CyberHusky: Empowering the Next Generation through AI Learning and Exploration

Dr. Yu Cai, Michigan Technological University

Dr. Yu Cai is a professor of cybersecurity in the College of Computing at Michigan Tech, where he also serves as the associate dean and the associate director of the Institute of Computing and Cybersystems (ICC). Additionally, Dr. Cai is the Director of the Computing Education Center, which is part of the ICC.

Dr. Cai's research interests include cybersecurity, computer networks, and computing education. He has been the lead PI on multi-million dollar external grants, with funding from sources such as the National Science Foundation (NSF), National Security Agency (NSA), and the State of Michigan. He is dedicated to applying his research to real-world challenges that positively impact society. Dr. Cai has also served as a consultant for companies like IBM and Ford, and he plays an active role as an ABET program evaluator for computing accreditation.

Aston Purdom, Michigan Technological University

CyberHusky: Empowering the Next Generation through AI Learning and Exploration

Abstract:

The rapid advancement of artificial intelligence (AI) has created both opportunities and challenges for K–12 education. Preparing the next generation of learners to understand and apply AI technologies is essential for building a diverse and inclusive AI workforce. This paper presents Michigan Technological University's CyberHusky initiative, an innovative AI training and outreach program designed for high school students. Through hands-on workshops, competitions, and community engagement events, CyberHusky introduces participants to core AI concepts, such as machine learning, data science, and ethical use of AI. The program emphasizes active learning, project-based exploration, and real-world problem solving, helping students develop not only technical skills but also critical thinking and teamwork.

The CyberHusky program integrates accessible, cloud-based AI coding platforms and open-source tools to make advanced concepts approachable for beginners. Evaluation results indicate that participants demonstrate noticeable gains in AI literacy, self-efficacy, and interest in computing-related careers. This paper describes the curriculum design, instructional strategies, and assessment results of the CyberHusky AI training program, highlighting its potential as a scalable model for K–12 AI education that bridges the gap between cybersecurity, artificial intelligence, and community engagement.

1. Introduction

Artificial intelligence (AI) is rapidly reshaping nearly every sector of society, including K-12 education, healthcare, transportation, manufacturing, finance, and national security. As AI systems increasingly influence everyday life, there is a growing consensus that AI literacy should begin well before postsecondary education. However, most K–12 students have limited exposure to AI concepts, and when exposure does exist, it is often fragmented, theoretical, or inaccessible to students without prior computing experience.

At the same time, concerns persist regarding equity and access in AI education. Students from rural, underrepresented, or economically disadvantaged communities often lack opportunities to engage with emerging technologies, contributing to persistent disparities in computing participation and workforce representation. Addressing these challenges requires educational models that are accessible, engaging, and grounded in real-world relevance.

In response, Michigan Technological University developed *CyberHusky*, an outreach initiative designed to introduce high school students to AI through experiential learning, cybersecurity-inspired challenges, and community engagement. Building on the university's longstanding K–12 cybersecurity outreach efforts, CyberHusky expands the scope to include AI coding, data-driven reasoning, and ethical considerations of intelligent systems. Rather than treating AI as an abstract concept, the program emphasizes learning by doing, encouraging students to explore, experiment, and collaborate on meaningful projects.

This paper documents the design, implementation, and evaluation of the CyberHusky AI program. The primary research questions guiding this work are:

1. How can AI concepts be introduced effectively to high school students with diverse backgrounds and limited prior experience?
2. What instructional strategies support student engagement, confidence, and persistence in AI learning?
3. To what extent does participation in CyberHusky influence students' AI literacy, self-efficacy, and interest in computing careers?

2. Background and Related Work

2.1 AI Education in K–12

Recent years have seen increased interest in integrating AI into K–12 education [1, 2, 3]. National and international initiatives emphasize the importance of AI literacy, ethical awareness, and computational thinking as essential skills for the future workforce. Prior research [8, 9] suggests that early exposure to computing and AI positively influences students' academic trajectories and career aspirations, particularly when learning experiences are hands-on and contextualized.

Despite these efforts, significant challenges remain [10, 11]. Many AI curricula presume prior programming backgrounds, which limits accessibility for beginners. Conversely, AI curricula designed for students without a computing background often introduce only surface-level concepts, resulting in limited learning gains. Additionally, teacher preparation and resource constraints often hinder sustained implementation in K–12 settings. These limitations highlight the need for outreach-based models that supplement formal schooling and provide authentic learning experiences.

2.2 Project-Based and Experiential Learning

Project-based learning (PBL) and experiential learning [4, 6, 7] have been widely shown to improve student engagement, conceptual understanding, and problem-solving skills in STEM education. PBL is particularly well suited for AI education, as it allows learners to experiment with data, algorithms, and models in realistic contexts. Experiential learning approaches also support teamwork, communication, and reflection, skills critical for both academic success and workforce readiness.

2.3 Cybersecurity as a Gateway to AI

Cybersecurity education [5] has long leveraged competition-based and challenge-driven learning to engage students. Many cybersecurity concepts, such as anomaly detection, pattern recognition, and risk analysis, naturally align with AI and machine learning techniques. CyberHusky intentionally builds on this alignment, using cybersecurity-inspired scenarios to introduce AI concepts in ways that are concrete and motivating for students.

3. Program Overview: The CyberHusky Initiative

CyberHusky is a university-led outreach program designed to engage high school students in computing, cybersecurity, and AI learning. The program serves students from local and regional schools, with an emphasis on inclusivity and community partnership.

3.1 Program Goals

The primary goals of CyberHusky are to:

- Increase AI literacy among high school students
- Build confidence and self-efficacy in computing and coding
- Foster interest in AI- and cybersecurity-related careers
- Promote ethical awareness and responsible use of AI
- Strengthen connections between the university, K–12 schools, and the local community

3.2 Target Audience and Participation

CyberHusky primarily targets students in grades 8–12. Participants come from diverse academic backgrounds, including students with little or no prior programming experience. The program is offered through workshops, after-school sessions, summer activities, and competition-based events.

3.3 Learning Environment and Tools

To reduce technical barriers, CyberHusky uses cloud-based AI coding platforms and browser-accessible development environments. These platforms include ChatGPT, Replit, Immersivelabs, and Google Colab. These platforms allow students to focus on concepts and experimentation without the need for complex software installation. Open-source datasets and tools are used whenever possible to promote transparency and reproducibility.

3.4 Funding Support

CyberHusky has been supported through a combination of internal institutional resources and externally funded computing education initiatives that collectively enable its sustained operation and growth. Primary support has come from the university's computing education center resources, which have provided base funding for materials, student mentors, and local program coordination. In addition, elements of CyberHusky activities have been aligned with broader research efforts in cybersecurity and AI education, allowing limited use of external project funds to support curriculum development, evaluation activities, and student engagement when consistent with sponsor guidelines. This blended funding model has allowed CyberHusky to operate as a low-cost, high-impact outreach program while maintaining flexibility to expand through future external grants and partnerships with regional schools and community organizations.

4. Curriculum Design and Instructional Strategies

4.1 Curriculum Structure

The CyberHusky AI curriculum is modular and flexible, allowing it to be adapted for different timeframes and student experience levels. Core modules include:

1. **Introduction to AI and Data** – What is AI? How do machines learn from data?
2. **Machine Learning Fundamentals** – Supervised learning, classification, and basic model evaluation
3. **AI Coding and Exploration** – Hands-on coding using cloud-based notebooks
4. **AI in Cybersecurity** – Applying AI to detect anomalies and security threats
5. **Ethical and Societal Impacts of AI** – Bias, privacy, and responsible AI use
6. **Capstone Projects and Competitions** – Team-based problem solving and presentation

4.2 Pedagogical Approach

CyberHusky adopts an active learning and project-based pedagogy. Instruction emphasizes short concept introductions followed by guided exploration and hands-on practice. Students work in small teams, encouraging peer learning and collaboration.

Mentorship plays a critical role in the program. University faculty, graduate students, and trained undergraduate mentors provide guidance, model problem-solving strategies, and support student learning without taking over the work.

4.3 Community and Competition Elements

Competitions and showcase events are integrated into the program to provide motivation and a sense of accomplishment. These events emphasize learning and teamwork rather than solely ranking, reinforcing a growth-oriented learning culture.

There are several targeted competition-based events integrated into the CyberHusky program, including the Presidential AI Challenge held each January, the Congressional App Challenge in October, the CyberPatriot competition in the fall, and the National Cyber League (NCL) competition in the spring. Participation in these competitions provides students with authentic, real-world learning experiences that extend beyond traditional classroom instruction. Through competition preparation and participation, students apply AI, cybersecurity, and computing concepts to open-ended, practice-driven problems, reinforcing technical knowledge while developing critical skills such as problem solving, teamwork, communication, and time management.

These competitions also expose students to nationally recognized benchmarks and professional standards, helping them understand how their skills compare within a broader peer community. In addition, the competitive yet collaborative environment fosters motivation, persistence, and confidence, particularly for students who may be new to computing or lack prior exposure to advanced technical topics. Collectively, these competition experiences play a key role in connecting learning with real-world impact, strengthening students' interest in computing-related pathways, and preparing them for future academic and career opportunities in AI and cybersecurity.

5. Evaluation Results and Team Achievement

5.1 Survey Design and Participants

To evaluate the educational and motivational impact of the CyberHusky program, an assessment survey was administered at the conclusion of the 2025 program cycle. A total of 12 student participants completed the survey. The instrument consisted of Likert-scale items (1 = strongly disagree to 5 = strongly agree) designed to measure perceived gains in knowledge and skill development, confidence and self-efficacy, and interest in computing and related careers.

Descriptive statistics were computed for each survey item, and results were grouped into three outcome categories aligned with program goals:

1. knowledge and skill development,
2. confidence and self-efficacy, and
3. interest and career awareness.

5.2 Knowledge and Skill Development

Participants reported strong perceived gains in foundational computing, cybersecurity, and AI knowledge. Students indicated improved understanding of basic computing and programming concepts ($M = 3.71$), fundamental cybersecurity concepts ($M = 4.00$), and introductory AI concepts ($M = 3.80$). Students also reported increased ability to apply learned concepts to real-world problems ($M = 3.12$) and increased comfort using tools introduced during the program ($M = 3.82$).

These findings suggest that the CyberHusky curriculum successfully introduces core technical concepts in an accessible manner while enabling students to connect abstract ideas to practical applications. The use of hands-on activities, guided coding exercises, and project-based exploration appears to support meaningful learning gains among students with varied prior experience.

5.3 Confidence and Self-Efficacy Outcomes

Students also reported notable improvements in confidence related to computing and technical problem solving. Participants indicated increased confidence in learning new computing skills ($M = 3.80$), troubleshooting technical problems ($M = 3.75$), and participating in technical discussions or competitions ($M = 3.88$). Students further reported increased confidence in their ability to succeed in more advanced computing courses ($M = 3.82$) and in explaining technical concepts to others ($M = 3.27$).

These results indicate that CyberHusky not only builds technical knowledge but also strengthens students' self-efficacy in computing contexts. Confidence gains are particularly important for students with limited prior exposure to computing and may contribute to continued engagement in STEM learning pathways.

5.4 Interest and Career Awareness

Survey responses indicate that CyberHusky participation positively influenced students' interest in computing-related fields and awareness of career pathways. Students reported increased interest in computing ($M = 4.00$), AI and data-related topics ($M = 3.45$), and cybersecurity ($M = 3.64$). Participants also reported greater awareness of computing and cybersecurity career pathways ($M = 3.80$) and increased likelihood of pursuing related fields in the future ($M = 3.40$).

Although interest in cybersecurity showed slightly lower gains than general computing interest, overall results suggest that CyberHusky serves as an effective entry point for introducing students to computing disciplines and helping them envision future academic and career opportunities.

5.5 Summary of Assessment Findings

Across all three outcome categories, survey results indicate strong positive perceptions of learning and engagement. Participants reported meaningful gains in technical understanding, confidence, and interest in computing pathways. The consistency of responses across items suggests that the program's combination of hands-on learning, mentorship, and competition-inspired activities effectively supports student learning and motivation.

While the findings are based on self-reported data, small sample size, and a single program cohort, the results provide encouraging evidence that short-term, university-led outreach programs can positively influence high school students' AI literacy, computing confidence, and interest in STEM careers. These outcomes support the continued development and expansion of CyberHusky as a scalable model for K–12 AI and cybersecurity outreach.

5.6 Team Achievements

Over the past several years, the CyberHusky team has achieved significant competitive success and external recognition, highlighting its strength as a student-led computing organization and its effectiveness in experiential learning. Through sustained participation in regional and national competitions, CyberHusky students have demonstrated strong technical proficiency, teamwork, and problem-solving skills across a broad range of computing domains.

In the 2025 CyberPatriot National Competition, CyberHusky teams achieved their best results to date: one team placed 4th in Michigan's Platinum tier, another earned 7th place in the same tier, and a third secured 12th place in the Gold tier, marking the first time the program placed two teams in the top ten of the Platinum division since its inception. These results reflect substantial growth in technical capability and competitive maturity among middle and high school participants coached through the program.

In addition to state-level success, CyberHusky teams have made strong showings on the national stage in the National Cyber League (NCL) competitions. Notably, in spring 2025 the high school teams achieved top national rankings, with one team placing #20 among over 900 competitors and others ranking within the top 150, and several individual students finished within the top 100 nationally for individual performance. Historically, the program has also earned high national placements in previous NCL seasons and achieved top-tier rankings in earlier CyberPatriot and Michigan Governor's High School Cyber Challenge events, demonstrating sustained excellence and impact in cybersecurity education and competition for K–12 students.

6. Limitations and Future Work

This study has several limitations. The participant sample size is modest, and results are based primarily on self-reported data. Future work will include longitudinal tracking of participants and expanded assessment of learning outcomes.

Planned program enhancements include deeper exploration of generative AI, expanded teacher professional development, and broader dissemination through partnerships with additional schools and organizations.

7. Conclusion

CyberHusky provides a promising model for K–12 AI education that is accessible, engaging, and grounded in real-world applications. By combining AI learning with cybersecurity contexts, project-based pedagogy, and community engagement, the program supports the development of AI literacy, confidence, and career interest among high school students. The findings suggest that similar outreach initiatives can play a vital role in preparing the next generation for an AI-driven future.

Acknowledgment

This project is supported by the National Science Foundation under Awards No. 2043022 and No. 2247492.

References

[1] Di Wu, Meng Chen, Xu Chen, Xing Liu, Analyzing K-12 AI education: A large language model study of classroom instruction on learning theories, pedagogy, tools, and AI literacy, Computers and Education: Artificial Intelligence, Volume 7, 2024

[2] Ming Ma, Davy Tsz Kit Ng, Zhichun Liu, Gary K.W. Wong, Fostering responsible AI literacy: A systematic review of K-12 AI ethics education, Computers and Education: Artificial Intelligence, Volume 8, 2025

[3] Iris Heung Yue Yim, Jiahong Su. 2025. Artificial intelligence literacy education in primary schools: A review. International Journal of Technology and Design Education, 35, 2175–2204.

[4] Sarah Nite, Wesley Brashear, Thomas Gray, and Debabrata Chakravorty. 2025. Project-based learning in K–12 cybersecurity education. Journal of the Colloquium for Information Systems Security Education 12, 1 (2025), Article 6.

[5] Ahmed Ibrahim, Michael McKee, L. F. Sikos, and N. F. Johnson. 2024. A Systematic Review of K-12 Cybersecurity Education Around the World, in IEEE Access, vol. 12, pp. 59726-59738, 2024

[6] Yu Cai, Andrew Youngstrom and Wenbin Zhang, Exploring Approaches for Teaching Cybersecurity and AI for K-12, 2023 IEEE International Conference on Data Mining Workshops, 2023

[7] Abhishek Vaish et al. 2024. Development of an cyber security platform for Experiential Learning. Journal of Cybersecurity, Education, Research & Practice, Vol. 2024, No. 1

[8] Di Wu, Meng Chen, Xu Chen, Xing Liu, Analyzing K-12 AI education: A large language model study of classroom instruction on learning theories, pedagogy, tools, and AI literacy, Computers and Education: Artificial Intelligence, Volume 7, 2024

[9] Baichang Zhong, Xiaofan Liu, Evaluating AI literacy of secondary students: Framework and scale development, Computers & Education, Volume 227, 2025

[10] Ibrahim, Ahmed & McKee, Marnie & Sikos, Leslie & Johnson, Nicola. (2024). A Systematic Review of K-12 Cybersecurity Education Around the World. IEEE Access. 12.

[11] Ming Ma, Davy Tsz Kit Ng, Zhichun Liu, Gary K.W. Wong, Fostering responsible AI literacy: A systematic review of K-12 AI ethics education, Computers and Education: Artificial Intelligence, Volume 8, 2025