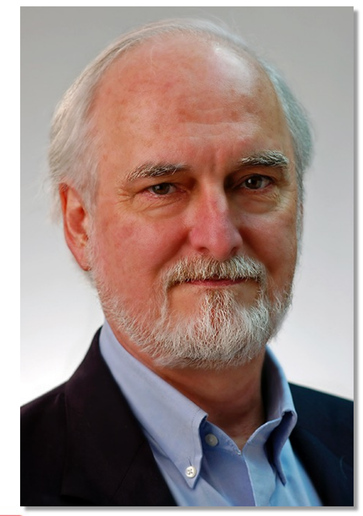
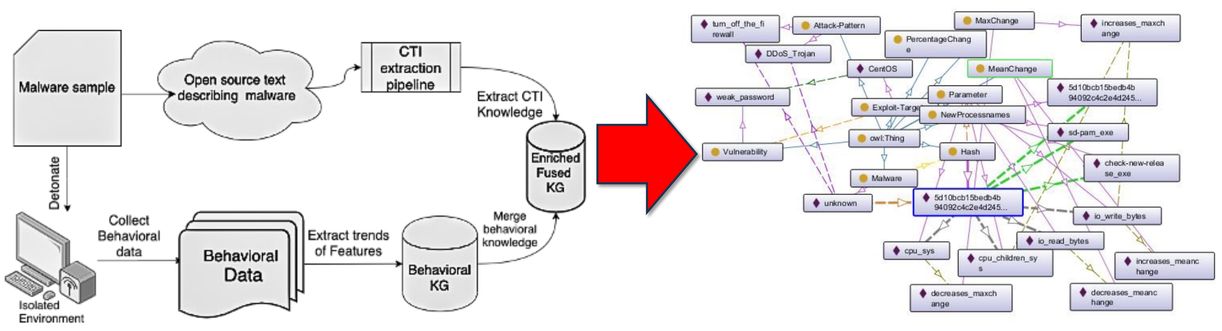
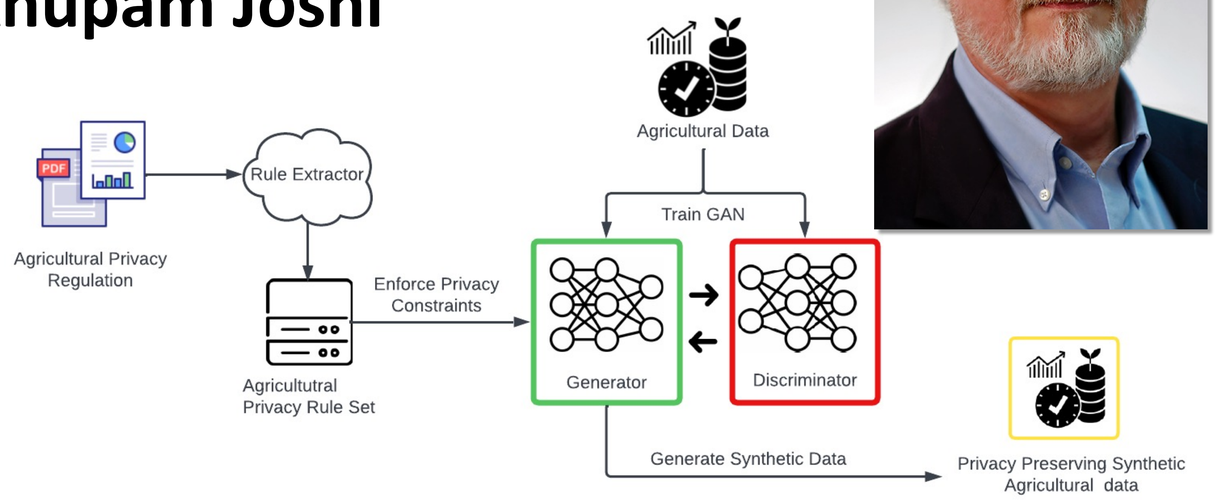
Collaborative Research: EAGER SaTC-EDU:
AI and Cybersecurity: from Research to the Classroom

PI: Tim Finin; CO-PIs: Alan Sherman and Anupam Joshi





Knowledge Guided Two-player Reinforcement Learning for Cyber Attacks and Defenses



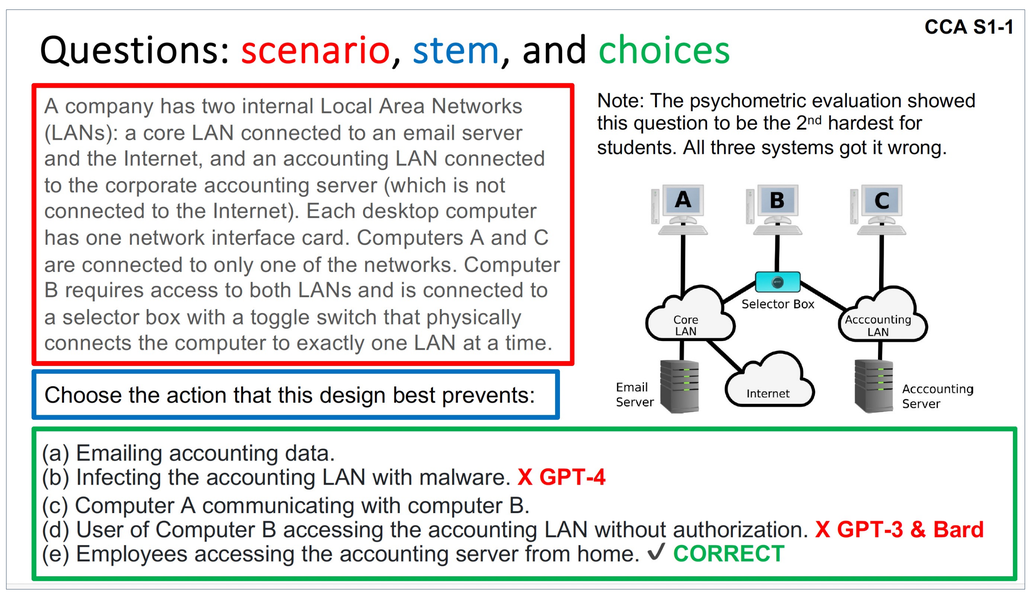
Privacy-Preserving Data Generation in Agriculture with Privacy Policy Enforcement

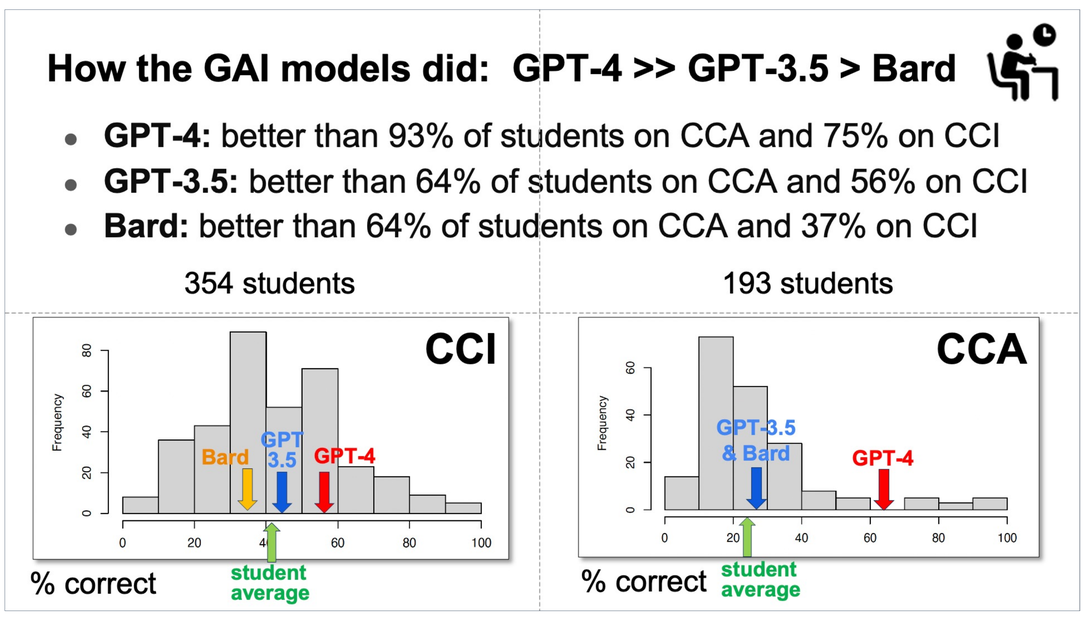
Objectives and Challenges:

- Explore ways different AI technologies can be applied to cybersecurity
- Develop and evaluate systems applicable to multiple cybersecurity problems
- Engage students at all levels: BS, MS, PhD
- Support students from groups under-represented in computing

Scientific Impact:

- Developed shared ontologies for cybersecurity knowledge graphs
- Created NLP systems to populate knowledge graphs with cybersecurity data
- Reinforcement learning to train malware defense
- New generative models for privacy-preserving data sharing





Impact on society

- Latest AI technologies can improve critical cybersecurity systems
- Help detect disinformation on the Internet and social media
- Learn to recognize evolving Malware attacks
- Protect privacy by generating synthetic data from real data

Impact on education

- Evaluated competency of GenAI systems using CCA and CCI exams
- Developing systems to recognize misleading data graphs and charts
- Developed material for a course on knowledge graphs
- Developed modules for AI courses

Impact on participation

- Supported four PhD students, three of whom were women
- Supported one female MS student
- Supported five undergrads, four of whom were Meyerhoff Scholars
- Presented new AI technologies to MD legislators, H.S. and college teachers