

SaTC: CORE: Medium: Privacy for All: Ensuring Fair Privacy Protection in Machine Learning

PIs: Wendy Hui Wang (Stevens Institute of Technology),
Jun Xu (University of Utah)

Co-PI: Yu Tao (Stevens Institute of Technology)

CNS 2029038, Jan 2021 – Dec 2024

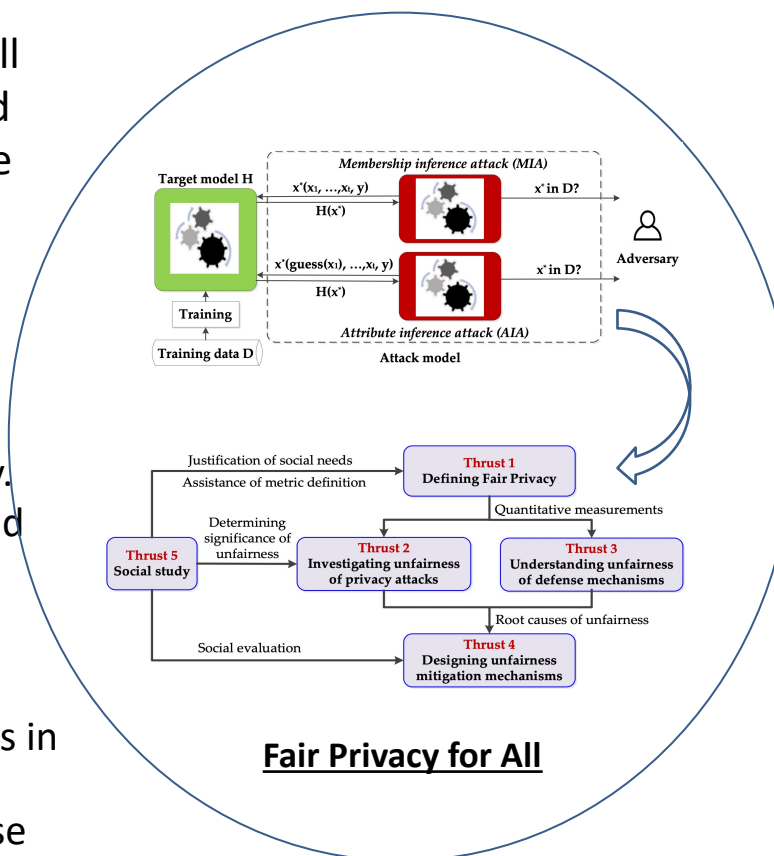


Challenge:

How to ensure the privacy of all groups and individuals involved in machine learning models are protected equitably?

Solution:

- Define metrics of fair privacy.
- Understand the existence and significance of unfairness in existing privacy protection techniques.
- Develop data-processing techniques to ensure fairness in privacy protection.
- Perform social studies to raise awareness in the society.



Scientific Impact:

- Unveil a new form of fairness issues and its impacts in the use of machine learning
- Provide pioneering techniques to mitigate the fairness issues under privacy context.

Broader Impact:

- Publications in AsiaCCS'22 and American Sociological Association conference (ASA);
- A large social study with ~740 SIT students;
- Open-source tools & datasets
- 2 new courses at SIT & Utah
- 3 PhD students (1 female) and 3 master RAs.