

Clement Fung

PHD CANDIDATE · CARNEGIE MELLON UNIVERSITY

✉ clementf@andrew.cmu.edu | 🏠 clementfung.me | 📧 clementfung | 📺 clfung | 📱 Clement Fung

Education

Carnegie Mellon University, School of Computer Science

PH.D IN SOCIETAL COMPUTING, SOFTWARE AND SOCIETAL SYSTEMS DEPARTMENT (GPA: 4.0 / 4.33)

- Thesis (proposed):
 - Proposing Guidelines and Approaches to Make Anomaly Detection More Effective for Industrial Control SystemsAdvisor: Lujo Bauer

Pittsburgh, PA, USA

08/2019 - present

University of British Columbia

M.SC IN COMPUTER SCIENCE (GPA: 88 / 100)

- Thesis:
 - Dancing in the dark: Private Multi-Party Machine Learning in an Untrusted SettingAdvisor: Ivan Beschastnikh

Vancouver, BC, Canada

09/2016 - 12/2018

University of Waterloo

B.A.SC IN SYSTEMS DESIGN ENGINEERING, HONOURS (GPA: 88 / 100)

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

Waterloo, ON, Canada

09/2011 - 05/2016

Publications

REFEREED PUBLICATIONS

Adopting AI to Protect Industrial Control Systems: Assessing Challenges and Opportunities from the Operators' Perspective

Clement Fung, Eric Zeng, Lujo Bauer.
21st Symposium on Usable Privacy and Security.

SOUPS 2025

Seattle, WA, USA

Model Selection of Anomaly Detectors in the Absence of Labeled Validation Data

Clement Fung, Chen Qiu, Aodong Li, Maja Rudolph.
IEEE Transactions on Artificial Intelligence.

TAI 2025

Targeted Image Transformation for Improving Robustness in Long Range Aircraft Detection

Rebecca Martin, Clement Fung, Nikhil Varma Keetha, Lujo Bauer, Sebastian Scherer.
2024 IEEE/RSJ International Conference on Intelligent Robots and Systems.

IROS 2024

Abu Dhabi, UAE

Attributions for ML-based ICS Anomaly Detection: From Theory to Practice

Clement Fung, Eric Zeng, Lujo Bauer.
31st Network and Distributed System Security Symposium.

NDSS 2024

San Diego, CA, USA

Perspectives from a Comprehensive Evaluation of Reconstruction-based Anomaly Detection in Industrial Control Systems

Clement Fung, Shreya Srinarasi, Keane Lucas, Hay Bryan Phee, Lujo Bauer.
27th European Symposium on Research in Computer Security.

ESORICS 2022

Copenhagen, Denmark

Biscotti: A Blockchain System for Private and Secure Federated Learning

Muhammad Shayan, Clement Fung, Chris J.M. Yoon, Ivan Beschastnikh.
IEEE Transactions on Parallel and Distributed Systems, Volume 32, Issue 7.

TPDS 2021

Towards a Lightweight, Hybrid Approach for Detecting DOM XSS Vulnerabilities with Machine Learning

William Melicher, Clement Fung, Lujo Bauer, Limin Jia.
The Web Conference 2021.

WWW 2021

Ljubljana, Slovenia (Virtual)

The Limitations of Federated Learning in Sybil Settings

Clement Fung, Chris J.M Yoon, Ivan Beschastnikh.
23rd International Symposium on Research in Attacks, Intrusions and Defenses.

RAID 2020

San Sebastian, Spain (Virtual)

Brokered Agreements in Multi-Party Machine Learning

Clement Fung, Ivan Beschastnikh.
10th ACM SIGOPS Asia-Pacific Workshop on Systems.

APSys 2019

Hangzhou, China

GainForest: Scaling Climate Finance for Forest Conservation using Interpretable Machine Learning on Satellite Imagery

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

ICML 2019 Workshop

Long Beach, CA, USA

OTHER

Dancing in the Dark: Private Multi-Party Machine Learning in an Untrusted Setting

Clement Fung, Jamie Koerner, Stewart Grant, Ivan Beschastnikh.

ArXiv Preprint: 1811.09712

ArXiv 2018

Mitigating Sybils in Federated Learning Poisoning

Clement Fung, Chris J.M. Yoon, Ivan Beschastnikh.

ArXiv Preprint: 1808.04866

ArXiv 2018

Teaching

Carnegie Mellon University

TEACHING ASSISTANT

- 17-331: Information Security, Privacy, and Policy Instructor: Norman Sadeh Fall 2024
- 11-667: Large Language Models Methods and Applications Instructors: Daphne Ippolito, Chenyan Xiong Fall 2023

FUTURE FACULTY PROGRAM, EBERLY CENTER FOR TEACHING EXCELLENCE AND EDUCATIONAL INNOVATION

- Completed a program that prepares graduate students for teaching in future faculty careers 2024
- Designed a course syllabus, taught two guest lectures, and participated in nine teaching seminars

University of British Columbia

TEACHING ASSISTANT

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

Professional Experience

Bosch Center for Artificial Intelligence

MACHINE LEARNING RESEARCH INTERN

- Research on applications of diffusion models to anomaly detection

Pittsburgh, PA, USA

05/2023 - 08/2023

Oasis Labs

SOFTWARE ENGINEER

- Developing a secure, private, data-sharing platform in an early-stage blockchain startup

Berkeley, CA, USA

01/2019 - 07/2019

LinkedIn Corporation

SOFTWARE ENGINEERING INTERN

- Search, Network, and Analytics Team: Building infrastructure for online ML-based relevance scoring at scale

Sunnyvale, CA, USA

06/2015 - 08/2015

LinkedIn Corporation

SOFTWARE ENGINEERING INTERN

- Distributed Data Systems Team: Designed and prototyped a derived-data serving system, Venice

Mountain View, CA, USA

09/2014 - 12/2014

Voicebox Technologies

SOFTWARE ENGINEERING INTERN

- Server and Tools Team: Developed concurrent database access layer for a mobile voice-assistant service

Bellevue, WA, USA

01/2014 - 04/2014

Ontario Institute for Cancer Research

SOFTWARE DEVELOPER INTERN

- Developer for the Boutros Lab: a bio-informatics research group

Toronto, ON, Canada

05/2013 - 08/2013

External Service

PROGRAM COMMITTEE

- ISC 2025
- RAID 2025
- 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. Information Forensics & Security 2025 (2x)
- Springer Machine Learning 2025
- IEEE Trans. Networking 2024
- ACM CCS Posters 2021
- IEEE Trans. Industrial Informatics 2021

CONFERENCE VOLUNTEER

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

Internal Service

CMU SOFTWARE AND SOCIETAL SYSTEMS DEPARTMENT

- Student Representative for Faculty Meetings, 2024–2025
- 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 Sports Committee, 2021–2023

UBC DEPARTMENT OF COMPUTER SCIENCE

- Computer Science Graduate Student Association (President), 2017
- Department Strategy Committee, 2017
- Space and Safety Committee, 2017

Awards and Honors

2024	Best Poster Award (\$300)	IAP CMU Workshop: AI and Security in the Cloud
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