Wenqi Wei

Tenure-Track Assistant Professor
Computer and Information Sciences department
Address: 113 West 60th street, Room 610H, New York, NY 10023
Email: wenqiwei@fordham.edu
Mobile: 404-213-8068
Homepage: https://wenqiwei789.github.io/Homepage/

Education

- **Georgia Institute of Technology** Atlanta, GA
  PhD in Computer Science *Aug. 2017 to May 2022*
  - **Current research areas of Interest**: AI and ML algorithm for big data systems and services; security, privacy, and fairness enhanced ML and AI systems; efficient AI; data mining.
  - **Thesis**: Adversarial Resilient and Privacy Preserving Deep learning
  - **PhD Minor**: Quantitative and Computational Finance with focus on AI-augmented financial data system
- **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

Experience

- **Fordham University** New York, NY
  Computer and Information Sciences Department
  Tenure-Track Assistant Professor (January 2023 - now)
  - **Research**: Delivering AI/privacy/security/fairness solutions to big data systems.
- **IBM Almaden Research Center** San Jose, CA
  Applied Intelligence Department
  Research Staff Member (May 2022 - January 2023)
  - **Project**: Trustworthy foundation models for financial services, Vehicle-IOT collaboration for Smart City, OpenShift for AI-driven Ransomware detection on Cloud.
- **Georgia Institute of Technology** Atlanta, GA
  Distributed Data Intensive Systems Lab *advisor: Ling Liu*
  Graduate Research Assistant (Aug 2017 - May 2022)
  - **AI Privacy**: Research on identifying privacy risks and designing privacy-preserving solutions in AI systems.
  - **AI Security**: Research on identifying and mitigating AI vulnerabilities including poisoning and backdoor at training phase and adversarial example and outlier input at inference phase.
  - **AI Fairness**: Research on eliminating algorithmic bias and improving accountability and transparency of AI.
  - **Machine Learning Services**: Research on ML algorithm and system design, performance measurement, model efficiency (model compression and component design).
  - **Data Mining with Representation Learning**: Research on 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, May 2021 - August 2021)
  - **Project**: Accelerating ransomware detection with graph learning (2020), Graph Neural Networks ensemble learning (2021). 2 patents at USPTO under review.
- **IBM Thomas J. Watson Research Center** Yorktown Heights, NY
  Enterprise Solutions Department
  Research Intern (May 2019 - August 2019)

    - **Project**: Graph representation learning for Bitcoin transaction data mining. Paper published on IEEE TETC.

- **Samsung Research America** Mountain View, CA
  Data Intelligence Group, AI center
  Research Intern (May 2018 - August 2018)
    - **Project**: Computation-efficient deep learning with differential privacy.
- **Huazhong University of Science and Technology** Wuhan, China
  Signal Processing and Information Networking in Communication Lab *advisor: Pan Zhou*
  Undergraduate Research Assistant (Sept 2015 - June 2017)
    - **Privacy-Preserving Networking**: Research on game-theoretic mechanism design with differential privacy for large-scale spectrum sharing while protecting user data privacy.

Publications

[29] Ka-Ho Chow, Ling Liu, **Wenqi Wei**, Fatih Ilhan, Yanzhao Wu. ”STDLens: Securing Federated Learning Against Model Hijacking Attacks.”, IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Vancouver, Canada, June 2023.

[28] Jingya Zhou, Ling Liu, **Wenqi Wei**, and Jianxi Fan “Network Representation Learning: From Preprocessing, Feature Extraction to Node Embedding”, ACM Computing Surveys (ACM CSUR), 2023.

[27] Xigang Sun, Jingya Zhou, Ling Liu, and **Wenqi Wei**, ”Explicit Time Embedding Based Cascade Attention Network for Information Popularity Prediction”, accepted by Information Processing and Management (IP&M), 2023.

[26] **Wenqi Wei**, Mu Qiao, Eric Butler, and Divyesh Jadav. ”Graph Representation Learning based Vulnerable Target Identification in Ransomware Attack.”, IEEE International Conference on Big Data (Big Data), Osaka, Japan, December 2022.

[25] **Wenqi Wei**, and Ling Liu, “Gradient Leakage Attack Resilient Deep Learning”, IEEE Transactions on Information Forensics and Security (IEEE TIFS), vol. 17, pp. 303-316, 2022.

[24] Mehmet Emre Gursoy, Ling Liu, Ka-Ho Chow, Stacey Truex, and **Wenqi Wei**, “An Adversarial Approach to Protocol Analysis and Selection in Local Differential Privacy”, accepted by IEEE Transactions on Information Forensics and Security, 2022.

[23] **Wenqi Wei**, Ling Liu, Yanzhao Wu, Gong Su, and Arun Iyengar, “Gradient-Leakage Resilient Federated Learning”, IEEE International Conference of Distributed Computing Systems (IEEE ICDCS), Washington DC, USA. July, 2021. (virtual)

[22] Yanzhao Wu, Ling Liu, Zhongwei Xie, Ka-Ho Chow, and **Wenqi Wei**. ”Boosting Ensemble Accuracy by Revisiting Ensemble Diversity Metrics”, IEEE/CVF Conference on Computer Vision and Pattern Recognition (IEEE CVPR), Nashville, Tennessee, June, 2021. (virtual)

[21] **Wenqi Wei**, and Ling Liu, “Robust Deep Learning Ensemble against Deception”, IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), 18(4), 1513-1527, 2021.

[20] Mehmet Emre Gursoy, Acar Tamersoy, Stacey Truex, **Wenqi Wei**, and Ling Liu, “Secure and Utility-Aware Data Collection with Condensed Local Differential Privacy”, IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), 18(5), 2365-2378, 2021.

[19] **Wenqi Wei**, Qi Zhang, and Ling Liu, “Bitcoin Transaction Forecasting with Deep Network Representation Learning”, IEEE Transactions on Emerging Topics in Computing (IEEE TETC), 9(3), 1359-1371, 2021.

[18] Stacey Truex, Ling Liu, Emre Gursoy, **Wenqi Wei**, and Ka-Ho Chow. “The TSC-PFed Architecture for Privacy-Preserving FL” IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS), virtual, USA. December 2021.

[17] Huanhuan Xu, Jingya Zhou, **Wenqi Wei**, and Baolei Cheng. “Multi-user Computation Offloading for Long-term Sequential Tasks in MEC Environments” accepted by Tsinghua Science and Technology. 2021.

[16] **Wenqi Wei**, Ling Liu, Margaret Loper, Ka-Ho Chow, Emre Gursoy, Stacey Truex, and Yanzhao Wu. “Cross-layer Strategic Ensemble Defense against Adversarial Examples” International Conference on Computing, Networking and Communications (ICNC), Big Island, Hawaii, USA. February 2020.

[15] **Wenqi Wei**, Ling Liu, Margaret Loper, Ka-Ho Chow, Mehmet Emre Gursoy, Stacey Truex, and Yanzhao Wu. “Adversarial Deception in Deep Learning: Analysis and Mitigation”, IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS), Atlanta, Georgia, USA. December 2020. (virtual)

[14] Stacey Truex, Ling Liu, Ka-Ho Chow, Mehmet Emre Gursoy, and **Wenqi Wei**. “LDP-Fed: Federated Learning with Local Differential Privacy”, ACM International Workshop on Edge Systems, Analytics and Networking (ACM EdgeSys), Heraklion, Crete, Greece. April 2020 (**best paper**). (virtual)

[13] **Wenqi Wei**, Ling Liu, Margaret Loper, Ka-Ho Chow, Mehmet Emre Gursoy, Stacey Truex, and Yanzhao Wu. “A Framework for Evaluating Gradient Leakage Attacks in Federated Learning”, European Symposium on Research in Computer Security (ESORICS), Guildford, UK. September 2020. (virtual)

[12] Ka-Ho Chow, Ling Liu, Mehmet Gursoy, Stacey Truex, **Wenqi Wei** and Yanzhao Wu. “Understanding Object Detection Through An Adversarial Lens”, European Symposium on Research in Computer Security (ESORICS), Guildford, UK. September 2020. (virtual)

[11] Yanzhao Wu, Ling Liu, Zhongwei Xie, Juhyun Bae, Ka-Ho Chow, and **Wenqi Wei**. “Promoting High Diversity Ensemble Learning with EnsembleBench”, IEEE International Conference on Cognitive Machine Intelligence (IEEE CogMI), Atlanta, Georgia, USA. December 2020. (virtual)

[10] Ka-Ho Chow, Ling Liu, Margaret Loper, Mehmet Emre Gursoy, Stacey Truex, **Wenqi Wei** and Yanzhao Wu. “Adversarial Objectness Gradient Attacks on Real-time Object Detection Systems”, IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS), Atlanta, Georgia, USA. December 2020. (virtual)

[9] 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” IEEE International Conference on Mobile Ad-Hoc and Smart Systems (IEEE MASS), Monterey, California, USA. November 2019.

[8] Stacey Truex, Ling Liu, Mehmet Emre Gursoy, **Wenqi Wei**, and Lei Yu, “Effects of Differential Privacy and Data Skewness on Membership Inference Vulnerability” IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS), Los Angeles, California, USA. December 2019.

[7] Ka-Ho Chow, **Wenqi Wei**, Yanzhao Wu, and Ling Liu, “Denoising and Verification Cross-Layer Ensemble Against Black-box Adversarial Attacks” IEEE International Conference on Big Data (IEEE Big Data), Los Angeles, California, USA. December 2019.

[6] 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” IEEE International Conference on Big Data (IEEE Big Data), Los Angeles, California, USA. December 2019.

[5] Yanzhao Wu, Ling Liu, Calton Pu, Wenqi Cao, Semih Sahin, **Wenqi Wei**, and Qi Zhang, “A Comparative Measurement Study of Deep Learning as a Service Framework”, IEEE Transactions on Services Computing (IEEE TSC), 2019.

[4] Stacey Truex, Ling Liu, Mehmet Emre Gursoy, Lei Yu, and **Wenqi Wei**. “Demystifying Membership Inference Attacks in Machine Learning as a Service” IEEE Transactions on Services Computing (IEEE TSC), 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” ACM Conference on Computer and Communications Security (ACM CCS), Toronto, Canada. October 2018.

[2] Ling Liu, Yanzhao Wu, **Wenqi Wei**, Wenqi Cao, Semih Sahin, and Qi Zhang. “Benchmarking deep learning frameworks: Design considerations, metrics and beyond” IEEE International Conference on Distributed Computing Systems (IEEE ICDCS), Vienna, Austria. July 2018.

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

[Patent 1] Mu Qiao, **Wenqi Wei**, Eric Butler, and Divyesh Jadav, “Machine Learning based Vulnerable Target Identification in Ransomware Attack”, US Patent, published June 2022.

Teaching Experience

- Instructor of CISC4080 Computer Algorithms, Fordham University 2023 Spring
- Instructor of CISC5835 Algorithms for Data Science, Fordham University 2023 Spring
- TA of CS6220 Big Data Systems, Georgia Tech 2021 Fall, 2020 Fall, 2019 Fall
- TA of CS6675/CS4675 Advanced Internet Computing, Georgia Tech 2022 Spring, 2019 Spring

Presentation and Talks

- IEEE International Conference on Big Data, Osaka, Japan, Dec. 17-20, 2022. (virtual)
- IEEE International Conference on Distributed Computing Systems, Washington DC, USA, Jul. 7-10, 2021. (virtual)
- IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, Atlanta, GA, USA, Dec. 1-3, 2020. (virtual)
- European Symposium on Research in Computer Security, Guildford, UK, Sep. 14-18, 2020 (virtual).
- IEEE International Conference on Mobile Ad-Hoc and Smart Systems, Monterey, CA, USA. Nov.4-7, 2019.
- Cybersecurity Summit, Institute for Information Security & Privacy, Atlanta, GA, USA, Sep. 10, 2019.
- Cybersecurity Summit, Institute for Information Security & Privacy, Atlanta, GA, USA, Oct. 4, 2018.
- Southern Data Science Conference, Atlanta, GA, USA, Apr. 13-14, 2018.

Services

- **Student volunteer**: ACM FAcct18
- **Conference reviewer/PC**: ICDE18, ICDM (20,21), TheWebConf(21,23), ICLR-DPML21, KDD(21,22,23), MM21, Middleware21, NeurIPS-AI4Science21, ICML-AI4Science22, NeurIPS-ML4H (20,21,22), AAAI(22,23), CVPR(22,23), ECCV22, TPS22, SDM22, NeurIPS(22,23), ICWSM23, IJCAI23, ICCV23
- **Conference chairing**: Publicity chair (CIC/TPS/CogMI22, 23), Session chair (AAAI23), Tutorial co-chair (IEEE Big Data 2023)
- **Journal reviewer**: IEEE TIFS, IEEE TMC, IEEE TNNLS, IEEE ToN, IEEE TNSE, IEEE TSC, IEEE CL, IEEE IoTJ, ACM TOIT, Elsevier JISA, Elsevier CHB, Springer SCIS, Springer ML, SCN