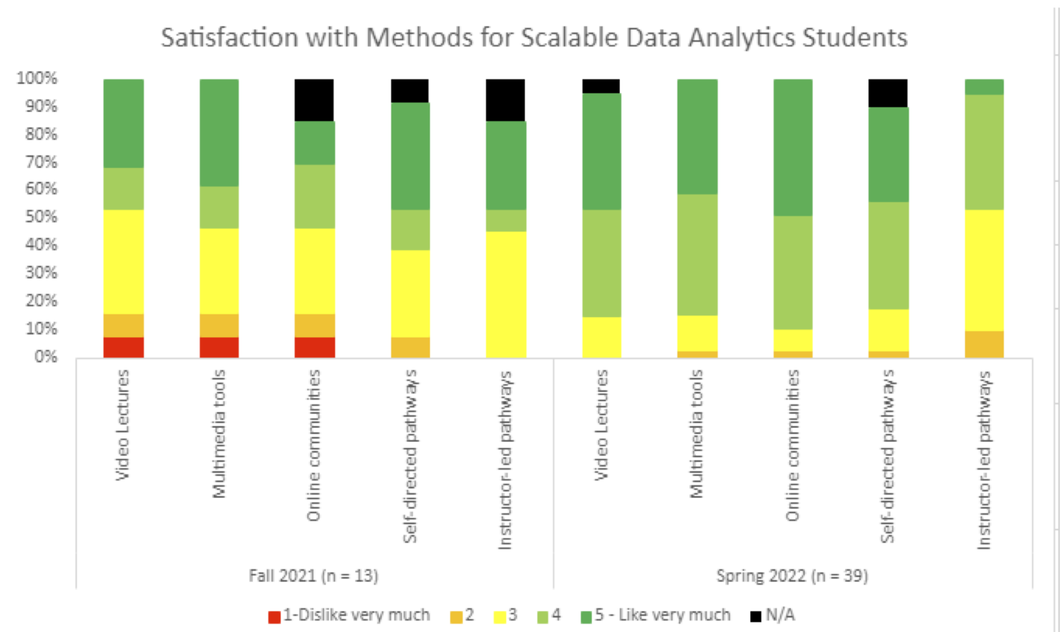
EAGER: SaTC AI-Cybersecurity: Secure and Privacy-Preserving Adaptive Artificial Intelligence Curriculum Development for Cyber Security

Latifur Khan, Kim Nimon, Lin Lin

lkhan@utdallas.edu, knimon@uttyler.edu, lin.lin@unt.edu

Scalable Advanced Analytics	**CyS for ML (Adversarial ML)**
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	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



Challenges:

- 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
- Answering questions regarding self-directed and instructor led modules

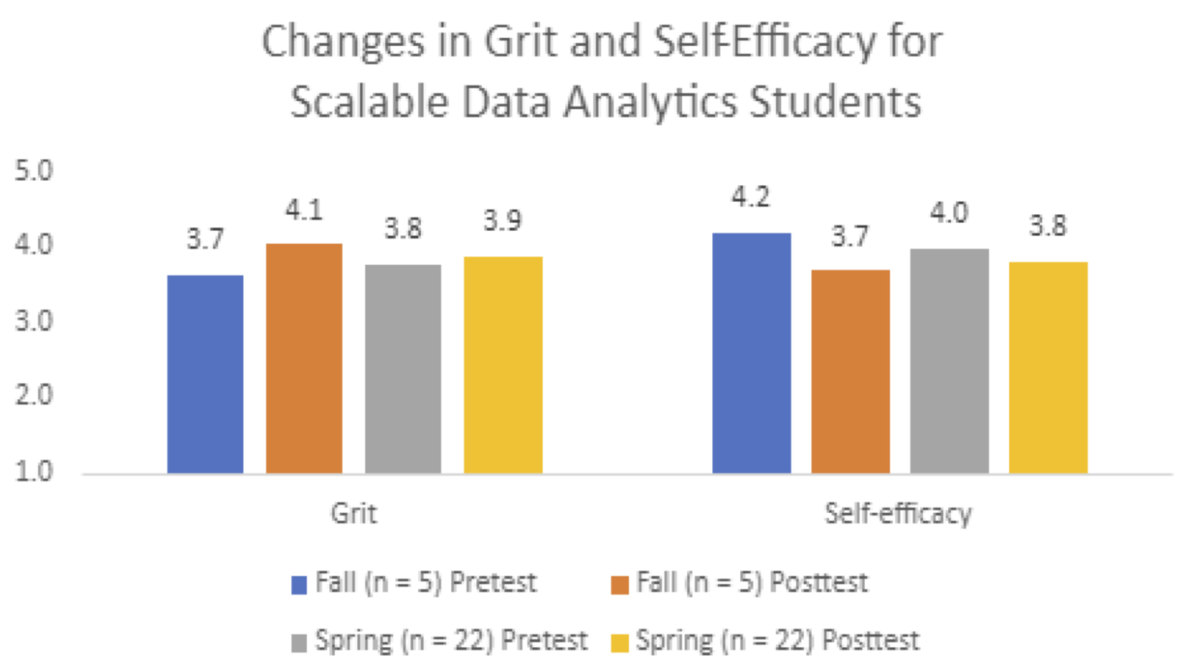
Solutions:

- Creating modularized courses
- Investigating the impact of various design strategies
- Repeating our observations over various courses for generalizability.

Scientific Impact:

Answers to important questions such as:

- As a consequence of completing one or more of our courses, do students' self-beliefs improve?
- What is the student satisfaction with the design strategies employed in our courses?



Broader Impact (On Society)

Our courses deal with important content such as cybersecurity, and exposure to our courses will help society at large by making them aware of security issues, as well as the latest advances in machine learning and their implications.

Broader Impact (Education and outreach)

These courses will be made available to a wide audience, and students will gain knowledge on important issues across areas ranging from big data to security. These courses will increase interest in their respective areas.

Broader Impact and Participation

Increased interest in the intersection of artificial intelligence and cybersecurity will bring in more practitioners, who will consequently bolster the field as a whole