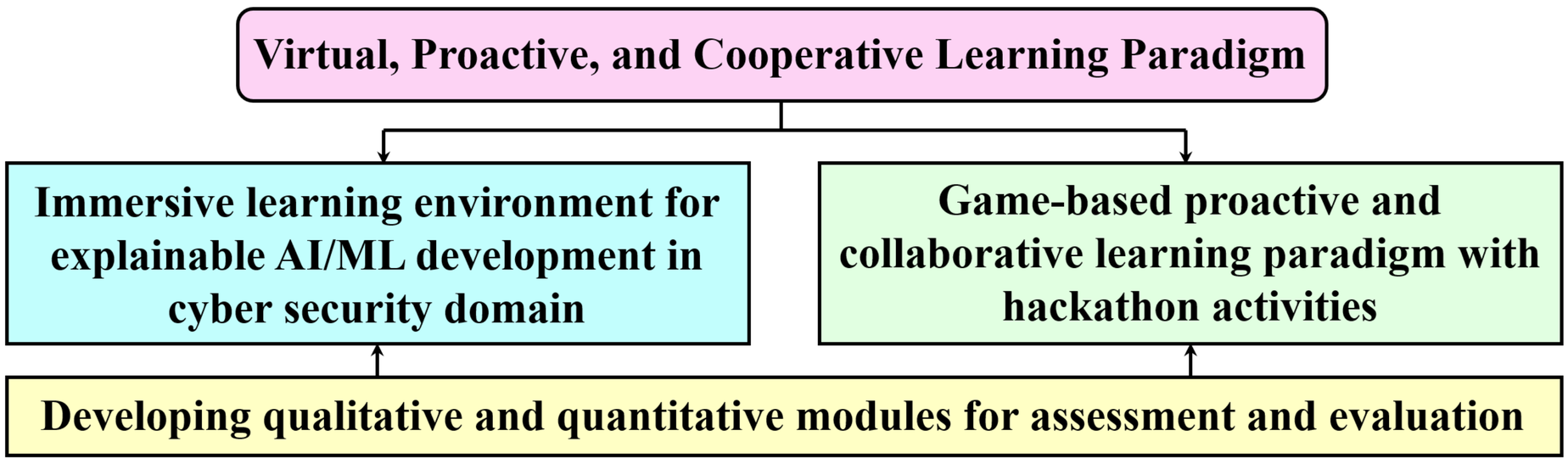
EAGER: SaTC-EDU: Cybersecurity Education in the Age of Artificial Intelligence: A Novel Proactive and Collaborative Learning Paradigm

Dr. Jin Wei-Kocsis, Purdue University

https://polytechnic.purdue.edu/AI-Cybersecurity-Learning



Challenge:

- There is an education and training gap to foster the qualified cyber-workforce that understands the usefulness, limitations, and best practices of artificial intelligence (AI) technologies, specially machine learning (ML), in cybersecurity domain.
- Efforts have been made to address the gap. However, there still remain essential challenges for effectively educating students on the interaction of AI and cybersecurity including: (1) the integration of AI and cybersecurity technologies are rapidly and dynamically evolving; (2) students can have very diverse knowledge background, and thus may have varied needs for inspiring skill and interaction engagement; and (3) while significant studies have been developed in understanding AI/ML-specific threats, very limited efforts have been made in the cybersecurity domain that is complex and rife with adversaries.

Scientific Impact:

- The success of this project will help the general public understand the security implications of AI technologies.
- This project also has the ability to transform education at the intersection of cybersecurity and AI/ML; shed light on explainable AI in cybersecurity; and grow a cybersecurity workforce that possesses AI competencies.

Solution:

- This project aims to design and implement a virtual, proactive, and collaborative learning paradigm that can engage learners with diverse background and enable effective retention and transfer of the multidisciplinary AI/ML-cybersecurity knowledge.
- To realize this proposed learning paradigm, we leverage multidisciplinary expertise in cybersecurity, AI, and statistics to systematically investigate two cohesive research and education goals: (1) developing an immersive learning environment that motivates the students to explore AI/ML development in the context of real-world cybersecurity scenarios by constructing learning models with tangible objects; and (2) designing a proactive education paradigm with the use of hackathon activities based on game-based learning, lifelong learning, and social constructivism.
- This transformative learning paradigm will inspire a wide range of learners to proactively and collaboratively formulate new AI-specific threats in cybersecurity domain and develop innovative trustworthy and robust AI/ML solutions.

Broader Impact and Broader Participation:

- The success of this project will have timely and fundamental impact on transforming the cybersecurity and AI/ML education and fostering robust workforce with integrated AI and cybersecurity competencies.
- This proposed transformative learning paradigm will benefit a larger range of learners, especially minority and underrepresented students.
- We will disseminate the research results via: (1) hosting workshops with hackathon activities; (2) participating AI and cybersecurity related conferences; (3) publishing articles in peer-reviewed journals; (4) exchanging experiences and results with collaborating institutions and organizations; and (5) designing outreach activities for K-12 students.
- This project will also lead to an early planning of a multi-institution education and research center focusing on AI/ML-powered cybersecurity.

Team Members: Dr. Jin Wei-Kocsis (PI), Dr. Baijian Yang (Co-PI), Dr. Tonglin Zhang (Co-PI), Mr. Moein Sabounchi (Research Assistant), and Mr. Huyunting Huang (Research Assistant).

Award ID#: 2114974

PURDUE UNIVERSITY