Ka-Ho Chow

Contact Information	Room 3337, Klaus Advanced Computing Building 266 Ferst Dr, Atlanta, GA, 30332-0765 USA	+1 (404) 368-9674 khchow@gatech.edu

Research Interests: Robust Machine Learning, Cybersecurity, Machine Learning for Systems, Mobile Computing

Education

Georgia Institute of Technology, Atlanta, GA, USA

Ph.D., Computer Science, January 2019 to present

- Advisor: Prof. Ling Liu

Hong Kong University of Science and Technology, Hong Kong

M.Phil., Computer Science, June 2018

- Thesis: Efficient Locality Classification for Indoor Fingerprint-based Systems
- Advisor: Prof. S.-H. Gary Chan

B.Eng., Computer Science, June 2016

Publications

1. **Ka-Ho Chow** and Ling Liu, "Robust Object Detection Fusion Against Deception," ACM SIGKDD Conference on Knowledge Discovery and Data Mining (SIGKDD), Singapore, Aug. 14-18, 2021.
2. **Ka-Ho Chow**, Umesh Deshpande, Sangeetha Seshadri and Ling Liu, "SRA: Smart Recovery Advisor for Cyber Attacks," ACM SIGMOD International Conference on Management of Data (SIGMOD), Xi'an, Shaanxi, China, Jun. 20-25, 2021.
3. 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 (CVPR), Nashville, TN, USA, Jun. 19-25, 2021.
4. **Ka-Ho Chow**, Ling Liu, Margaret Loper, Juhyun Bae, 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 (TPS), Atlanta, GA, USA, Dec. 1-3, 2020.
5. 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 (TPS), Atlanta, GA, USA, Dec. 1-3, 2020.
6. Yanzhao Wu, Juhyun Bae, **Ka-Ho Chow**, Wenqi Wei and Ling Liu, "EnsembleBench: An Evaluation Framework for Ensemble Learning," IEEE International Conference on Cognitive Machine Intelligence (CogMI), Atlanta, GA, USA, Dec. 1-3, 2020.
7. **Ka-Ho Chow**, Ling Liu, Mehmet Emre Gursoy, Stacey Truex, Wenqi Wei and Yanzhao Wu, "Understanding Object Detection Through An Adversarial Lens," European Symposium on Research in Computer Security (ESORICS), Guildford, United Kingdom, Sep. 14-18, 2020.
8. 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, United Kingdom, Sep. 14-18, 2020.

9. 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 (EdgeSys), Heraklion, Crete, Greece, Apr. 27, 2020. [Best Paper Award]

10. Wenqi Wei, Ling Liu, Margaret Loper, **Ka-Ho Chow**, Emre Gursoy, Stacey Truex and Yanzhao Wu, "Cross-Layer Strategic Ensemble Defense Against Adversarial Examples," IEEE International Conference on Computing, Networking and Communications (ICNC), Big Island, Hawaii, USA, Feb. 17-20, 2020.

11. Lei Yu, Ling Liu, Calton Pu, **Ka-Ho Chow**, Emre Gursoy, Stacey Truex, Wenqi Wei, Ming Hong, Arun Iyengar, Gong Su, Qi Zhang and Donna Dillenberger, "GRAHIES: Multi-Scale Graph Representation Learning with Latent Hierarchical Structure," IEEE International Conference on Cognitive Machine Intelligence (CogMI), Los Angeles, CA, USA, Dec. 12-14, 2019.

12. **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, Los Angeles, CA, USA, Dec. 9-12, 2019.

13. Yanzhao Wu, Ling Liu, Juhyun Bae, **Ka-Ho Chow**, Arun Iyengar, Calton Pu, Wenqi Wei, Lei Yu and Qi Zhang, "Demystifying Learning Rate Policies for High Accuracy Training of Deep Neural Networks," IEEE International Conference on Big Data, Los Angeles, CA, USA, Dec. 9-12, 2019.

14. Ling Liu, Wenqi Wei, **Ka-Ho Chow**, Margaret Loper, 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 (MASS), Monterey, CA, USA, Nov. 4-7, 2019.

15. **Ka-Ho Chow**, Suining He, Jiajie Tan and Shueng-Han Gary Chan, "Efficient Locality Classification for Indoor Fingerprint-based Systems," IEEE Transactions on Mobile Computing (TMC), Vol. 18, No. 2, pp. 290-304, February 2019.

16. **Ka-Ho Chow**, Anish Hiranandani, Yifeng Zhang and Shueng-Han Gary Chan, "Representation Learning of Pedestrian Trajectories Using Actor-Critic Sequence-to-Sequence Autoencoder."

Research Experience

Graduate Research Assistant — January 2019 to present
Distributed Data Intensive Systems Lab
School of Computer Science
Georgia Institute of Technology
Supervisor: Prof. Ling Liu

Research Intern — Summer 2021, Summer 2020
Storage Systems Research Group
IBM Research - Almaden
Supervisor: Dr. Umesh Deshpande, Dr. Wil Plouffe, Dr. Sangeetha Seshadri

Research Assistant — June 2015 to December 2018
Multimedia Technology Research Center,
Department of Computer Science and Engineering
Hong Kong University of Science and Technology
Supervisor: Prof. S.-H. Gary Chan

Work Experience

Engineering Intern — May 2019 to August 2019
SagaDigits Group, Hong Kong

Mobile Application Developer — June 2014 to May 2015
Code Free Soft Limited, Hong Kong

Teaching Experience

Graduate Teaching Assistant
School of Computer Science
Georgia Institute of Technology

- CS 6220 - Big Data Systems and Analytics — Fall 2019, Fall 2020
  Instructor: Prof. Ling Liu

Graduate Teaching Assistant
Department of Computer Science and Engineering
Hong Kong University of Science and Technology

- COMP 2012 - Object-Oriented Programming and Data Structures — Spring 2018
  Instructor: Prof. S.-H. Gary Chan
- COMP 1021 - Introduction to Computer Science — Spring 2017
  Instructor: Dr. David Rossiter
- COMP 1029P - Python Programming Bridging Course — Fall 2016
  Instructor: Dr. Gibson Lam

Achievements

- Croucher Scholarship for Doctoral Study, 2021-2022
- Best Paper Award, ACM International Workshop on Edge Systems, Analytics and Networking, 2020
- Student Travel Award, IEEE International Conference on Big Data, 2019
- Chair's Fellowship, Georgia Tech, 2019
- Postgraduate Studentship, HKUST, 2016-2017, 2017-2018
- Dean's List, HKUST, 2015-2016
- Hang Lung: Chan Tseng-Hsi Foundation, Hong Kong, 2013-2014
- Sir Edward Youde Memorial Prize, Hong Kong, 2009-2010

Reviewer

- IEEE/CVF Conference on Computer Vision and Pattern Recognition — 2021
- Machine Learning for Health Workshop at NeurIPS — 2020
- ACM Transactions on Internet Technology
- IEEE Transactions on Mobile Computing
- IEEE International Conference on Computer Communications — 2017, 2018
- MDPI ISPRS International Journal of Geo-Information
- MDPI Sensors