threat (S-T)	Reinforce factchecking in simulations
High Impact	S2 → O2 (Reducing Digital Divide →Overcoming Cyber-Awareness Limitations)	Strength-Opportunity (S-O)	Expand AI-based learning & outreach
Growth	W4 → O4 (Lack of Hands-on Learning → Gamified Learning)	Weakness-Opportunity (W-O)	Implement interactive learning tools

These strategies were refined using youth-centered design input, emphasizing the importance of developing safeguards that are understandable, engaging, and contextually relevant for young learners. More specifically, this input supported the use of gamified learning tasks, "explain your reasoning" checkpoints, and familiar platform-based scenarios to make the framework more practical for K-9 to K-12 settings.

(1) Real-time fact-checking integration (e.g., automated link verification and citation).
(2) Human-AI collaboration models, where educators guide and contextualize AI output.
(3) Usage guidelines for developers and institutions, focusing on protecting minors from AI hallucination content (e.g., fake hacking tutorials).

RQ1: How do the internal strengths and weaknesses of ChatGPT, when applied to K-9 to K-12 cybersecurity education, interact with external opportunities and threats to impact the design of a cyber awareness curriculum?

We conducted a SWOT analysis (Fig. 5, Table 1) using literature data and K-9 to K-12 students-centric analysis. Below, each major intercrossing is summarized and explicitly linked back to RQ1.

- S2 → O2 (Reducing digital divide → Overcoming cyber-awareness limitation) ChatGPT's scalability and 24/7 availability (S2) directly support under-resourced schools by filling gaps in cybersecurity instruction (O2). This confirms RQ1's prediction that ChatGPT strengths can leverage external opportunities to unify and extend cyber training.
- S5 → O5 (Real-time AI improvements → Adaptive feedback loops) The platform's real-time interactivity (S5) enables on-the-fly correction of misconceptions (O5). This supports RQ1 by showing adaptive lessons enhance learning continuity. S1 → T3 (Cyber-threat simulations → Spreading misinformation) While simulations (S1) train recognition of phishing, they may inadvertently reinforce false threat models if unvalidated (T3). This refines RQ1 by highlighting that without factchecking, strengths can exacerbate threats.
- S7 → T2 (Critical-thinking prompts → Overreliance reduction) Including reflection questions on paper task (S7) decreases students' overreliance to AI outputs (T2). This supports RQ1, that users can be over-reliant on built-in cues.
- W1 → O5 (Misinformation risk → Real-time feedback) The danger of hallucinations (W1) may be mitigated through instantaneous loops for correction (O5). This evidence supports RQ1 by suggesting that deficiencies can be compensated for with available AI capabilities.
- W4 → O4 (Not hands-on learning →Gamified module) ChatGPT's relational style of conversational format (W4) can have modules translated to gamified "escape rooms" (O4), this would help in making the learner more engaged. This finding provides support to view of RQ1 that having opportunities can convert weaknesses into learning benefits.
- W1 → T3 ((High importance) Hallucination risk → Dissemination of misinformation) Risk of hallucinations (W1) directly drives dispersion (T3). It is this crucial connection that emphasizes RQ1's caution against the untampered AI output, which can exacerbate the danger.
- W2 → T5 (Over-reliance → Regulatory challenges) Over the students' reliance on ChatGPT (W2), which complicates compliance with COPPA/GDPR-K policies (T5). This characterizes RQ1 by discovery of one policy loophole because of the DCS's and the user interaction.

ChatGPT's opportunities and its strengths in personalization, accessibility do align with high interest educational gaps (O2, O5), validating our hypothesis, however only if we control misinformation, over-reliance threats (W1 → T3, W2 → T5) using built-in validation and critical-thinking prompts. Overall, the SWOT analysis identifies and prioritizes the main strategic factors shaping the use of ChatGPT in cyber awareness education, including the most important enabling conditions, risks, and high-priority interactions.

Whereas the SWOT analysis identifies and prioritizes the main strategic factors, the fishbone-inspired causal maps extend the analysis by showing how the most important of these factors may operate in practice. Rather than repeating

the SWOT findings as a second list, this section group selected high-priority factors into causal pathways that influence cyber-awareness outcomes, including educational effectiveness, inclusion, safety, and responsible deployment. In this adapted representation, strengths and opportunities are treated as enabling influences, whereas weaknesses and threats are treated as constraining influences. The causal mapping was informed by literature analysis and supplemented by teen-centered and expert-informed interpretive considerations.

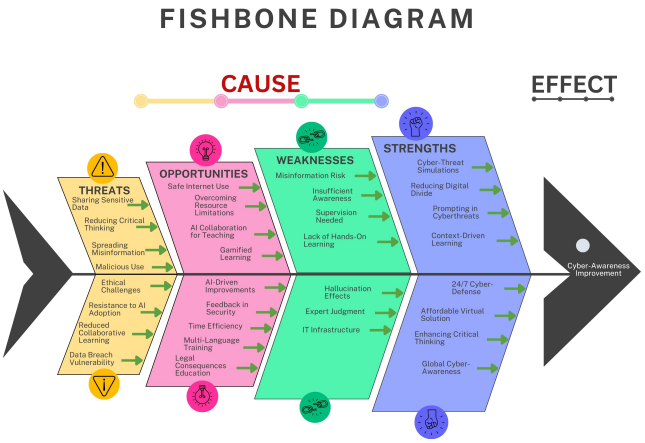

Fig. 6. Fishbone-inspired causal maps showing how strengths, weaknesses, opportunities, and threats associated with ChatGPT may shape cyber-awareness outcomes among young learners.

Fig. 6 provides an integrated causal view of how selected SWOT-derived factors may shape cyber-awareness outcomes among young learners. Its purpose is not to restate the SWOT categories, but to illustrate how prioritized factors interact and contribute to learning quality, accessibility, safety, and implementation challenges.

The following fishbone diagrams focus on the most analytically significant SWOT factors identified earlier and show how they may contribute to specific educational outcomes or constraints.

F. Strength

Fig. 7 presents a cause-effect view of strength-related enabling factors that may improve cyber-awareness outcomes in young learners. In this adapted framework, strengths are treated not as root causes of a problem, but as positive drivers that support educational effectiveness, learner engagement, accessibility, and self-paced digital safety learning. The figure complements RQ1 and RQ3 by showing how these internal advantages of ChatGPT may contribute to broader educational benefit when aligned with appropriate pedagogical use.

- Contemporary Cyber Threat Simulations (S1): ChatGPT allows for interactive, scenario-based learning environments in which students are exposed to simulated phishing attacks or privacy invasions. This type of learning fosters awareness of context and encourages active conduct in cyberspace.
- Digital Inclusion Support (S2): The text-based model, ChatGPT contributes to the reduction of the digital divide by augmenting the scaled availability of educational content. Youth from rural or underprivileged communities can gain access to the same caliber of cyber literacy resources as those in urban areas.
- Personalized Learning Experience (S3): ChatGPT personalizes explanations for the learner's understanding level using dynamic prompts and conversational feedback. It also gives you the ability to translate languages, which is great for ESL students.
- 24/7 Availability for On-Demand Learning (S4): The platform runs 24/7, which allows students to access information or seek clarification on any topic at any time and supports self-paced learning.
- Cost-Effective Cyber Awareness Training (S5): ChatGPT eliminates the necessity for high-cost licenses or instructor-led programs by providing a low-cost cost scalable AI-powered tutoring system for digital safety training.
- Enhancing Critical Thinking (S6): If prompted in the right way, ChatGPT might lead students to think critically about source credibility, confirm facts and reflect on safe digital practice.
- Global Awareness Cultivation (S7): Being exposed to global digital norms, laws and case based cyber incidents will help ChatGPT raise awareness from international cyber security practices.

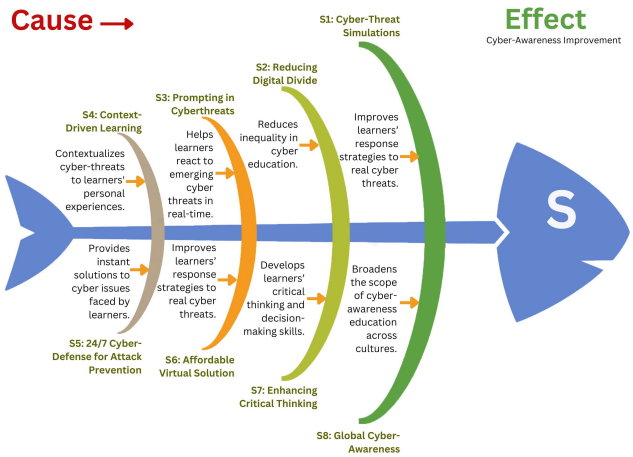

Fig. 7. Cause-effect diagram showing how strength-related enabling factors associated with ChatGPT may support improved cyber-awareness outcomes in K-9 to K-12 learners.

G. Weaknesses

Fig. 8 presents weakness-related constraining factors that may reduce the educational reliability and practical effectiveness of ChatGPT for cyber-awareness development in young learners. In contrast to the strength and opportunity diagrams, this figure is closer to a conventional barrier-oriented cause-effect representation, since it highlights factors such as misinformation susceptibility, contextual misunderstanding, accessibility limitations, and insufficient hands-on learning support. These issues directly inform RQ2 by identifying where mitigation strategies and instructional safeguards should be prioritized.

- Misinformation Risk (W1): ChatGPT may share out-of-date information and potentially misleading or hallucinated content that could inadvertently help to stoke the fires of misinformation among younger users.
- Lack of Supervision or Contextual Judgment (W2, W3): Responses may be misunderstood and advice can go without context. ChatGPT does not have human capability to assess the maturity or emotional state of a

user.

- Technical Accessibility Issues (W4, W7): Internet stable enough for access and a basic level of digital literacy are mandatory. Areas with inadequate infrastructure or low device penetration, however, could encounter difficulties with implementation.
- Content Gaps in Hands-On Learning (W5): ChatGPT lacks the hands-on nature of drag and drop, or gamified Cyber labs that are preferred by students in the younger years for engagement (W5).
- Customization Limitations (W6): While responsive, CS may not be able to easily integrate complex curricula without the guidance of experienced educators.

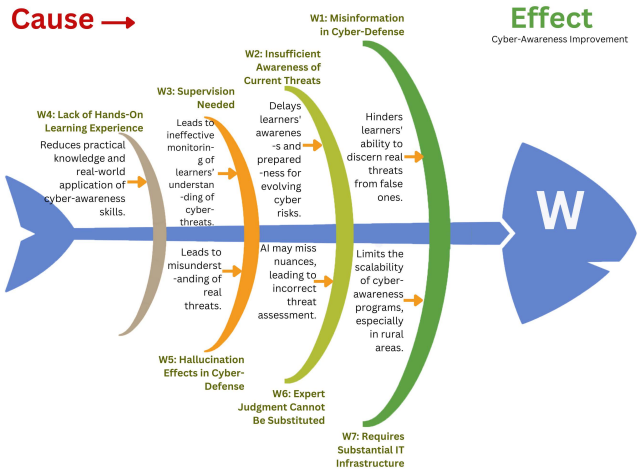

Fig. 8. Cause-effect diagram showing how weakness-related barriers may constrain cyber-awareness development in young learners.

H. Opportunities

Fig. 9 illustrates opportunity-related enabling conditions that may expand the beneficial educational use of ChatGPT in cyber-awareness programs for young learners. In this adapted cause-effect view, opportunities are treated as external drivers that can amplify impact through multilingual delivery, remote learning support, educator assistance, accessibility enhancement, and gamified instructional design. The figure supports RQ1 and RQ3 by showing how upstream institutional and technological conditions may strengthen the positive educational role of ChatGPT when governed appropriately.

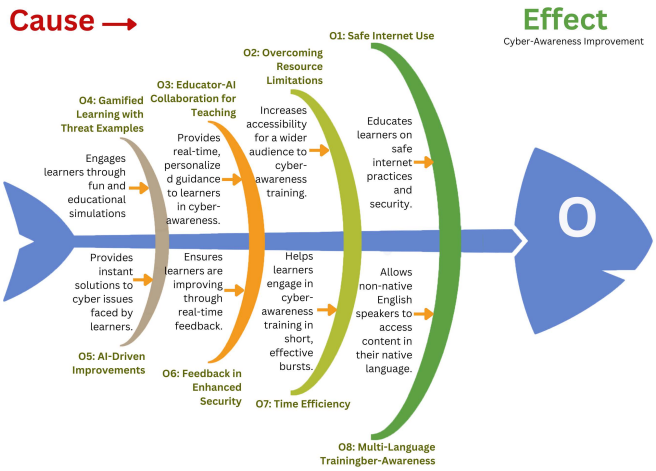

Fig. 9. Cause-effect diagram illustrating how opportunity-related external enablers may strengthen cyber-awareness education outcomes in young learners.

- Remote Cyber Literacy Programs (O1): Schools and non-profits can deploy ChatGPT to teach basic internet safety, password hygiene, and digital rights in remote or hybrid classrooms.
- Support for Multilingual Awareness (O2): With its multilingual capabilities, ChatGPT can deliver cyber awareness training in students' native languages, fostering better comprehension.
- Gamified Curriculum Design (O4): The tool can generate quizzes, challenges, and scenarios that simulate real-world digital dilemmas, encouraging active learning.
- Real Time Feedback & Intervention (O5): Teachers can use ChatGPT as a co-instructor to monitor student queries, identify patterns of misunderstanding, and respond quickly with corrections.
- Equity in Access to Digital Knowledge (O6): ChatGPT supports students with special needs through integrations with text to speech, audio explanations, or simplified outputs for cognitive disabilities.
- Educator Support and Resource Generation (O3): Teachers can leverage the tool for preparing safety modules, creating discussion prompts, and even translating cybersecurity policies into age-appropriate language.

I. Threats

Fig. 10 illustrates threat-related constraining factors that may negatively influence the safe and responsible use of ChatGPT in cyber-awareness education. These factors include misinformation amplification, educator resistance, overreliance on AI, privacy concerns, regulatory uncertainty, and misuse risks. In methodological terms, this figure aligns most closely with a traditional negative-effect cause-effect interpretation, and it directly supports RQ2 and RQ3 by highlighting where policy safeguards, oversight mechanisms, and real-time mitigation strategies are most needed.

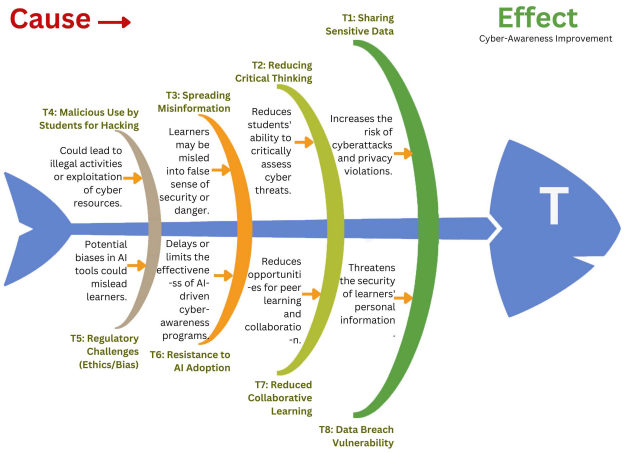

Fig. 10. Cause-effect diagram illustrating how threat-related external barriers may negatively affect cyber-awareness improvement in young learners.

- Viral Misinformation Spread (T3): Due to its conversational authority, students may share ChatGPT-generated misinformation with peers, reinforcing inaccuracies unless moderated.
- Resistance from Traditional Educators (T1): Some educators may perceive ChatGPT as a replacement rather than a supplement, leading to reluctance in adoption due to job displacement fears or skepticism about AI pedagogy.
- Data Privacy and Consent Concerns (T5): Interactions

with minors raise ethical issues around data storage, consent, and potential exploitation, especially in countries with strict child data regulations.

- Over Reliance on AI (T2): Students may become dependent on AI responses, which could limit critical thinking, problem solving, and teacher-student interactions.
- Compliance and Regulatory Challenges (T4): Schools may face legal restrictions or scrutiny if AI systems like ChatGPT inadvertently breach COPPA, FERPA, or GDPR K guidelines.
- Cybersecurity Risks from Misuse (T6): Unregulated access could lead to misuse of ChatGPT by students (e.g., generating fake phishing emails or bypassing restrictions), undermining the very goal of cyber awareness.

RQ2: What mitigation strategies can be employed to counter misinformation and other high-priority threats in ChatGPT-driven cyber awareness programs for K-12 students, and how can the platform's weaknesses be leveraged to enhance cyber resilience?

Using Ishikawa (Fishbone) diagrams (Figs. 7–10), we decomposed each SWOT category to identify root causes and targeted interventions. Key findings:

Misinformation Risk (W1): Root causes include training data bias and lack of real-time fact checking.

Mitigation: Integrate an external fact-check API and scaffolded prompts that require users to verify sources.

- This directly answers RQ2 by co-designing an automated validation layer to neutralize W1→T3.
- Over-reliance (W2): Caused by students' low digital literacy and conversational UI.

Mitigation: Embed "explain your reasoning" checkpoints before AI answers and peer-review tasks.

- This confirms RQ2's premise that critical-thinking scaffolds can reduce W2→T2.
- Lack of Hands-On Learning (W4): Arises from chat-only interactions.

Mitigation: Develop gamified labs (digital "escape rooms") informed by youth-centered feedback, reflecting student preference for more interactive and game-like learning formats.

This shows RQ2 strategies can turn weaknesses into interactive learning experiences.

Our fishbone analysis validates three priority interventions: automated fact checking, critical-thinking prompts, and gamified modules that neutralize top threats and leverage ChatGPT strengths, fulfilling RQ2.

V. Discussion

Through a multivariate analysis, this study sought to identify the promise and difficulties of using ChatGPT in cybersecurity awareness training for K-9 to K-12 students. These applications provided additional insights into what ChatGPT can do, where it falls short, and how it operates within the larger educational framework.

Our SWOT analysis revealed the following strengths of ChatGPT: always-on, personalized experience, and scalability. It also presents weaknesses such as hallucination, overfitting and misinformation risk. From a pragmatic view, this analysis enables points of discussion for stakeholders: "What do we want to achieve with ChatGPT?

One could take the route of solely prioritizing ChatGPT's weaknesses and threats, trying to restrict or ban its use in education. But experience has demonstrated that outlawing new technology is not often efficacious, particularly among teens born into a digital environment. Another possible response would be to rely on external detection tools (e.g., GPTZero) to detect AI-generated content, but this is a losing game of cat and mouse as AI tools continue to evolve faster than such detectors. These SWOT patterns are broadly consistent with recent education-focused studies on ChatGPT and generative AI, which report similar strengths (scalability, on-demand support, and personalized feedback) alongside recurring risks such as hallucinations/misinformation, bias, over-reliance, and equity constraints [47]. Recent K-12-oriented reviews and teacher-focused studies further emphasize that these benefits and risks depend strongly on implementation conditions such as educator preparedness, scaffolding, and oversight [52]. Building on these shared observations, our contribution is to contextualize these recurring themes for K-12 cybersecurity awareness, where risk boundaries are tighter and governance requirements (teacher-in-the-loop oversight, validation practices, and age-appropriate safeguards) become central to safe adoption [53]. A more proactive and future-proofed landscape would involve harnessing the opportunities that ChatGPT represents, such as learning authentic digital literacy skills and dynamic real-time engagement while making concerted efforts to mitigate its risks. This should involve a re-imagining of cyber awareness curricula in terms of interactive learning, critical thinking and the ethical use AI. Guided by educators, ChatGPT can nurture higher-level skill development.

The Fishbone diagram 6 provided a clearer picture of root causes to the misuse or improper use of ChatGPT in K-9 to K-12 students' education. It demonstrated that problems do not only come from the technology, but from systemic aspects such as lack of teacher training (Man), inadequate regulation (Method), bad content curation (Material) or unrestricted access areas (Zone). These results suggest that effective integration will require multi-level intervention: training for educators, mechanisms for moderating installment content, supportive policy as well as inclusive design.

Our combined analysis regarding RQ1–RQ3 constitutes both a scaffolding: ChatGPT is personalization to support cyber-awareness when complemented with systematic validation and critical thinking scaffolds, along with embedding within ethical governance, ensures safe and scalable deployment.

(1) Leverage Personalization (RQ1)

- Integrate gamified quizzes and simulations that align ChatGPT strengths (S1–S5) with learning opportunities (O2–O5).
- Embed language-toggle and accessibility features to bridge digital divides.

(2) Embed Validation & Oversight (RQ2)

- Deploy an external fact-check API before responses are shown.
- Introduce "explain your reasoning" and peer review checkpoints to foster critical evaluation.
- Train educators to moderate and contextualize AI outputs.

(3) Implement Ethical Governance (RQ3)

- Adopt the four-pillar framework: real-time validation, human-AI collaboration, clear usage policies (COPPA/GDPR-K), and adaptive access controls.
- Establish transparency dashboards for students, teachers, and policymakers.

For example, during a phishing-awareness lesson, a student may ask ChatGPT whether a suspicious message is legitimate. In the proposed framework, the response would be validated before display, the student would be prompted to explain their reasoning, and the teacher would supervise the interaction through a moderated classroom workflow. At the same time, school policies would restrict personal data sharing and enforce age-appropriate access and privacy safeguards. This example shows how the governance framework can operate as a practical combination of AI validation, human oversight, and policy-based protection.

As this study is conceptual rather than intervention-based, the following interpretations are intended to indicate plausible relationships and design implications rather than empirically verified effects.

To understand how these factors may interact, the analysis suggests that AI-generated misinformation (W1) could reinforce misinformation spread (T3), while gamified learning (O4) and simulation-based interventions (S1) may help moderate some of these risks. This approach is intended to provide a conceptual decision-support framework for educators and policymakers when considering possible interventions and their likely implications.

(1) Curriculum Design: Incorporate digital literacy, media awareness, and ethical AI usage into cyber awareness programs for students. Include activities that require critical engagement with AI outputs (e.g., evaluating ChatGPT-generated responses).
(2) Personalized Learning Support: Leverage ChatGPT's strength in providing individualized learning feedback, especially in underserved communities, while ensuring learners are guided to question and verify AI-generated content.
(3) Authentic and Formative Assessment: Move beyond traditional written exams and use portfolio-based assessments, peer review, and reflection logs to track learning that AI cannot fabricate easily.
(4) Gamification and Simulation: Use gamified approaches (O4) to promote engagement and reduce misinformation vulnerability (W1), especially through interactive simulations and scenario-based learning (S1).
(5) Continuous Teacher Training: Equip educators with skills to integrate AI tools like ChatGPT meaningfully, while also understanding its limitations and biases.
(6) Feedback Loops Monitoring: Monitor how misinformation (T3) and feedback systems (O6) may reinforce each other. Implement mechanisms to flag and break such loops early.
(7) Policy and Ethical Guidelines: Develop clear guidelines around ChatGPT's use with K-9 to K-12 learners, focusing on data privacy, bias, and regulatory compliance (e.g., GDPR K/COPPA).

Finally, while SWOT analysis helped frame the potential and risks, and the Fishbone diagram revealed deeper root causes. Together, they suggest that ChatGPT should not be banned or ignored; instead, it should be critically embraced with structured strategies that align with pedagogical goals and ethical safeguards. To effectively address the challenges identified, we propose integrating real-time fact-checking tools and gamified learning assessments into the ChatGPT framework. These strategies are proposed as possible ways to reduce the risks of misinformation and over-reliance on AI while potentially supporting student engagement and critical thinking. The integration of detection tools may improve the reliability of AI-generated content, while interactive, gamified assessments could offer more meaningful ways to evaluate students' understanding of cybersecurity concepts. These additions form part of the proposed governance framework, which emphasizes ethical AI deployment, teacher oversight, and continuous feedback loops to support safer and more scalable use of ChatGPT in K-9 to K-12 education.

VI. Ethical and Regulatory Compliance

The proposed governance framework for ChatGPT's integration into K-12 cybersecurity education is designed to comply with key regulatory frameworks such as COPPA, FERPA, and GDPR-K. The framework ensures that ethical considerations and data privacy are central to the deployment of ChatGPT in the classroom. Below, we explain how specific framework components align with these regulations and detail the compliance actions:

(1) Data Privacy and Student Consent (COPPA and FERPA)

- COPPA (Children's Online Privacy Protection Act) requires that online services directed at children under 13 obtain verifiable parental consent before collecting personal information. To comply, ChatGPT will be configured to limit data collection to the minimum necessary and ensure parental consent is obtained for students under 13 before they use the tool.
- FERPA (Family Educational Rights and Privacy Act) mandates that educational records are protected, and that parents and students have rights over their data. To align with FERPA, ChatGPT will not store personally identifiable information (PII) unless explicitly permitted, and students' interactions will be anonymized and deleted after each session.

(2) Data Handling and Security (GDPR-K)

- The GDPR-K (General Data Protection Regulation for Kids) extends data protection laws to children, ensuring that minors' personal data is handled with the highest level of security and transparency. Our framework ensures that ChatGPT's interactions with students are stored temporarily, anonymized, and fully compliant with data protection standards. Students and parents will be informed about the types of data collected, how it will be used, and the rights students have over their data, including the right to access, delete, and withdraw consent.
- To meet GDPR-K standards, we will also incorporate privacy by design in the development of ChatGPT, ensuring that privacy features (e.g., data anonymization, limited data retention, and encrypted storage) are integrated from the outset.

(3) Content Validation and Ethical AI (COPPA and FERPA)

- Given the potential for misinformation or AI

hallucinations in ChatGPT's responses, the framework includes real-time validation mechanisms to ensure content accuracy. This aligns with the ethical standards set forth by these regulations, as it aims to prevent the spread of harmful or misleading content, especially when minors are involved. Moreover, content will be reviewed regularly to ensure that AI-generated content does not violate privacy laws or expose sensitive data.

- Human oversight is an integral part of the framework. Teachers will be trained to moderate ChatGPT's outputs, ensuring that all interactions are safe and ethically sound, in line with COPPA's requirement for monitoring children's interactions with digital tools.

(4) Teacher-in-the-Loop Oversight (FERPA and GDPR-K)

- FERPA allows educational institutions to oversee and control how student data is used, and our framework explicitly integrates teacher oversight in every ChatGPT interaction. Teachers are responsible for moderating and providing contextual guidance, ensuring that students' privacy rights are respected while fostering a safe learning environment.
- Additionally, ChatGPT's response logging will be transparent, with teachers having the ability to review and delete data when necessary to comply with student privacy rights as per FERPA and GDPR-K.

VII. Conclusion

This study synthesizes the potential and risks of using ChatGPT to support cybersecurity awareness for K-9 to K-12 learners using a structured analysis (SWOT and fishbone) grounded in prompt-generated ChatGPT outputs and prior literature. Overall, the findings suggest that ChatGPT can support interactive and scalable learning support (e.g., explanations, practice questions, and scenario discussion), but these benefits must be balanced against risks such as hallucinations/misinformation, over-reliance, bias, inequitable access, and compliance concerns.

The findings suggest that ChatGPT has the potential to support interactive and scalable learning, providing explanations, practice questions, and scenario-based discussions. However, these conclusions are based on a conceptual framework and not on empirical testing. While the study outlines the conceptual feasibility of the framework, further research is necessary to examine these proposed benefits in real-world educational settings.

The analysis has several practical implications for real-world adoption. First, educators should treat ChatGPT as a guided support tool rather than an authority, using structured prompts, source-checking routines, and "teacher-in-the-loop" review for sensitive topics. Second, schools and administrators should implement governance measures such as age-appropriate access controls, clear acceptable-use policies, and basic monitoring/auditing practices, along with professional development to build teacher capacity. Third, curriculum designers should embed digital literacy and verification skills (evaluating credibility, identifying misinformation, and safe reporting pathways) directly into cyber awareness activities. Finally, policymakers and procurement teams should align deployment with child privacy and data protection requirements (e.g., COPPA/FERPA/GDPR-K) through vendor review, data-minimization practices, and transparency expectations.

However, the study is constrained by its reliance on simulated contexts and supplementary expert- and youth-informed design input rather than real-world classroom data in longitudinal form. This limits the generalizability and empirical robustness of the results. The governance framework should be examined in real-world educational settings to assess its practical applicability. Subsequent research should focus on large-scale empirical studies across diverse classrooms to explore longer-term effects on students' behavior and learning outcomes. Additionally, as AI technologies and regulatory frameworks continue to evolve, ongoing updates to policy and pedagogical approaches are essential to ensure the safe and effective integration of AI-enhanced cybersecurity education.

Future research should focus on specific study designs to empirically test the proposed framework in real-world educational settings. We recommend pilot trials to evaluate the immediate impact of ChatGPT-enhanced cybersecurity education on student engagement and learning outcomes. Longitudinal studies are also necessary to assess the long-term effects on cybersecurity knowledge and behavioral changes among students. Additionally, quasi-experimental designs could be used to compare ChatGPT-enabled learning environments with traditional methods, measuring engagement, knowledge retention, and critical thinking skills. These studies should involve diverse student populations across various educational contexts (e.g., rural vs. urban schools) and evaluate teacher and student feedback to refine the governance framework and ensure practical feasibility.

Conflict of Interest

The authors declare no conflicts of interest.

Author Contributions

Conceptualization, M.A.S.A.R. and G.H.; methodology, M.A.S.A.R. and G.H.; formal analysis, M.A.S.A.R.; investigation, M.A.S.A.R., G.H., and M.A.S.A.; resources, G.H. and M.A.S.A.; writing, original draft preparation, M.A.S.A.R.; writing, review and editing, M.A.S.A.R., G.H., M.A.S.A., and P.R.O.; visualization, M.A.S.A.R.; supervision, M.A.S.A. and P.R.O.; project administration, G.H. All authors had approved the final version.

Funding

This work is partially funded by the US Office of Naval Research, Award Number N000142312454 along with SCORE Lab at the University of North Texas for providing resources and research support.

Reference

[1] J. Wiredu, M. Kumi, and P. H. Ademola, "An investigation on the characteristics, abilities, constraints, and functions of Artificial Intelligence (AI): The age of ChatGPT as an essential," *Information and Management*, vol. 108, no. 3, pp. 62614–62620, 2023. doi: 10.37118/ijdr.26689.05.2023

[2] C. Gonzalez, "Building human-like artificial agents: A general cognitive algorithm for emulating human decision-making in dynamic environments," *Perspectives on Psychological Science*, vol. 19, no. 5, pp. 860–873, 2024. doi: 10.1177/17456916231196766

[3] P. Reddy, K. Ch, K. Sharma, B. Sharma, and S. Sharma, "Evolution of generative artificial intelligence: A review of the developed and developing," *Engineered Science*, vol. 35, 1529, 2025. doi: 10.30919/es1529

[4] K. I. Vorobyeva, S. Belous, N. V. Savchenko, L. M. Smirnova, S. A. Nikitina, and S. P. Zhdanov, "Personalized learning through AI: Pedagogical approaches and critical insights," *Contemporary Educational Technology*, vol. 17, no. 2, 2025.

[5] B. Quadir, K. Mostafa, J. C. Yang, J. Shen, and R. Akter, "ARCS approach to PTA-based programming language practice sessions: Factors influencing programming problem-solving skills," *Education and Information Technologies*, vol. 28, no. 10, pp. 13713–13735, 2023. doi: 10.1007/s10639-023-11740-6

[6] D. Patel, C. K. Sahu, and R. Rai, "Security in modern manufacturing systems: Integrating blockchain in artificial intelligence-assisted manufacturing," *International Journal of Production Research*, vol. 62, no. 3, pp. 1041–1071, 2024. doi: 10.1080/00207543.2023.2262050

[7] A. Rokaya, S. M. T. Islam, H. Zhang, L. Sun, M. Zhu, and L. Zhao, "Acceptance of chatbot based on emotional intelligence through machine learning algorithm," in *Proc. 2022 2nd Int. Conf. Frontiers of Electronics, Information and Computation Technologies (ICFEICT)*, Aug. 2022, pp. 610–616. doi: 10.1109/ICFEICT57213.2022.00111

[8] I. Naik, D. Naik, and N. Naik, "Chat generative pre-trained transformer (ChatGPT): Comprehending its operational structure, AI techniques, working, features and limitations," in *Proc. 2023 IEEE Int. Conf. ICT in Business Industry & Government (ICTBIG)*, Dec. 2023, pp. 1–9. doi: 10.1109/ICTBIG59752.2023.10456201

[9] S. Singh, S. Bansal, A. E. Saddik, and M. Saini, "From ChatGPT to DeepSeek AI: A comprehensive analysis of evolution, deviation, and future implications in AI-language models," arXiv preprint, arXiv:2504.03219, 2025, doi: 10.48550/arXiv.2504.03219

[10] D. Gong, X. Wan, and D. Wang, "Working memory capacity of ChatGPT: An empirical study," in *Proc. AAAI Conf. Artificial Intelligence*, vol. 38, no. 9, Mar. 2024, pp. 10048–10056. doi: 10.1609/aaai.v38i9.28868

[11] OpenAI. (2024). Introducing deep research. [Online]. Available: https://openai.com/index/introducing-deep-research/

[12] O. V. Johnson, O. M. Alyasiri, D. A. Akhtom, and O. E. Johnson, "Image analysis through the lens of ChatGPT-4," *Journal of Applied Artificial Intelligence*, vol. 4, no. 2, pp. 31–46, 2023. doi: 10.48185/jaai.v4i2.870

[13] C. I. Font Julián, E. Orduña Malea, and L. Codina, "ChatGPT Search as a tool for scholarly tasks: Evolution or devolution?" *Infonomy*, vol. 2, no. 5, 2024. doi: 10.3145/infonomy.24.059

[14] I. Seth, B. Lim, J. Cevik, F. Sofiadellis, R. J. Ross, R. Cuomo, and W. M. Rozen, "Utilizing GPT-4 and generative artificial intelligence platforms for surgical education: An experimental study on skin ulcers," *European Journal of Plastic Surgery*, vol. 47, no. 1, 19, 2024. doi: 10.1007/s00238-024-02162-9

[15] J. E. Seaman and J. Seaman, "Conflicted digital adoption: Educational resources in US K-12 education, 2024," *Bay View Analytics*, 2024.

[16] Y. Tekeci, B. Torpil, and O. Altuntaş, "The impact of screen exposure on screen addiction and sensory processing in typically developing children aged 6–10 years," *Children*, vol. 11, no. 4, 464, 2024. doi: 10.3390/children11040464

[17] W. Chen, Y. He, X. Tian, and W. He, "Exploring cybersecurity education at the K-12 level," in *Proc. SITE Interactive Conf.*, Oct. 2021, pp. 108–114.

[18] Center for Internet Security (CIS). (2025). 2025 CIS MS-ISAC K-12 cybersecurity report: Where education meets community resilience. [Online]. Available: https://www.cisecurity.org/insights/white-papers/2025-k12-cybersecurity-report

[19] I. Alkaher, D. Goldman, and I. Aram, "An environmental and sustainability education center in Israel as a 'street-level policy entrepreneur' for promoting teachers as change agents for sustainability," *Environmental Education Research*, vol. 30, no. 10, pp. 1684–1709, 2024. doi: 10.1080/13504622.2024.2335612

[20] A. Brem, F. Giones, and M. Werle, "The AI digital revolution in innovation: A conceptual framework of artificial intelligence technologies for the management of innovation," *IEEE Transactions on Engineering Management*, vol. 70, no. 2, pp. 770–776, 2021. doi: 10.1109/TEM.2021.3109983

[21] E. Kasneci *et al.*, "ChatGPT for good? On opportunities and challenges of large language models for education," *Learning and Individual Differences*, vol. 103, 102274, 2023. doi: 10.1016/j.lindif.2023.102274

[22] A. Alfarwan, "Generative AI use in K-12 education: A systematic review," *Frontiers in Education*, vol. 10, 1647573, Sep. 2025. doi: 10.3389/feduc.2025.1647573

[23] G. Childers, C. L. Linsky, B. Payne, J. Byers, and D. Baker, "K-12 educators' self-confidence in designing and implementing cybersecurity lessons," *Computers and Education Open*, vol. 4, 100119, 2023. doi: 10.1016/j.caeo.2022.100119

[24] K. K. Nwabueze *et al.*, "Exploring the prevalence and risk factors of adolescent mental health issues in the COVID and post-COVID era in the UK: A systematic review," *EXCLI Journal*, vol. 24, 508, 2025. doi: 10.17179/excli2025-8325

[25] R. Vinay, G. Spitale, N. Biller-Andorno, and F. Germani, "Emotional prompting amplifies disinformation generation in AI large language models," *Frontiers in Artificial Intelligence*, vol. 8, 1543603, 2025. doi: 10.3389/frai.2025.1543603

[26] M. Peng, N. Chen, J. Tang, and J. Li, "How does misinformation affect large language model behaviors and preferences?" arXiv preprint, arXiv:2505.21608, 2025. doi: 10.18653/v1/2025.acl-long.674

[27] M. D. Kakhki, A. Oguz, and M. Gendron, "Exploring the affordances of chatbots in higher education: A framework for understanding and utilizing ChatGPT," *Journal of Information Systems Education*, vol. 35, no. 3, pp. 284–302, 2024.

[28] M. H. M. Hamadaqa, M. Alnajjar, M. N. Ayyad, M. A. Al-Nakhal, B. S. Abunasser, and S. S. Abu-Naser, "Leveraging artificial intelligence for strategic business decision-making: Opportunities and challenges," *International Journal of Academic Information Systems Research (IJAISR)*, vol. 8, issue 8, pp. 16–23 2024.

[29] E. M. Lim, "Metaphor analysis on pre-service early childhood teachers' conception of Artificial Intelligence (AI) education for young children," *Thinking Skills and Creativity*, vol. 51, 101455, 2024. doi: 10.1016/j.tsc.2023.101455

[30] N. Moroianu, S. E. Iacob, and A. Constantin, "Artificial intelligence in education: A systematic review," *Geopolitical Perspectives and Technological Challenges for Sustainable Growth in the 21st Century*, pp. 906–921, 2023. doi: 10.2478/9788367405546-084

[31] C. Merino-Campos, "The impact of artificial intelligence on personalized learning in higher education: A systematic review," *Trends in Higher Education*, vol. 4, no. 2, 17, 2025. doi: 10.3390/higheredu4020017

[32] N. F. Davar, M. A. A. Dewan, and X. Zhang, "AI chatbots in education: Challenges and opportunities," *Information*, vol. 16, no. 3, 235, 2025. doi: 10.3390/info16030235

[33] J. Wang and W. Fan, "The effect of ChatGPT on students' learning performance, learning perception, and higher-order thinking: Insights from a meta-analysis," *Humanities and Social Sciences Communications*, vol. 12, no. 1, pp. 1–21, 2025. doi: 10.1057/s41599-025-04787-y

[34] R. Arum, M. Calderon Leon, X. Li, and J. Lopes, "ChatGPT early adoption in higher education: Variation in student usage, instructional support, and educational equity," *AERA Open*, vol. 11, 23328584251331956, 2025. doi: 10.1177/2332858425133195

[35] J. Dempere, K. Modugu, A. Hesham, and L. K. Ramasamy, "The impact of ChatGPT on higher education," *Frontiers in Education*, vol. 8, 1206936, Sep. 2023. doi: 10.3389/feduc.2023.1206936

[36] T. Fütterer, C. Fischer, A. Alekseeva, X. Chen, T. Tate, M. Warschauer, and P. Gerjets, "ChatGPT in education: Global reactions to AI innovations," *Scientific Reports*, vol. 13, no. 1, 15310, 2023. doi: 10.1038/s41598-023-42227-6

[37] H. B. Essel, D. Vlachopoulos, A. B. Essuman, and J. O. Amankwa, "ChatGPT effects on cognitive skills of undergraduate students: Receiving instant responses from AI-based conversational Large Language Models (LLMs)," *Computers and Education: Artificial Intelligence*, vol. 6, 100198, 2024. doi: 10.1016/j.caeai.2023.100198

[38] A. Gasaymeh, A. A. Abu Qbeita, R. AlMohtadi, and M. Beirat, "Exploring education students' use of ChatGPT for academic and personal purposes: Insights from a developing country context," *Frontiers in Education*, vol. 10, 1580310, May 2025. doi: 10.3389/feduc.2025.1580310

[39] M. E. Jucunda, "ChatGPT in education: Boon or bane?" *Journal of Information Technology Teaching Cases*, 2025. doi: 10.1177/20438869251326278

[40] S. Patwary, *Leadership and Crisis Communication in Cybersecurity: Enhancing the Contingency Plan for a Data Breach Scenario*, 2025.

[41] M. S. Amin, S. Kim, M. A. S. A. Rishat, Z. Tang, and H. Ahn, "A systematic literature review of privacy information disclosure in AI-integrated Internet of Things (IoT) technologies," *Sustainability*, vol. 17, no. 1, 8, 2024. doi: 10.3390/su17010008

[42] M. H. M. Altarawneh, A. Althunibat, M. H. Almajali, N. Alzriqat, and S. Alazzam, "Cybersecurity awareness among school students: Exploring influencing factors, legal implications, and knowledge gaps," *International Journal of Innovative Research and Scientific Studies*, vol. 8, no. 1, pp. 1516–1529, 2025.

[43] I. U. Idierukevbe and A. Addo, "Bridging the cybersecurity skills gap: A gamification model," *Journal of Business Studies Quarterly*, vol. 14, no. 1, pp. 1–16, 2024.
[44] D. Huitema and A. Wong, "A case study in gamification for a cybersecurity education program: A game for cryptography," arXiv preprint, arXiv:2502.06706, 2025. doi: 10.48550/arXiv.2502.06706
[45] M. Farrokhnia, S. K. Banihashem, O. Noroozi, and A. Wals, "A SWOT analysis of ChatGPT: Implications for educational practice and research," *Innovations in Education and Teaching International*, vol. 61, no. 3, pp. 460–474, 2024. doi: 10.1080/14703297.2023.2195846
[46] M. Taktak, M. S. Bellibas, and M. Özgenel, "Use of ChatGPT in education: Future strategic road map with SWOT analysis," *Educational Process: International Journal*, vol. 13, no. 3, pp. 7–21, 2024.
[47] G. Wagner and L. Thurner, "Teaching tip: Rethinking how we teach Git: Pedagogical recommendations and practical strategies for the information systems curriculum," *Journal of Information Systems Education*, vol. 36, no. 1, pp. 1–12, 2025. doi: 10.62273/BTKM5634
[48] D. W. Piandani et al., "Analysis of strength, weakness, opportunities, and threats in planning to improve the quality of education at SDN 003 Teluk Bayur, Berau Regency," *Journal of Education and Sociology*, vol. 4, no. 4, pp. 7–14, 2025.
[49] T. Luo, C. Wu, and L. Duan, "Fishbone diagram and risk matrix analysis method and its application in safety assessment of a natural gas spherical tank," *Journal of Cleaner Production*, vol. 174, pp. 296–304, 2018. doi: 10.1016/j.jclepro.2017.10.334
[50] D. D. Shinde, S. Ahirrao, and R. Prasad, "Fishbone diagram: Application to identify the root causes of student-staff problems in technical education," *Wireless Personal Communications*, vol. 100, pp. 653–664, 2018. doi: 10.1007/s11277-018-5344-y
[51] M. Farrokhnia, S. K. Banihashem, O. Noroozi, and A. Wals, "A SWOT analysis of ChatGPT: Implications for educational practice and research," *Innovations in Education and Teaching International*, vol. 61, no. 3, pp. 460–474, 2024. doi: 10.1080/14703297.2023.2195846
[52] M. Mas'adi, A. A. Priyanto, and A. Nurhadi, "SWOT analysis as a basis for determining waste processing strategies at TPSTs throughout Pamulang District, South Tangerang," *Scientific Journal of Management, Economics, & Accounting (MEA)*, vol. 4, no. 3, pp. 715–727, 2020. (in Indonesian)
[53] M. Arda, D. Andriany, and Y. H. Manurung, "Analisis SWOT dalam menentukan strategi pengelolaan sampah rumah tangga Kota Medan," in *Proc. Konferensi Nasional Ekonomi Manajemen dan Akuntansi (*KNEMA*)*, vol. 1, no. 1, 2020.
[54] F. Mujayyin, D. A. Gunarso, and N. D. Mukhsinin, "Analysis of the reliability of landfill waste processing technology into Refuse Derived Fuels (RDF) using the six sigma DMAIC approach," *Applied Mechanics Journal*, vol. 1, no. 2, pp. 133–141, 2020. doi: 10.32722/jmt.v1i2.3360
[55] Y. H. Cheah, J. Lu, and J. Kim, "Integrating generative artificial intelligence in K-12 education: Examining teachers' preparedness, practices, and barriers," *Computers and Education: Artificial Intelligence*, vol. 8, 100363, 2025 doi: 10.1016/j.caeai.2025.100363