Clement **Fung**

PhD Student · Carnegie Mellon University

✉ clementf@andrew.cmu.edu | clementfung.me | clementfung | clfung | Clement Fung

Education

Carnegie Mellon University, School of Computer Science *Pittsburgh, PA, USA*

Ph.D in Societal Computing, Software and Societal Systems Department (GPA: 4.0 / 4.33) *08/2019 - present*

- Thesis (proposed):
  - Proposing Guidelines and Approaches to Make Anomaly Detection More Effective for Industrial Control Systems
    Advisor: Lujo Bauer
- Research Projects:
  - ICS-ML: Improving detection and attribution for ML-based ICS anomaly detection *(NDSS '24, ESORICS '22)*
  - DOM-XSS-ML: A hybrid, ML-based system to detect DOM-XSS with reduced overhead *(WWW '21)*

University of British Columbia *Vancouver, BC, Canada*

M.Sc in Computer Science (GPA: 88 / 100) *09/2016 - 12/2018*

- Thesis:
  - Dancing in the dark: Private Multi-Party Machine Learning in an Untrusted Setting
    Advisor: Ivan Beschastnikh
- Research Projects:
  - Biscotti: A secure, private blockchain-based system for multi-party ML *(TPDS '21)*
  - FoolsGold: A sybil-resilient federated learning protocol against model poisoning *(RAID '20)*
  - TorMentor: A system for distributed, collaborative, anonymous ML *(ApSys '19)*

University of Waterloo *Waterloo, ON, Canada*

B.A.Sc in Systems Design Engineering, Honours (GPA: 88 / 100) *09/2011 - 05/2016*

- Capstone Project:
  - Driven: An Automated System for Intelligent Annotation and Analysis of Lane Change Sentiment
    Advisor: Alexander Wong

Publications

Refereed publications

Targeted Image Transformation for Improving Robustness in Long Range Aircraft Detection *IROS 2024*
Rebecca Martin, Clement Fung, Nikhil Varma Keetha, Lujo Bauer, Sebastian Scherer. *Abu Dhabi, UAE*
To appear in *2024 IEEE/RSJ International Conference on Intelligent Robots and Systems.*

Attributions for ML-based ICS Anomaly Detection: From Theory to Practice *NDSS 2024*
Clement Fung, Eric Zeng, Lujo Bauer. *San Diego, CA, USA*
31st Network and Distributed System Security Symposium.

Perspectives from a Comprehensive Evaluation of Reconstruction-based Anomaly Detection in Industrial Control Systems *ESORICS 2022*
Clement Fung, Shreya Srinarasi, Keane Lucas, Hay Bryan Phee, Lujo Bauer. *Copenhagen, Denmark*
27th European Symposium on Research in Computer Security.

Biscotti: A Blockchain System for Private and Secure Federated Learning *TPDS 2021*
Muhammad Shayan, Clement Fung, Chris J.M. Yoon, Ivan Beschastnikh.
IEEE Transactions on Parallel and Distributed Systems, Volume 32, Issue 7.

Towards a Lightweight, Hybrid Approach for Detecting DOM XSS Vulnerabilities with Machine Learning *WWW 2021*
William Melicher, Clement Fung, Lujo Bauer, Limin Jia. *Ljubjana, Slovenia (Virtual)*
The Web Conference 2021.

The Limitations of Federated Learning in Sybil Settings *RAID 2020*
Clement Fung, Chris J.M Yoon, Ivan Beschastnikh. *San Sebastian, Spain (Virtual)*
23rd International Symposium on Research in Attacks, Intrusions and Defenses.

Brokered Agreements in Multi-Party Machine Learning *APSys 2019*
Clement Fung, Ivan Beschastnikh. *Hangzhou, China*
10th ACM SIGOPS Asia-Pacific Workshop on Systems.

GainForest: Scaling Climate Finance for Forest Conservation using Interpretable Machine Learning on Satellite Imagery *ICML 2019 Workshop*
Long Beach, CA, USA
David Dao, Catherine Cang, Clement Fung, Ming Zhang, Nick Pawlowski, Reuven Gonzales, Nick Beglinger, Ce Zhang
Climate Change: How Can AI Help?: ICML 2019 Workshop

Pre-prints

Model Selection of Anomaly Detectors in the Absence of Labeled Validation Data *ArXiv 2023*
Clement Fung, Chen Qiu, Aodong Li, Maja Rudolph.
ArXiv Preprint: 2310.10461

Dancing in the Dark: Private Multi-Party Machine Learning in an Untrusted Setting *ArXiv 2018*
Clement Fung, Jamie Koerner, Stewart Grant, Ivan Beschastnikh.
ArXiv Preprint: 1811.09712

Mitigating Sybils in Federated Learning Poisoning *ArXiv 2018*
Clement Fung, Chris J.M. Yoon, Ivan Beschastnikh.
ArXiv Preprint: 1808.04866

Professional Experience

Bosch Center for Artificial Intelligence *Pittsburgh, PA, USA*
Machine Learning Research Intern *05/2023 - 08/2023*
- Research on applications of diffusion models to anomaly detection

Oasis Labs *Berkeley, CA, USA*
Software Engineer *01/2019 - 07/2019*
- Developer for secure data sharing platform and other confidential use cases in an early-stage blockchain startup

LinkedIn Corporation *Sunnyvale, CA, USA*
Software Engineering Intern *06/2015 - 08/2015*
- Search, Network, and Analytics Team: Building infrastructure for online relevance scoring at scale

LinkedIn Corporation *Mountain View, CA, USA*
Software Engineering Intern *09/2014 - 12/2014*
- Distributed Data Systems Team: Prototyped and designed a new derived-data serving system, Venice

Voicebox Technologies *Bellevue, WA, USA*
Software Engineering Intern *01/2014 - 04/2014*
- Server and Tools Team: Implemented layer for concurrent database access on a mobile service

Ontario Institute for Cancer Research *Toronto, ON, Canada*
Software Developer Intern *05/2013 - 08/2013*
- Software developer in Prof. Paul Boutros' bioinformatics research group

Teaching

Carnegie Mellon University
Teaching Assistant
- 11-667: Large Language Models Methods and Applications Fall 2023
  Instructors: Daphne Ippolito, Chenyan Xiong

University of British Columbia
Teaching Assistant
- DSCI 571: Supervised Learning Fall 2018
  Instructors: Michael Gelbart, Varada Kolhatkar
- DSCI 523: Data Wrangling Fall 2018
  Instructors: Jenny Bryan, Rodolfo Lourenzutti
- CPSC 340: Machine Learning Winter 2018
  Instructor: Michael Gelbart
- CPSC 340: Machine Learning Fall 2017
  Instructor: Mark Schmidt
- CPSC 210: Software Construction Winter 2017
  Instructors: Norman Hutchinson, Paul Carter, Mehrdad Oveisi
- CPSC 210: Software Construction Fall 2016
  Instructors: Norman Hutchinson, Ryan Vogt, Jonatan Schroeder

Service

Academic Service

Program Committee

- WISW 2024
- ACM FAccT 2023
- ACM FAccT 2022

External Reviewer

- USENIX Security 2024 (4x)
- IEEE S&P 2024
- IEEE SaTML 2024 (2x)
- USENIX Security 2023 (2x)
- USENIX Security 2022
- IEEE S&P 2021
- NDSS 2021 (2x)
- USENIX Security 2020
- SOUPS 2020
- ISSRE 2017

Invited Reviewer

- IEEE Trans. Networking 2024
- ACM CCS Posters 2021
- IEEE Trans. Industrial Informatics 2021

Committees and Volunteering

CMU Software and Societal Systems Department

- Student Representative for Faculty Meetings, 2024
- PhD Student Admissions Committee, 2023
- Faculty Hiring Committee, 2022
- Community Building Committee, 2022–2023
- Prospective PhD Student Visit Day Organizer, 2020–2022

CMU CyLab

- CyLab Sporting Committee, 2021–2023

UBC Department of Computer Science

- President of the Computer Science Graduate Student Association, 2017
- Department Strategy Committee, 2017
- Space and Safety Committee, 2017

Academic Conference Volunteer

- WOSOC 2024
- SOUPS 2021
- EuroS&P 2021
- EuroS&P 2020

Awards

2024	**AINet Fellow in “Safety and Security of AI”**	Deutscher Akademischer Austauschdienst (DAAD)
2017	**CS Department Graduate Teaching Assistant Award**	University of British Columbia
2017	**CS Department Student Service Award**	University of British Columbia
2016	**Sanford Fleming Award for Co-operative Proficiency**	University of Waterloo
2016	**GM Canada Innovation Award** *($500)*	University of Waterloo
2015	**W.W. King Exchange Fellowship** *($500)*	University of Waterloo
2014	**President’s International Experience Award** *($1500)*	University of Waterloo
2013	**Sanford Fleming Award for Outstanding Work Term Report** *($300)*	University of Waterloo
2011	**Colonel Hugh Heasley Engineering Scholarship** *($10000)*	University of Waterloo
2011	**President’s Scholarship of Distinction** *($2000)*	University of Waterloo
Winter 2016	**Dean’s Honour’s List,** *Class Rank Unknown*	University of Waterloo
Winter 2013	**Dean’s Honour’s List,** *Class Rank 2/81*	University of Waterloo
Spring 2012	**Dean’s Honour’s List,** *Class Rank 2/85*	University of Waterloo
Fall 2011	**Dean’s Honour’s List,** *Class Rank 3/94*	University of Waterloo