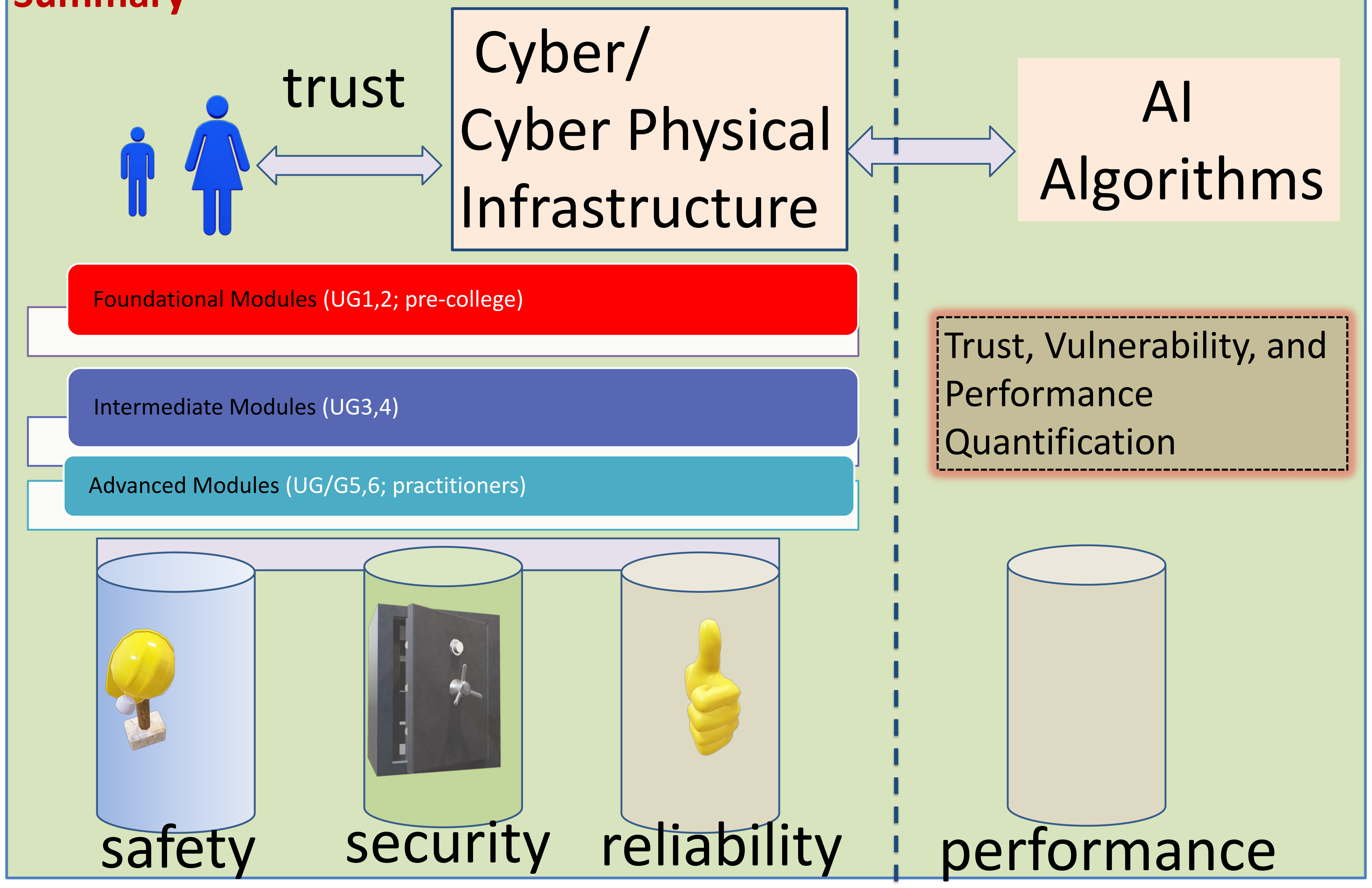
CyberTraining: Pilot: Modular experiential learning for secure, safe, and reliable AI (MELSSRAI)

Alvis Fong (PI), Ajay Gupta (Co-PI), Steve Carr (Co-PI), Shameek Bhattacharjee (Co-PI), **Western Michigan University (WMU)**, Award# 2017289

Project URL: https://fong.cs.wmich.edu/

Summary



trust

Cyber/ Cyber Physical Infrastructure

AI Algorithms

Foundational Modules (UG1,2; pre-college)

Intermediate Modules (UG3,4)

Advanced Modules (UG/G5,6; practitioners)

Trust, Vulnerability, and Performance Quantification

safety

security

reliability

performance

Challenges

- How to promote trust between Cyber Physical Infrastructure users and Artificial Intelligence (AI) based Algorithms
- Training students on how to balance trade-off between improving Security, Safety and Reliability of AI and the sacrifice in algorithmic performance
- Building education tools for foundational understanding of vulnerabilities in AI and how they manifest in context to varying application domains (e.g. Blog analysis, smart grid, vehicular crowdsensing)
- Design effective teaching and training strategies for the above for various education levels viz. K12, undergraduate, graduate studies

Contributions

Training and Education

- Develop experiential learning modules to rapidly upskill CI users
- Hands-on-projects given to experience how a given AI/ML method fails under given situations
- Feedback collected from students in a module by module basis
- New Course on Artificial Intelligence based Security for CPS
- Information retrieval course focused on removing bias in training AI approaches

Research Contributions and Impact

- Tutorial on *how cognitive biases* impact decisions taken in online recommendation systems and suggest mitigation strategies
- Data Poisoning Attack Strategies against Anomaly Detection Schemes using AI
- *Quantified vulnerability level* of using ML based Anomaly Detection in Smart Grids under Data Poisoning and Evasion Strategies
- Proposed a *Unified Threat Landscape of Vulnerabilities* that arise from using AI in the operations of Mobile Crowdsensing Systems.

Broader Scientific Impact

- How efficiency in performance results in more vulnerable AI
- Education and Training modules made public
- Case studies on for smart energy, transportation, crowdsensing, common sense reasoning (ongoing)
- Classroom strategies with positive
- Commonsense reasoning for robust AI approaches

Feedback are being reported in CS education conferences

Outreach

1. Bhattacharjee *has entered into annual collaboration with Kalamazoo Math Science Center (KAMSC)* for advising in high school engineering projects that compete at the state

2. Bhattacharjee offered a new course on Artificial Intelligence based Security

3. Bhattacharjee gave a invited lecture in Missouri S & T on vulnerabilities of using AI for security in Cyber Physical Systems

4. Carr reached out to IBM for secure coding practices for building AI applications.

Impact of Participation

1. One PhD student funded;

2. Two women PhD student recruited at WMU

3. K-12 students participating in the project won best computer science project award for high school regional science fair with KAMSC

4. 5 undergraduate students in WMU participated in learning and building of training materials.

5. 3 students recruited through the REU supplement and currently undergoing active involvement with assisting in module development.

Publications/Products

1. S. Saeedi, A. Fong, S. Mohanty, S. Carr, A. Gupta, "Consumer Artificial Intelligence Mishaps and Mitigation Strategies, ***IEEE Consumer Electronics Magazine**, 2021.*

2. S. Bhattacharjee, M. Islam, S. Abed-Zadeh, "Robust Anomaly based Attack Detection in Smart Grids under Data Poisoning Attacks "***ACM Asia' CCS Workshop. on Cyber Physical Sec***., 2022

3. S. Saeedi, A. Panahi, A. Fong, "Evaluation of state-of-the-art NLP-Deep Learning Architectures on Commonsense Reasoning Tasks" ***14th Intl. Workshop. on Semantic Evaluation***, 2020

4. P. Madhavarapu, S. Bhattacharjee, S. Das "A Generative Model for Evasion Attacks in Smart Grids", ***IEEE INFOCOM Workshop on Big Data Security**, 2022*

5. P. Madhavarapu, P. Roy, S. Bhattacharjee, S. Das, "Active Learning Augmented Folded Gaussian Model for Anomaly Detection in Smart Transportation", ***IEEE ICC***, 2022

6. S. Bhattacharjee and S.K. Das, "Unified Threat Landscape Specification for Participatory Mobile Crowdsensing Applications, ***IEEE Pervasive Computing***, under review

The 5th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
June 1-2, 2022 | Arlington, Virginia