

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

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

Pittsburgh, PA, USA

08/2019 - present

- Research projects:
 - ICS-ML: Explainable machine-learning-based anomaly detection for industrial control systems
 - DOM-XSS-ML: A hybrid, machine-learning-based system to detect DOM-XSS with reduced overhead
- Graduate Courses:
 - 17-881 - Sensing and Internet-of-Things (Prof. Yuvraj Agarwal)
 - 17-737 - Artificial Intelligence Methods for Social Good (Prof. Fei Fang)
 - 18-731 - Network Security (Prof. Vyas Sekar)
 - 17-762 - Law of Computer Technology (Prof. Michael Shamos)
 - 36-700 - Probability and Mathematical Statistics (Prof. Valerie Ventura)
 - 18-739 - Security and Fairness of Deep Learning (Prof. Piotr Mardziel)
 - 18-730 - Introduction to Computer Security (Prof. Virgil Gligor)

University of British Columbia

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

Vancouver, BC, Canada

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 machine learning
 - FoolsGold: A sybil-resilient federated learning protocol against model poisoning
 - TorMentor: A system for distributed, collaborative, anonymous machine learning
- Graduate Courses:
 - CPSC 532R - Graphical Models (Prof. Siamak Ravanbakhsh)
 - CPSC 540 - Advanced Machine Learning (Prof. Mark Schmidt)
 - CPSC 538W - Data At Scale (Prof. Andrew Warfield)
 - CPSC 538B - Distributed Systems (Prof. Ivan Beschastnikh)
 - CPSC 536F - Algorithmic Game Theory (Prof. Hu Fu)
 - CPSC 340 - Machine Learning (Prof. Mark Schmidt)

University of Waterloo

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

Waterloo, ON, Canada

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

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

Clement Fung, Eric Zeng, Lujo Bauer.

To appear at the 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 2022

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

Ljubjana, 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

PRE-PRINTS

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

Clement Fung, Chen Qiu, Aodong Li, Maja Rudolph.

ArXiv Preprint: 2310.10461

ArXiv 2023

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

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

- Secure data sharing and other confidential use cases in an early stage blockchain startup.

Berkeley, CA, USA

01/2019 - 07/2019

LinkedIn Corporation

SOFTWARE ENGINEERING INTERN

- Analytics: Building infrastructure for online relevance scoring at scale

Sunnyvale, CA, USA

06/2015 - 08/2015

LinkedIn Corporation

SOFTWARE ENGINEERING INTERN

- Distributed Data Systems: Prototyped and designed new derived data serving system, Venice

Mountain View, CA, USA

09/2014 - 12/2014

Voicebox Technologies

SOFTWARE ENGINEERING INTERN

- Server and Tools: Implemented layer for concurrent database access on a mobile service

Bellevue, WA, USA

01/2014 - 04/2014

Ontario Institute for Cancer Research

SOFTWARE DEVELOPER INTERN

- Software developer in Prof. Paul Boutros' bioinformatics research group

Toronto, ON, Canada

05/2013 - 08/2013

Teaching

Carnegie Mellon University

TEACHING ASSISTANT

- 11-667: Large Language Models Methods and Applications
Instructors: Daphne Ippolito, Chenyan Xiong

Fall 2023

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

2022 - 2023	Program Committee	ACM FAccT 2023, 2022 IEEE S&P 2024, 2021
2019 - 2023	External Reviewer	USENIX Security 2024, 2023, 2022, 2020 IEEE SaTML 2024 NDSS 2021 SOUPS 2020
2021	Invited Reviewer	IEEE Transactions on Industrial Informatics 2021 ACM CCS Posters 2021

ORGANIZATIONAL SERVICE

2023	PhD Student Admissions Committee	Software and Societal Systems Department
2022	Faculty Hiring Committee	Software and Societal Systems Department
2022 - 2023	Community Building Committee	Software and Societal Systems Department
2020 - 2022	Prospective PhD Visit Day Organizer	Software and Societal Systems Department
2020 - 2021	Academic Conference Volunteer	SOUPS 2021, Euro S&P 2021, Euro S&P 2020

Awards

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