

# 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)

- 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

#### Targeted Image Transformation for Improving Robustness in Long Range Aircraft Detection

Rebecca Martin, Clement Fung, Nikhil Varma Keetha, Lujo Bauer, Sebastian Scherer.

To appear in 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

### 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

## 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

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

Fall 2024

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 Oveis
- CPSC 210: Software Construction  
Instructors: Norman Hutchinson, Ryan Vogt, Jonatan Schroeder

Fall 2018

Fall 2018

Winter 2018

Fall 2017

Winter 2017

Fall 2016

## Service

### External 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

#### 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
- 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

## Awards

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