Cybersecurity Education in the intersection of AI and Cybersecurity

NSF 2038029: Privacy Enhancing Techniques and Innovations for AI-Cybersecurity Cross Training

PI: Professor Dr. Ling Liu, School of Computer Science, Georgia Institute of Technology

Image source: Yolo-github

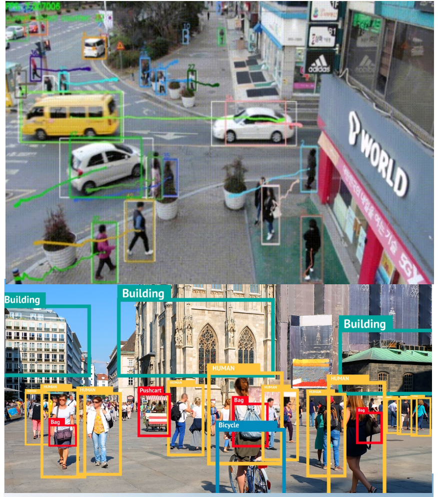
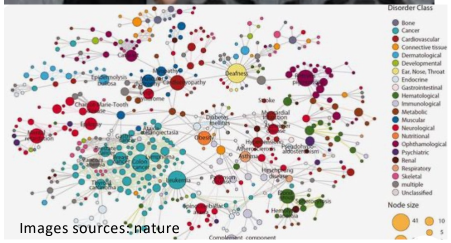
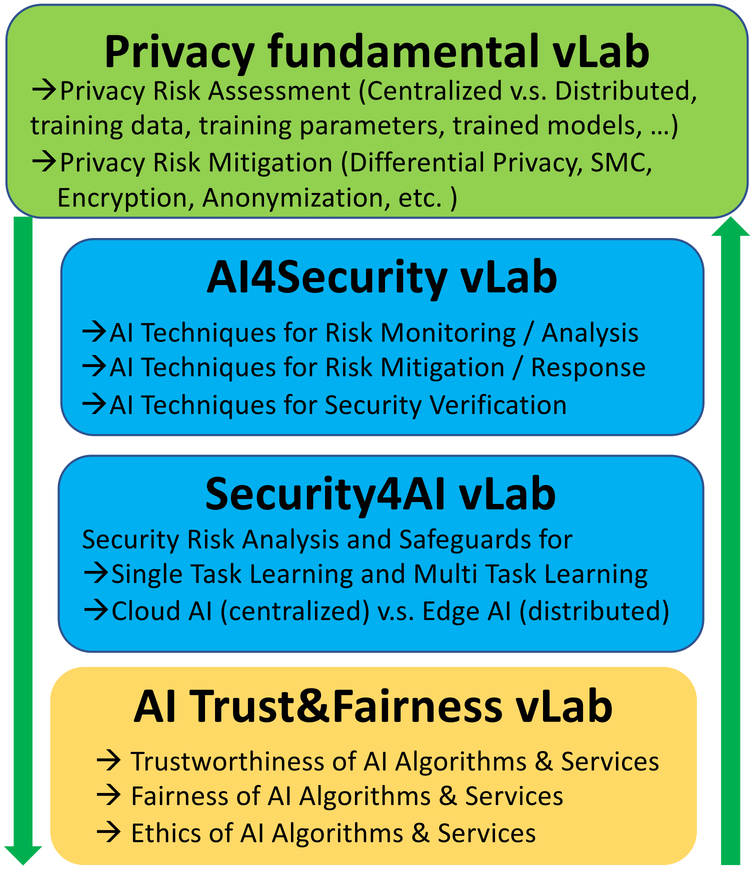


Image source: fpv-drones@store.dji.com



Images sources: nature

AI techniques provide cybersecurity with automated monitoring, analysis, and responses.



Privacy fundamental vLab

→Privacy Risk Assessment (Centralized v.s. Distributed, training data, training parameters, trained models, …)
→Privacy Risk Mitigation (Differential Privacy, SMC, Encryption, Anonymization, etc.)

AI4Security vLab

→AI Techniques for Risk Monitoring / Analysis
→AI Techniques for Risk Mitigation / Response
→AI Techniques for Security Verification

Security4AI vLab

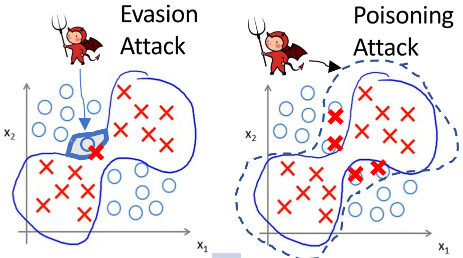
Security Risk Analysis and Safeguards for
→Single Task Learning and Multi Task Learning
→Cloud AI (centralized) v.s. Edge AI (distributed)

AI Trust&Fairness vLab

→ Trustworthiness of AI Algorithms & Services
→ Fairness of AI Algorithms & Services
→ Ethics of AI Algorithms & Services

AI-Cybersecurity cross training for next generation of AI-Cybersecurity workforce

Guarding AI technologies from unintended uses and adversarial exploitation with Cybersecurity practices



Picture: Getty Images