Wenqi Wei

Email: wenqiwei@gatech.edu
Mobile: 4042138068
Homepage: https://wenqiwei789.github.io/Homepage/

Education

- **Georgia Institute of Technology** Atlanta, GA
  Ph.D. student in Computer Science *Aug. 2017 to present*
  Current research areas of Interest: Systems for Machine Learning and AI, Machine Learning and AI algorithm for Big Data Applications and Services, Security and Privacy in Machine Learning.
- **Huazhong University of Science and Technology** Wuhan, China
  Bachelor of Engineering in Electronics and Information Engineering *Sept. 2013 to June. 2017*
  Signal processing track, Graduated with Honors

Research Experience

- **Georgia Institute of Technology** Atlanta, GA
  Distributed Data Intensive Systems Lab *advisor: Prof. Ling Liu*
  Graduate Research Assistant(Aug 2017 - present)
  - **Machine Learning**: Research on deep learning systems, including deep learning algorithm and system design, performance measurement (benchmarking) and model optimization(model compression and parameter tuning). Proficient in TensorFlow and Python, hands on experience on Caffe, Torch and Theano.
  - **Privacy-preserving Deep Learning**: Research on providing privacy preserving deep learning models that could give accurate results while preserving data privacy.
  - **Adversarial Deep Learning: Attacks and Defenses**: Research on characterizing adversarial examples in deep learning and designing attack mitigation strategies.
  - **DeepEyes: Deep Learning with Crowdsourcing for real-time Localization**: Research and development of infrastructure-free localization system and service with DeepID-based multi-class identification and crowdsourcing.
- **Samsung Research America** Mountain View, CA
  Data Intelligence Group, AI center
  Research Intern(May 2018 - August 2018)
- **Huazhong University of Science and Technology** Wuhan, China
  Signal Processing and Information Networking in Communication Lab *advisor: Prof. Pan Zhou*
  Undergraduate Research Assistant(Sept 2015 - June 2017)
  - **Privacy-preserving Machine Learning**: Worked on designing differentially private online learning (multi-armed bandit) algorithm for providing privacy-preserving and near-optimal social network advertising recommendation. Research on algorithmic game-theoretic mechanism design with differential privacy. Our model protects user data privacy while improving utility in large-scale spectrum sharing.
  - **Bandit based Online Learning**: Worked on designing contextual X-armed bandit-based recommendation algorithms for self-diagnosis in ubiquitous healthcare.

Publications

[1] Pan Zhou*, Wenqi Wei*, Kaigui Bian, Dapeng Oliver Wu, Yuchong Hu, Qian Wang. “Private and Truthful Aggregative Game for Large-Scale Spectrum Sharing”, IEEE Journal on Selected Areas in Communications, 35(2), 463-477,2017. (* equal contribution)

[2] Ling Liu, Yanzhao Wu, Wenqi Wei, Wenqi Cao, Semih Sahin, and Qi Zhang. “Benchmarking Deep Learning Frameworks: Design Considerations, Metrics and Beyond.” In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2018.

[3] Wenqi Wei, Yanzhao Wu, Ling Liu. ”DeepEyes: Integrating Deep Learning and Crowd Sourcing for Localization”, Southern Data Science Conference, 2018 (research track poster).

[4] Mehmet Emre Gursoy, Ling Liu, Stacey Truex, Lei Yu, Wenqi Wei. ”Utility-aware synthesis of differentially private and attack-resilient location traces”, in 25th ACM Conference on Computer and Communications Security (CCS), 2018.

[5] Wenqi Wei, Yilin Shen, Xiangyu Zeng, Hongxia Jin, ”Efficient Data Privacy Protection with Spectral Deep Learning”, under the submission of SIAM International Conference on Data Mining (SDM19).

[6] Stacey Truex, Ling Liu, Mehmet Emre Gursoy, Lei Yu, and Wenqi Wei, ”Demystifying Membership Inference Attacks in Machine Learning as a Service”, accepted by IEEE Transaction on Service Computing.

[7] Wenqi Wei, Ling Liu, Stacey Truex, Lei Yu, and Mehmet Emre Gursoy, ”Adversarial Examples in Deep Learning: Characterization and Divergence”, under the submission of IEEE Transaction on Dependable and Secure Computing (https://arxiv.org/abs/1807.00051).