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: 3.94 / 4) — *08/2019 - present*

- Research projects:
  - ICS-ML: Explainable and robust machine-learning-based anomaly detection for industrial control systems
  - DOM-XSS-ML: A hybrid, machine learning system to detect DOM-XSS with reduced overhead

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
    Supervisor: 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
  - InsuLearn: A system for distributed learning on private medical data
  - DistributedClocks: A library for vector clock instrumentation of distributed systems

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
    Supervisor: Alexander Wong

Publications

Refereed publications

Perspectives from a Comprehensive Evaluation of Reconstruction-based Anomaly Detection in Industrial Control Systems — *ESORICS 2022*, *Copenhagen, Denmark*

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

Biscotti: A Blockchain System for Private and Secure Federated Learning — *TPDS 2022*

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*, *Ljubjana, Slovenia (Virtual)*

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

The Limitations of Federated Learning in Sybil Settings — *RAID 2020*, *San Sebastian, Spain (Virtual)*

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

Brokered Agreements in Multi-Party Machine Learning — *APSys 2019*, *Hangzhou, China*

Clement Fung, Ivan Beschastnikh.
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*, *Long Beach, CA, USA*

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

Pre-prints

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

Carnegie Mellon University *Pittsburgh, PA, USA*
Research Assistant *08/2019 - present*
- Research on machine learning, security and the industrial internet-of-things in CyLab.

Oasis Labs *Berkeley, CA, USA*
Software Engineer *01/2019 - 07/2019*
- Developed applications for secure data sharing and other confidential use cases in an early stage blockchain startup.

University of British Columbia *Vancouver, BC, Canada*
Research Assistant *01/2017 - 12/2018*
- Research on the security of machine learning systems in the Networks, Systems and Security (NSS) Lab.

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 Paul Boutros' bioinformatics research group

Teaching

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

Organizational Service

2022	**Community Building Committee**	Institute for Software Research
2022	**Faculty Hiring Committee**	Institute for Software Research
2020-2022	**Prospective PhD Visit Day Organizer**	Institute for Software Research
2021	**Student Volunteer**	SOUPS 2021
2021	**Student Volunteer**	IEEE Euro S&P 2021
2020	**Student Volunteer**	IEEE Euro S&P 2020

Academic Service

2022	**External Reviewer**	USENIX Security 2023
2022	**Program Committee**	ACM FAccT 2022
2021	**External Reviewer**	USENIX Security 2022
2021	**External Reviewer**	ACM CCS 2021 Posters
2021	**External Reviewer**	IEEE Security and Privacy (S&P) 2021
2021	**Invited Reviewer**	IEEE Transactions on Industrial Informatrics 2021
2021	**External Reviewer** *(2x)*	NDSS 2021
2020	**External Reviewer**	SOUPS 2020
2019	**External Reviewer**	USENIX Security 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,** *Rank Unknown*	University of Waterloo
Winter 2013	**Dean's Honour's List,** *Rank 2/81*	University of Waterloo
Spring 2012	**Dean's Honour's List,** *Rank 2/85*	University of Waterloo
Fall 2011	**Dean's Honour's List,** *Rank 3/94*	University of Waterloo