Using AI Assistants in the Creation of an Academic Program of Study (PoS) in CyberAI

PAIGE ZALEPPA, SIDDHARTH KAZA, AND BLAIR TAYLOR

This project is partially funded by the National Science Foundation through the CyberCorps program DGE#1663184 at Towson University.

AGENDA

- Background
- Research Questions
- Methodology and System Design
- Observations
- Final Knowledge Units

BACKGROUND

- Artificial Intelligence (AI) is increasingly taking on many critical roles necessary to secure modern computing systems
- 2022 CHIPS and Science Act has required the National Science Foundation (NSF) to determine the workforce needs of the US Government and determine the feasibility of a Scholarship Program for students in AI programs at 2- and 4-year colleges/universities [19]
- Has brought up the following question:
  - What AI topics should be taught within cybersecurity programs?

CYBERAI PROGRAM OF STUDY (PoS)

- In February 2024, the National Security Agency (NSA) National Centers of Academic Excellence in Cybersecurity (NCAE-C) program in collaboration with the National Science Foundation (NSF), launched an initiative to outline the AI content cybersecurity academic programs need to teach their students.

- PoS Development:
  - Collaborative process between educators, government entities, and industry representatives
  - Labor-intensive and iterative process that can take years
- CyberAI PoS Challenges:
  - Timeline was ~6 months
  - The field of AI is evolving as quickly as the PoS was being developed

NCAE-C PROGRAM OF STUDY

- A PoS is a series of courses and experiences that students can realistically complete while working towards a degree or certificate [16]
- Academic institutions document their fulfillment of requirements for a PoS through the process of Knowledge Unit (KU) alignment
  - A KU is a thematic grouping of learning outcomes and topics
- Alignment is a continuous process that must be completed every 5 years [18]

Knowledge Unit Template

Title

The intent of this KU is to provide students …..

KU Learning Outcomes

Students will be able to:
1.
2.
3.

Topics
1.
2.
3.

Notes/Prerequisites
Special instructions or explanations

AI ASSISTANTS

- AI has become more accessible due to the development of user-friendly interfaces like chatbots
  - These interfaces provide opportunities for both non-technical users and technical experts to save time by building LLM-based solutions for everyday tasks [3]
- AI Assistants are software systems that use AI models to respond to human inquiries
  - Example: ChatGPT, which uses the a specific GPT model version to respond to user queries [7]
- Democratization of AI allows people of all technical abilities to leverage AI for unique tasks that were previously unattainable [3]

RESEARCH QUESTIONS

- **RQ1**: How can AI assist in the development of the guidelines for academic programs of study?

- **RQ2**: What attributes of a knowledge unit and a program of study can an AI effectively contribute to?

METHODOLOGY

CYBERAI KU DEVELOPMENT

- Six-month collaborative effort involving:
  - In-person and virtual workshops
  - Asynchronous feedback mechanisms
- 235 participants from education, government, and industry contributed to the final document
- Iterative process using a series of evolving documents:
  - Initial drafts called "Strawman"
  - Final version called "Stoneman"

Iteration	Publication Date	AI Assistant
Strawman 1	May 14, 2024	None (human creation only)
Strawman 2	July 11, 2024	Custom GPT
Strawman 3	July 19, 2024	Custom GPT
Strawman 4	July 22, 2024	None
Strawman 5	July 23, 2024	None
Strawman 6	July 23, 2024	None
Stoneman	August 29, 2024	Custom GPT

AI Assistants were utilized in several iterations to refine the KUs

HUMAN KU CREATION PROCESS

- All PoS within the NCAE-C Community consist of KUs that share the same structure
  - Title
  - Description
  - Learning Outcomes
    - Built using Bloom's Taxonomy [17]
  - Topics
    - Areas the learning outcomes will cover and intentionally left broad to allow for variation among schools [18]
  - Notes
    - Any additional information needed for succsessful alignment

Knowledge Unit Template

Title

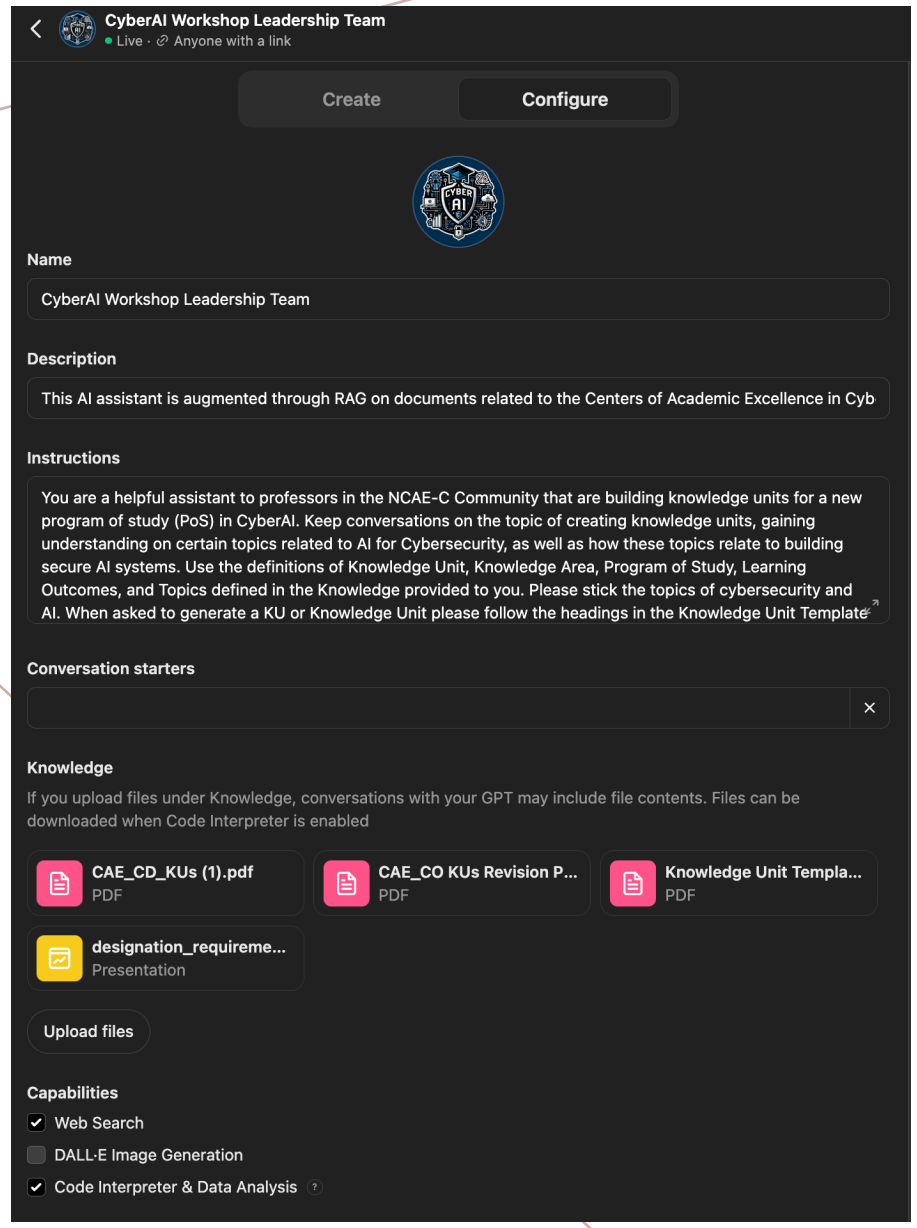
The intent of this KU is to provide students …..

KU Learning Outcomes

Students will be able to:
1.
2.
3.

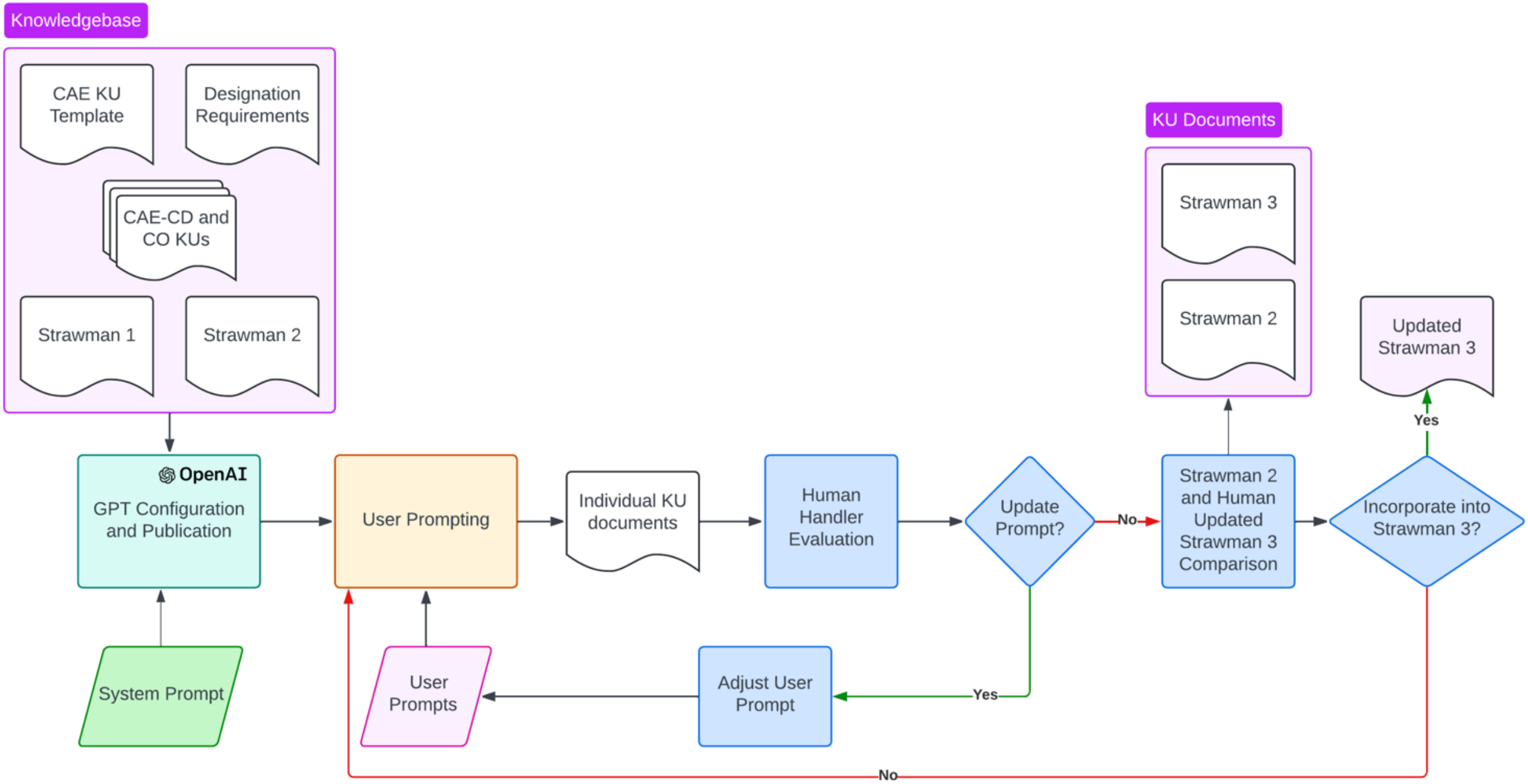
Topics
1.
2.
3.

Notes/Prerequisites
Special instructions or explanations



METHODOLOGY: AI ASSISTANT CREATION

- GPTs are tailored versions of ChatGPT that do not require in-depth machine learning or programming skills to finetune for a specific task [13]. Can be given additional abilities such as:
  - Search the web
  - Generate images
  - Use a specific uploaded knowledgebase of documents
  - Following a system instruction


Knowledgebase
CAE KU Template
Designation Requirements
CAE-CD and CO KUs
Strawman 1
Strawman 2
OpenAI
GPT Configuration and Publication
System Prompt
User Prompting
User Prompts
Individual KU documents
Human Handler Evaluation
Update Prompt?
Yes
Adjust User Prompt
No
KU Documents
Strawman 3
Strawman 2
Strawman 2 and Human Updated Strawman 3 Comparison
Incorporate into Strawman 3?
Yes
Updated Strawman 3
No

AI ASSISTANT CREATION: SYSTEM PROMPT

You are a helpful assistant to professors in the NCAE-C Community that are building knowledge units for a new program of study (PoS) in AI for Cybersecurity and Security of AI. Keep all conversations on the topic of creating knowledge units, gaining understanding on certain topics related to either AI for Cybersecurity or Security of AI. Use the definitions of Knowledge Unit, Knowledge Area, Program of Study, Learning Outcomes, and Topics defined in the documents provided to you in your Knowledge. When asked to generate a KU or Knowledge Unit please follow the headings in the Knowledge Unit Template provided in the documents. A single knowledge unit should not be larger or more complicated than what could reasonably be taught during a 15-week college semester. The Strawman 2 document provided in your knowledge is what human participants have generated for a list of Knowledge units for a program of study in AI for Cybersecurity and Security of AI. Strawman 1 is a previous version of this document and provided to you as a reference. If asked to provide input on the KUs in that document, always indicate the changes or suggestions you are making in your response.

AI ASSISTANT CREATION: KNOWLEDGEBASE

NCAE-CO KUs

NCAE-CD KUs

Designation Requirements

Knowledge Unit Template

Strawman 1

Strawman 2

AI ASSISTANT CREATION: USER PROMPT

For the {{ name }} KU in the Strawman 2 document make adjustments to the outcomes and topics list in order to make it easier for a professor trying to align the content taught in their courses to the knowledge unit. Adjustments can include additions or subtractions to either list, reordering learning outcomes to be in an order that reflects verbs in Blooms taxonomy taxons, combining topics into a single topic, breaking out topics into multiple topics, or adjusting words to better articulate the outcome or topic.

AI ASSISTANT OUTPUT

- Output was reviewed by a human evaluator for potential inclusion
  - Decided if AI suggestions were selected for inclusion in the final document
- Areas where the Assistant was helpful:
  - Learning Outcomes
  - Reducing list of topics
  - Descriptions
- Areas where the Assistant was not helpful:
  - Title
  - Notes
  - Adding additional topics

AI ASSISTANT OUTPUT EXAMPLE

- AI Algorithms KU: Strawman 2 Version
- AI Algorithms KU: AI Assistant Updated Version

OBSERVATIONS

- Human authors viewed the AI Assistant as a beneficial addition to the process
  - Humans reviewed AI suggestions in a similar way to a human
- Benefits:
  - Increased diversity of Bloom's taxonomy verbs for learning outcomes
  - Generated uniform and descriptive KU descriptions
  - Encouraged human review of descriptions and learning outcomes
- Limitations:
  - Limited ability to expand on topics in KUs
  - Minimal impact on notes
  - Unable to assist in expanding topics

FINAL KUS (20)

- Cybersecurity Fundamentals
- IT Systems Components
- Basic Scripting and Programming
- Math Fundamentals
- Computer Science Fundamentals
- AI Governance, Laws, and Ethics *
- AI Fundamentals *
- Basic Networking
- Advanced Math for AI
- Network Defense
- Deep Learning *
- Machine Learning Fundamentals *
- Model Selection, Evaluation, and Specification *
- Securing the AI Lifecycle*
- Risk Management of AI *
- Adversarial Learning *
- AI for Security Assessments *
- Defensive Applications of AI *
- Offensive Applications of AI *
- Machine Learning Algorithms *

*AI Assistance

QUESTIONS?

REFERENCES

[1] N. N. Y. Vo, Q. T. Vu, N. H. Vu, T. A. Vu, B. D. Mach, and G. Xu, "Domain-specific NLP system to support learning path and curriculum design at tech universities," *Computers and Education: Artificial Intelligence*, vol. 3, p. 100042, 2022. DOI: 10.1016/j.caeai.2021.100042.

[2] S. Grassini, "Shaping the future of education: Exploring the potential and consequences of AI and ChatGPT in educational settings," *Education Sciences*, vol. 13, no. 7, p. 692, 2023, doi: 10.3390/educsci13070692.

[3] A. Przegalińska, "Collaborative artificial intelligence: The example of virtual assistants and conversational AI," in *Artificial Intelligence (AI) as a Megatrend Shaping Education: How to Prepare for the Socio-Economic Opportunities and Challenges Presented by Artificial Intelligence?*, pp. 13-23, 2022. [Online]. Available: https://kwalifikacje.gov.pl/images/Publikacje/Artificial-Intelligence_AI_as-a-Megatrend-Shaping-Education.pdf.

[4] J. H. Klemmer, S. A. Horstmann, N. Patnaik, C. Ludden, C. Burton Jr, C. Powers, F. Massacci, A. Rahman, D. Votipka, H. R. Lipford, A. Rashid, A. Naiakshina, and S. Fahl, "Using AI assistants in software development: A qualitative study on security practices and concerns," *arXiv*, 2024. DOI: 10.48550/arXiv.2405.06371.

[5] A. Padovano and M. Cardamone, "Towards human-AI collaboration in the competency-based curriculum development process: The case of industrial engineering and management education," *Computers and Education: Artificial Intelligence*, vol. 7, 2024. DOI: 10.1016/j.caeai.2024.100256.

[6] J. W. Ayers, A. Poliak, M. Dredze, E. C. Leas, Z. Zhu, J. B. Kelley, D. J. Faix, A. M. Goodman, C. A. Longhurst, M. Hogarth, and D. M. Smith, "Comparing Physician and Artificial Intelligence Chatbot Responses to Patient Questions Posted to a Public Social Media Forum," *JAMA Internal Medicine*, vol. 183, no. 6, pp. 589-596, 2023. 10.1001/jamainternmed.2023.1838.

[7] J. Rudolph, S. Tan, and S. Tan, "ChatGPT: Bullshit spewer or the end of traditional assessments in higher education?," *Journal of Applied Learning and Teaching*, vol. 6, no. 1, pp. 342-263, 2023. DOI: 10.37074/jalt.2023.6.1.9.

[8] T. Baker, L. Smith, and N. Anissa, *Educ-AI-tion Rebooted? Exploring the Future of Artificial Intelligence in Schools and Colleges*, Nesta, 2019. [Online]. Available: https://media.nesta.org.uk/documents/Future_of_AI_and_education_v5_WEB.pdf.

[9] O. Almatrafi, "Assessing ChatGPT's capability to generate course learning outcomes," in *Proceedings of the 7th International Conference on Information and Computer Technologies (ICICT)*, pp. 527-531, 2024. DOI: 10.1109/ICICT62343.2024.00092.

[10] E. Kasneci, K. Sessler, S. Küchemann, M. Bannert, D. Dementieva, F. Fischer, U. Gasser, G. Groh, S. Günnemann, E. Hüllermeier, S. Krusche, G. Kutyniok, T. Michaeli, C. Nerdel, J. Pfeffer, O. Poquet, M. Sailer, A. Schmidt, T. Seidel, M. Stadler, J. Weller, J. Kuhn, and G. Kasneci, "ChatGPT for good? On opportunities and challenges of large language models for education," *Learning and Individual Differences*, vol. 103, 2023. DOI: 10.1016/j.lindif.2023.102274.

[11] P. Denny, H. Khosravi, A. Hellas, J. Leinonen, and S. Sarsa, "Can we trust AI-generated educational content? Comparative analysis of human and AI-generated learning resources," *arXiv*, 2023. DOI: 10.48550/arXiv.2306.10509.

[12] P. Sridhar, A. Doyle, A. Agarwal, C. Bogart, J. Savelka, and M. Sakr, "Harnessing LLMs in curricular design: Using GPT-4 to support authoring of learning objectives," in *Proceedings of the Workshop on Empowering Education with LLMs—the Next-Gen Interface and Content Generation at AIED 2023*, 2023. DOI: 10.48550/arXiv.2306.17459.

[13] OpenAI, "Introducing GPTs," OpenAI, [Online]. Available: https://openai.com/index/introducing-gpts/. [Accessed: Aug. 31, 2024].

REFERENCES

[14] P. Lewis, E. Perez, A. Piktus, F. Petroni, V. Karpukhin, N. Goyal, H. Küttler, M. Lewis, W. Yih, T. Rocktäschel, S. Riedel, and D. Kiela, "Retrieval-augmented generation for knowledge-intensive NLP tasks," in *Proceedings of the 34th Conference on Neural Information Processing Systems (NeurIPS 2020)*, 2020. DOI: 10.48550/arXiv.2005.11401.

[15] X. Wang, Z. Wang, X. Gao, F. Zhang, Y. Wu, Z. Xu, T. Shi, Z. Wang, S. Li, Q. Qian, R. Yin, C. Lv, X. Zheng, and X. Huang, "Searching for Best Practices in Retrieval-Augmented Generation," arXiv preprint arXiv:2407.01219, 2024. [Online]. Available: https://arxiv.org/abs/2407.01219.

[16] National Security Agency, "Centers of Academic Excellence," National Security Agency, [Online]. Available: https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/. [Accessed: 31-Aug-2024].

[17] D. R. Krathwohl, A revision of bloom's taxonomy: An overview, Theory into practice 41 (2002) 212–218.

[18] "CAE-CD designation requirements," *Cyber.mil*, [Online]. Available: https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_designation_requirements.pdf. [Accessed: 31-Aug-2024].

[19] "CHIPS and Science Act of 2022," *National Science Foundation*, [Online]. Available: https://new.nsf.gov/chips. [Accessed: 7-Sep-2024].