Hongsheng Hu

Faculty of Engineering
University of Auckland
Auckland, New Zealand

+64 21 082 93616
hhu603@aucklanduni.ac.nz

EDUCATION

PhD, Computer Systems Engineering
University of Auckland (UoA), Auckland, New Zealand — Sep 2018 ∼ Present

Bachelor of Science, Mathematics and Statistics
University of Calgary, Calgary, Canada — Jan 2018 ∼ July 2018

Bachelor of Science, Mathematics and Applied Mathematics
China University of Petroleum (East China), Qingdao, China — Sep 2014 ∼ Jan 2018
Thesis: Comparison with survival models with application to head neck and lung cancer

WORK EXPERIENCE

University of Auckland (UoA), New Zealand — 2020 ∼ Present
Graduate Teaching Assistant of Department of Engineering Science.

AWARDS & HONOURS

- University of Auckland Doctoral Scholarship — Sep 2018 ∼ Feb 2022
- China Council Scholarship (Top-1 in the class) — Jan 2018 ∼ July 2018

PROFESSIONAL SERVICES

- Conference Sub-Reviewer
  - IJCAI'22, 21; AAAI'22, 21; ICDM'21 etc.
- Journal Article Reviewer
  - IEEE TII, IEEE TCSS, IEEE IOT, IEEE I-TIS etc.

RESEARCH INTEREST

- Privacy-Preserving Machine Learning; Secure Machine Learning
- Privacy Attacks, especially Membership Inference Attacks
- Federated Learning; Big Data Analytics and Mining; Differential Privacy

PUBLICATIONS

- Conference Papers

[1] **Hongsheng, Hu**, Zoran Salcic, Lichao Sun, Gillian Dobbie, and Xuyun Zhang. "Source Inference Attacks in Federated Learning." In 2021 IEEE International Conference on Data Mining (ICDM), pp. 1102-1107. IEEE, 2021. **(CORE: A*)**

[2] **Hongsheng, Hu**, Gillian Dobbie, Zoran Salcic, Meng Liu, Jianbing Zhang, and Xuyun Zhang. "A Locality Sensitive Hashing Based Approach for Federated Recommender System." In 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID), pp. 836-842. IEEE, 2020. **(CORE: A)**

[3] **Hongsheng, Hu**, Zoran Salcic, Gillian Dobbie, Yi Chen, and Xuyun Zhang. "EAR: an enhanced adversarial regularization approach against membership inference attacks." In 2021 International Joint Conference on Neural Networks (IJCNN), pp. 1-8. IEEE, 2021. **(CORE: A)**

- Journal Articles

[1] **Hongsheng Hu**, Zoran Salcic, Lichao Sun, Gillian Dobbie, Philip S. Yu, and Xuyun Zhang. "Membership inference attacks on machine learning: A survey." ACM Computing Surveys, 2021. **(CORE: A*; IF: 10.2)**

[2] **Hongsheng Hu**, Gillian Dobbie, Zoran Salcic, Meng Liu, Jianbing Zhang, Lingjuan Lyu, and Xuyun Zhang. "Differentially private locality sensitive hashing based federated recommender system." Concurrency and Computation: Practice and Experience (2021): e6233. **(CORE: A)**

[3] **Hongsheng Hu** and Karen Kopciuk. "Comparison of survival models with application to head neck and lung cancers.". Journal of Undergraduate Research in Alberta 7.1 (2019): 23-29. Print. (**Based on the Bachelor Thesis)**

[4] Meng Liu, **Hongsheng Hu**, Haolong Xiang, Chi Yang, Lingjuan Lyu, and Xuyun Zhang. "Clustering-based efficient privacy-preserving face recognition scheme without compromising accuracy." ACM Transactions on Sensor Networks (TOSN) 17, no. 3 (2021): 1-27. **(IF: 3.52)**

- Paper Under Review

[1] **Hongsheng Hu**, Zoran Salcic, Gillian Dobbie, Lichao Sun, Jinjun Chen, and Xuyun Zhang. "Membership inference via backdooring." Under review at 31st International Joint Conference on Artificial Intelligence (IJCAI'22). **(CORE: A*)**

[2] **Hongsheng Hu**, Zoran Salcic, Gillian Dobbie, Lichao Sun, and Xuyun Zhang. "Source Inference Attacks: Beyond Membership Inference Attacks in Federated Learning." Under review at IEEE Transactions on Knowledge and Data Engineering. **(CORE: A*)**

REFEREES

- Prof. Zoran Salcic
  - Relationship: PhD Supervisor
  - Institution: University of Auckland
  - Email: z.salcic@auckland.ac.nz
- Prof. Gillian Dobbie
  - Relationship: PhD Supervisor
  - Institution: University of Auckland
  - Email: g.dobbie@auckland.ac.nz
- Dr. Xuyun Zhang
  - Relationship: PhD Supervisor
  - Institution: Macquarie University
  - Email: xuyun.zhang@mq.edu.au