# SaTC: CORE: Small: Deep Learning for Insider Threat Detection

UtahStateUniversity

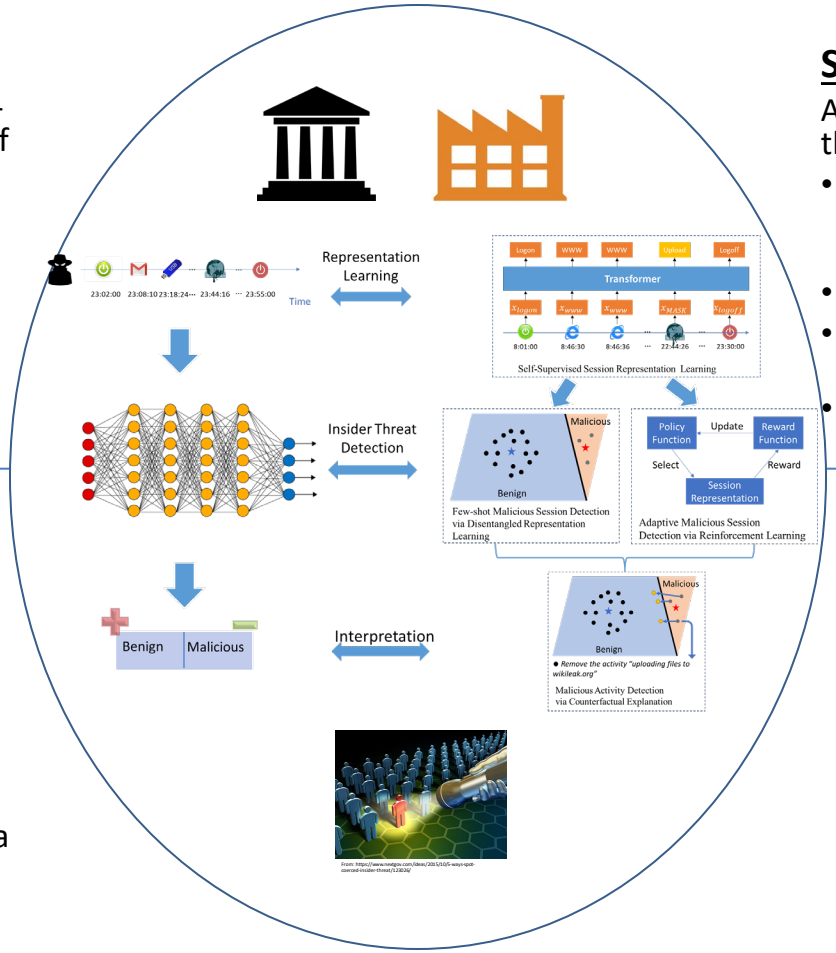
## Challenge:

- Extremely Unbalanced Data -- An extremely small number of insiders
- Subtle and adaptive activity changes – Hard to notice and adaptive changes to evade detection
- Fine-grained Insider Threat Detection – Detect suspicious activities

## Solution:

A deep learning framework:

- Self-supervised session representation learning
- Few-shot insider threat detection
- Adaptive threat detection via reinforcement learning;
- Malicious activity detection via counterfactual explanation




## Scientific Impact:

Advance the theory and practice of the broad task of fraud detection.

- Capture complicated activities from fraudsters without using any labeled data
- Detect subtle malicious activities
- Identify adaptive attacks from fraudsters
- Interpretable fraud detection

## Broader Impact and Broader Participation:

- Benefit industries and governments that are frequently under attack from malicious insiders.
- Proposed approaches can be adapted to achieve broad fraud detection scenarios.
- Integrate the project into courses


Project info (# 2103829,
UTAH STATE UNIVERSITY,
Shuhan Yuan, shuhan.yuan@usu.edu)