Wenqi Wei

Email: wenqiwei@gatech.edu
Mobile: 404-213-8068
Homepage: https://www.cc.gatech.edu/∼wwei66/

Education

- **Georgia Institute of Technology** — Atlanta, GA
  Ph.D. student in Computer Science — *Aug. 2017 to present*
  - **Current research areas of Interest**: Machine Learning and AI algorithm for Big Data Applications and Services; Security and Trust Enhanced ML and AI systems and Services; Efficient and Privacy-Preserving Federated Learning; Representation Learning, Graph Neural Networks and Graph Data Mining.
  - **Expected Graduation Time**: May, 2022

- **Huazhong University of Science and Technology** — Wuhan, China
  Bachelor of Engineering in Electronics and Information Engineering — *Sept. 2013 to June. 2017*
  Signal processing track, summa cum laude

Research Experience

- **Georgia Institute of Technology** — Atlanta, GA
  Distributed Data Intensive Systems Lab — *advisor: Prof. Ling Liu*
  Graduate Research Assistant(Aug 2017 - present)
  - **Security and Trust Enhanced ML and AI systems and Services**: Research on privacy-preserving deep learning and federated learning, which provides accurate results while preserving data privacy, and on Adversarial Deep Learning, which characterizes adversarial examples in deep learning and designing attack mitigation strategies.
  - **Machine Learning Services**: Research on deep learning systems and federated learning, including learning algorithm and system design, performance measurement (benchmarking) and model optimization(model compression and component design). Proficient in TensorFlow and PyTorch.
  - **Representation Learning**: Research on representation learning, including graph embedding, graph neural networks and distributed data mining.

- **IBM Almaden Research Center** — San Jose, CA
  Applied Intelligence Department
  Research Intern(June 2020 - August 2020).

- **IBM Thomas J. Watson Research Center** — Yorktown Heights, NY
  Enterprise Solutions Department
  Research Intern(May 2019 - August 2019).

- **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.

Selected Publications

[23] Jingya Zhou, Ling Liu, **Wenqi Wei**, and Jianxi Fan "Network Representation Learning: From Preprocessing, Feature Extraction to Node Embedding", Under the submission of ACM Computing Surveys

[22] Mehmet Emre Gursoy, Ling Liu, Ka-Ho Chow, Stacey Truex, and **Wenqi Wei** "Analyzing Local Differential Privacy Protocols Through a Bayesian Adversary Lens", Under the submission of CCS 2020

[21] Ka-Ho Chow, Ling Liu, Mehmet Emre Gursoy, Stacey Truex, **Wenqi Wei**, and Yanzhao Wu "Adversarial Objectness Gradient Attacks on Real-time Object Detection Systems", Under the submission of ACSAC 2020

[20] Yanzhao Wu, Ka-Ho Chow, **Wenqi Wei**, Ling Liu. "Boosting Ensemble Accuracy by Revisiting Ensemble Diversity Metrics.", under the submission of NeurIPS, 2020.

[19] Stacey Truex, Ling Liu, Ka-Ho Chow, Mehmet Emre Gursoy, **Wenqi Wei**. "LDP-Fed: Federated Learning with Local Differential Privacy.", under the submission of NeurIPS, 2020.

[18] **Wenqi Wei**, Ling Liu. "Robust Federated Learning against Gradient Leakage via Client Differential Privacy.", under the submission of NeurIPS, 2020.

[17] Ka-Ho Chow, Ling Liu, Mehmet Gursoy, Stacey Truex, **Wenqi Wei** and Yanzhao Wu. "Demystifying Adversarial Attacks in Real-time Object Detection Systems.", In ESORICS, Springer, 2020.

[16] **Wenqi Wei**, Ling Liu, Margaret Loper, Ka-Ho Chow, Mehmet Emre Gursoy, Stacey Truex, Yanzhao Wu. "A Framework for Evaluating Gradient Leakage Attacks in Federated Learning.", In ESORICS, Springer, 2020.

[15] Stacey Truex, Ling Liu, Ka-Ho Chow, Mehmet Emre Gursoy, and **Wenqi Wei**. "LDP-Fed: Federated Learning with Local Differential Privacy.", In ACM EdgeSys 2020, ACM, 2020. (**best paper**)

[14] Stacey Truex, Ling Liu, Mehmet Emre Gursoy, **Wenqi Wei**, and Lei Yu, "Effects of Differential Privacy and Data Skewness on Membership Inference Vulnerability." In the First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS), IEEE, 2019.

[13] Ka-Ho Chow, **Wenqi Wei**, Yanzhao Wu, and Ling Liu, "Denoising and Verification Cross-Layer Ensemble Against Black-box Adversarial Attacks." In 2019 IEEE International Conference on Big Data (Big Data), IEEE, 2019.

[12] Yanzhao Wu, Ling Liu, Juhyun Bae, Ka-Ho Chow, Arun Iyengar, Calton Pu, **Wenqi Wei**, Lei Yu, and Qi Zhang, "Demystifying Learning Rate Polices for High Accuracy Training of Deep Neural Networks." In 2019 IEEE International Conference on Big Data (Big Data), IEEE, 2019.

[11] **Wenqi Wei**, Qi Zhang, and Ling Liu, "DLForecast: Deep Spatiotemporal Forecasting on Bitcoin Transactions", under the submission of IEEE Transaction on Emerging Topics in Computing.

[10] **Wenqi Wei**, and Ling Liu, "Robust Deep Learning Ensemble against Deception", under the submission of IEEE Transaction on Dependable and Secure Computing.

[9] Mehmet Emre Gursoy, Acar Tamersoy, Stacey Truex, **Wenqi Wei**, and Ling Liu, "Secure and Utility-Aware Data Collection with Condensed Local Differential Privacy", accepted by IEEE Transaction on Dependable and Secure Computing (TDSC), 2019.

[8] **Wenqi Wei**, Ling Liu, Margaret Loper, Ka Ho Chow, Emre Gursoy, Stacey Truex, Yanzhao Wu. "Cross-layer Strategic Ensemble Defense against Adversarial Examples." In International Conference on Computing, Networking and Communications(ICNC), 2020.

[7] Ling Liu,**Wenqi Wei**, Ka-Ho Chow, Margaret Loper, Mehmet Emre Gursoy, Stacey Truex, and Yanzhao Wu, "Deep Neural Network Ensembles against Deception: Ensemble Diversity, Accuracy and Robustness." In the 16th IEEE International Conference on Mobile Ad-Hoc and Smart Systems (MASS), IEEE, 2019.

[6] **Wenqi Wei**, Ling Liu, Margaret Loper, Stacey Truex, Lei Yu, Mehmet Emre Gursoy, and Yanzhao Wu. "Adversarial examples in deep learning: Characterization and divergence." arXiv preprint arXiv:1807.00051 (2018).

[5] Yanzhao Wu, Ling Liu, Calton Pu, Wenqi Cao, Semih Sahin, **Wenqi Wei**, Qi Zhang, "A Comparative Measurement Study of Deep Learning as a Service Framework", accepted by IEEE Transaction on Service Computing (2019).

[4] 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 Transactions on Services Computing (2019).

[3] Mehmet Emre Gursoy, Ling Liu, Stacey Truex, Lei Yu, and **Wenqi Wei**. "Utility-Aware Synthesis of Differentially Private and Attack-Resilient Location Traces." In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 196-211. ACM, 2018.

[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), pp. 1258-1269. IEEE, 2018.

[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(JSAC), 35(2), 463-477,2017. (* equal contribution)