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, INSTITUTE FOR SOFTWARE RESEARCH (GPA: 4.0 / 4.33) *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 *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 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 *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

NDSS 2024
San Diego, CA, USA

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.*

ESORICS 2022
Copenhagen, Denmark

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.

TPDS 2022

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.

WWW 2021
Ljubjana, Slovenia (Virtual)

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.

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

LinkedIn Corporation *Sunnyvale, CA, USA*
SOFTWARE ENGINEERING INTERN *06/2015 - 08/2015*
- Analytics: Building infrastructure for online relevance scoring at scale

LinkedIn Corporation *Mountain View, CA, USA*
SOFTWARE ENGINEERING INTERN *09/2014 - 12/2014*
- Distributed Data Systems: Prototyped and designed new derived data serving system, Venice

Voicebox Technologies *Bellevue, WA, USA*
SOFTWARE ENGINEERING INTERN *01/2014 - 04/2014*
- Server and Tools: 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 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

Service

ACADEMIC SERVICE

2022 - 2023	**Program Committee**	ACM FAccT 2023, 2022
2019 - 2023	**External Reviewer**	IEEE S&P 2024, 2021 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**	Institute for Software Research
2022	**Faculty Hiring Committee**	Institute for Software Research
2022 - 2023	**Community Building Committee**	Institute for Software Research
2020 - 2022	**Prospective PhD Visit Day Organizer**	Institute for Software Research
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