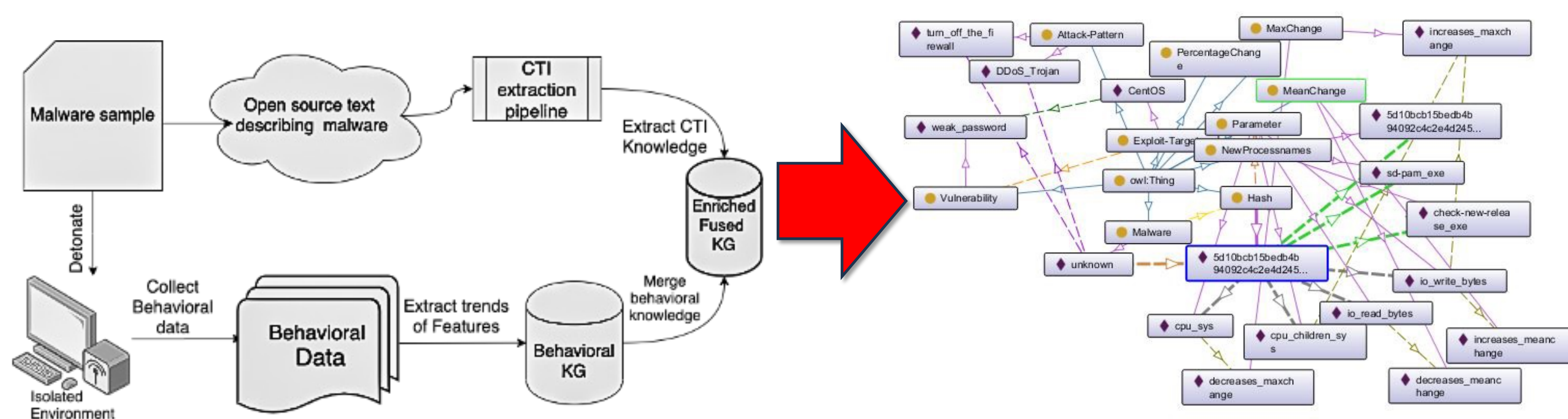
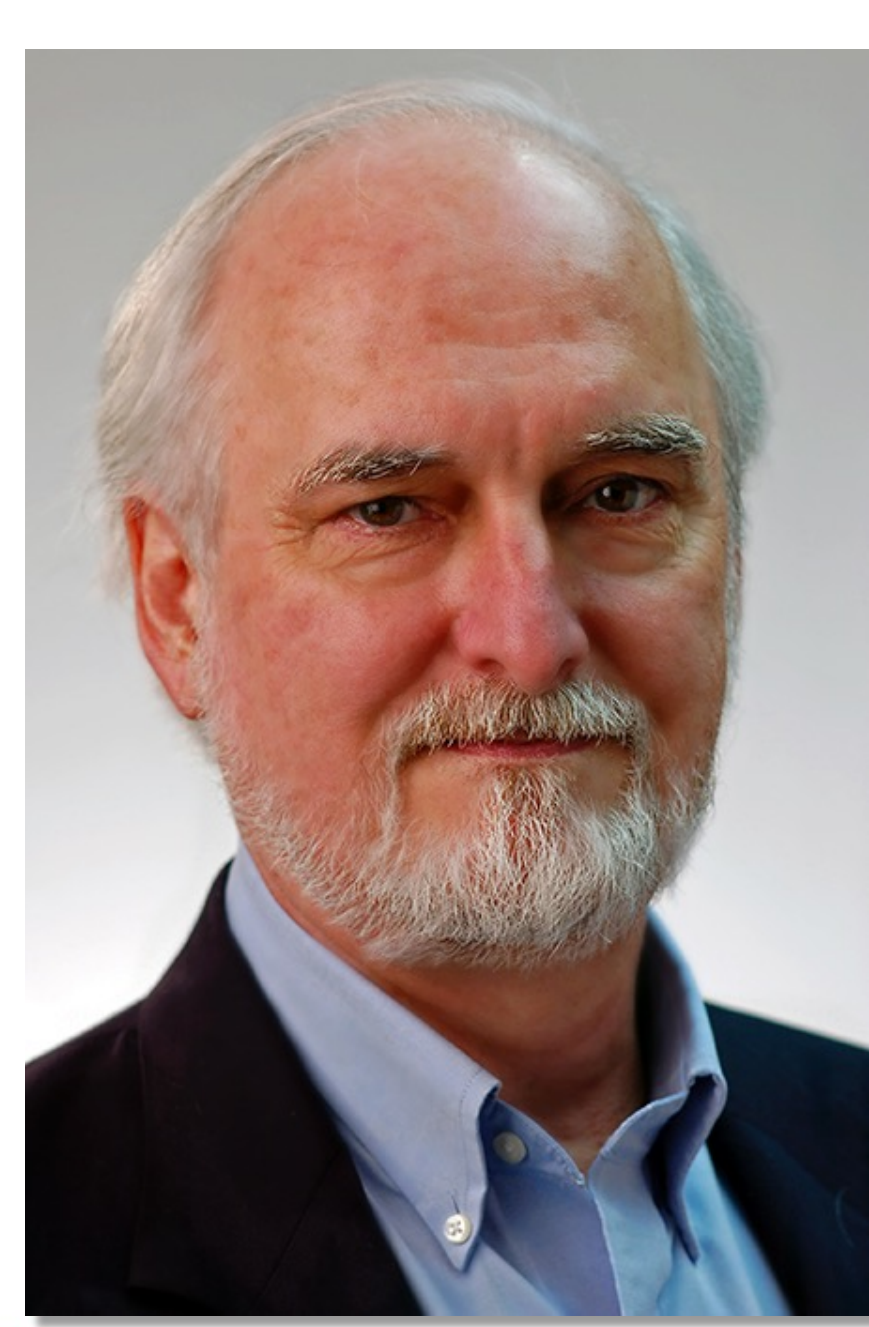
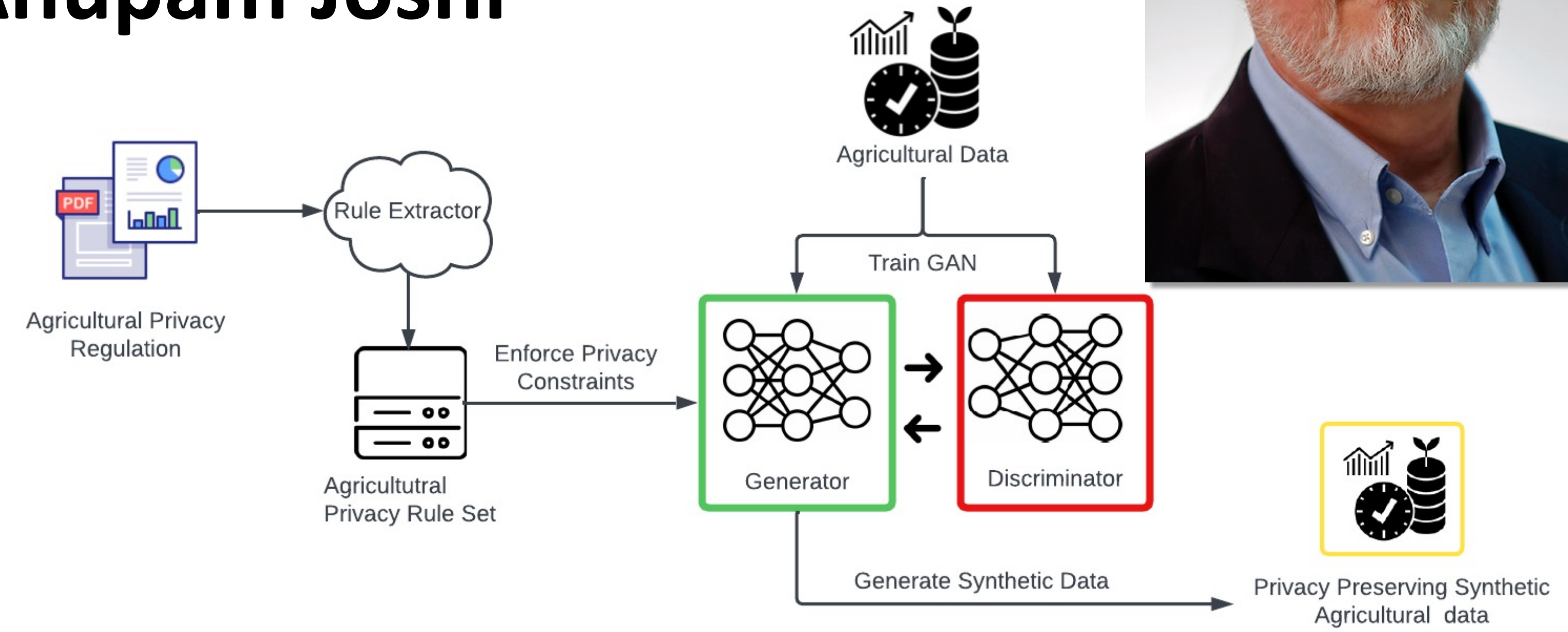


Collaborative Research: EAGER SaTC-EDU: AI and Cybersecurity: from Research to the Classroom

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

Questions: **scenario**, **stem**, and **choices** CCA S1-1

A company has two internal Local Area Networks (LANs): a core LAN connected to an email server and the Internet, and an accounting LAN connected to the corporate accounting server (which is not connected to the Internet). Each desktop computer has one network interface card. Computers A and C are connected to only one of the networks. Computer B requires access to both LANs and is connected to a selector box with a toggle switch that physically connects the computer to exactly one LAN at a time.

Note: The psychometric evaluation showed this question to be the 2nd hardest for students. All three systems got it wrong.

Choose the action that this design best prevents:

(a) Emailing accounting data.
 (b) Infecting the accounting LAN with malware. **X GPT-4**
 (c) Computer A communicating with computer B.
 (d) User of Computer B accessing the accounting LAN without authorization. **X GPT-3 & Bard**
 (e) Employees accessing the accounting server from home. **✓ CORRECT**

How the GAI models did: **GPT-4 >> GPT-3.5 > Bard**

- **GPT-4:** better than 93% of students on CCA and 75% on CCI
- **GPT-3.5:** better than 64% of students on CCA and 56% on CCI
- **Bard:** better than 64% of students on CCA and 37% on CCI

354 students

CCI

193 students

CCA

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

