EAGER: SaTC AI-Cybersecurity:
Secure and Privacy-Preserving Adaptive Artificial Intelligence Curriculum Development for Cyber Security

Challenge:

- Current materials are not always comprehensive, especially in new areas like adversarial machine learning.
- Content is highly technical, presenting everything all at once can be overwhelming

Solution:

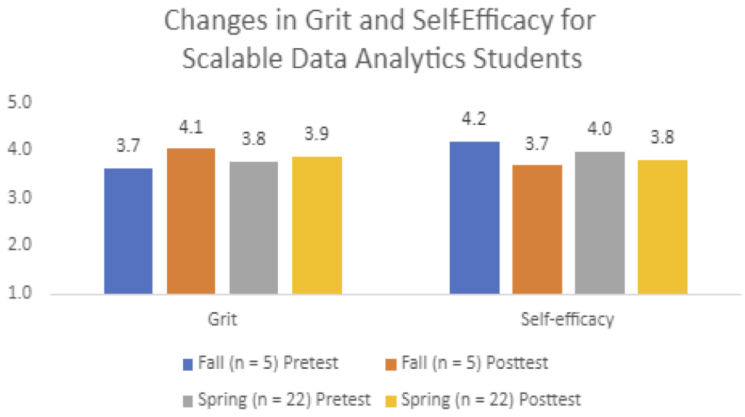
- Modularization: This has various benefits. Makes the curriculum more structured, also allows a "plug and play" format where learners can pick and choose what appeals more to them.
- Modules can also be reused where suitable across various courses.

Scalable Advanced Analytics

1-FeatureExtraction
|-- 1. Introduction to Text Classification.pptx
|-- 2. Text Pre-processing and Feature Extraction.pptx
|-- Assessment Quiz.docx
|-- Background for Data Preprocessing, Feature Extraction Module.docx
|-- Labs
|-- Lesson1 Lab.docx
|-- Lesson2 Lab.docx
|-- Lesson1 Lab – Solutions
|-- Lesson2 Lab - Solutions
|-- videos

CyS for ML (Adversarial ML)

1- Fast Gradient Sign Method
| -- FGSM.pptx
| -- Homework 1
| --Associated Publications
2- DeepFool
| -- DeepFool.pptx
| -- Homework 2
3 – SHAP
| -- SHAP.pptx
| -- Associated Publications
4 – Targeted Bit Trojan
| -- TBT.pptx
| -- Associated Publications



Scientific Impact:

- Answers to important questions such as whether students who complete self-directed learning modules perform as well on end-of-pathway competency assessment as students who complete instructor-led modules

Broader Impact and Broader Participation:

- Awareness regarding cybersecurity is absolutely essential and often in the national interest.
- Knowing how and when to protect digital assets/systems will save both money, time, as well as create a safer society which safeguards privacy.

Project Number: 2039542
Institution: The University of Texas at Dallas

Contact: Latifur Khan