

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

- Research projects:
 - ICS-ML: Attributions for ML-based anomaly detection for industrial control systems (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

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.

Ljubljana, 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

David Dao, Catherine Cang, Clement Fung, Ming Zhang, Nick Pawlowski, Reuven Gonzales, Nick Beglinger, Ce Zhang

Long Beach, CA, USA

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

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

- Developer for secure data sharing platform and other confidential use cases 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 relevance scoring at scale

Sunnyvale, CA, USA

06/2015 - 08/2015

LinkedIn Corporation

SOFTWARE ENGINEERING INTERN

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

Mountain View, CA, USA

09/2014 - 12/2014

Voicebox Technologies

SOFTWARE ENGINEERING INTERN

- Server and Tools Team: 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
Instructors: Michael Gelbart, Varada Kolhatkar
- DSCI 523: Data Wrangling
Instructors: Jenny Bryan, Rodolfo Lourenzutti
- CPSC 340: Machine Learning
Instructor: Michael Gelbart
- CPSC 340: Machine Learning
Instructor: Mark Schmidt
- CPSC 210: Software Construction
Instructors: Norman Hutchinson, Paul Carter, Mehrdad Oveisi
- CPSC 210: Software Construction
Instructors: Norman Hutchinson, Ryan Vogt, Jonatan Schroeder

Fall 2018

Fall 2018

Winter 2018

Fall 2017

Winter 2017

Fall 2016

Academic Service

PROGRAM COMMITTEE

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

Committees and Volunteering

CMU SOFTWARE AND SOCIETAL SYSTEMS DEPARTMENT

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

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

- SOUPS 2021
- EuroS&P 2021
- EuroS&P 2020

Awards

2024	AINet Fellow in “Safety and Security of AI”	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