

# Clement Fung

[✉ clementf@andrew.cmu.edu](mailto:clementf@andrew.cmu.edu) | [🏡 clementfung.me](http://clementfung.me) | [🌐 clementfung](https://clementfung.com) | [💻 clfung](https://clfung.com) | [🎓 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:

- Proposing Guidelines and Approaches to Make Anomaly Detection More Effective for Industrial Control Systems  
Advisor: Lujo Bauer

Pittsburgh, PA, USA

08/2019 - 09/2025

### 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 Setting  
Advisor: 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 Sentiment  
Advisor: Alexander Wong

Waterloo, ON, Canada

09/2011 - 05/2016

## Research

### REFEREED PUBLICATIONS

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

TAI 2025

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

*IEEE Transactions on Artificial Intelligence, Volume 6, Issue 12.*

#### Adopting AI to Protect Industrial Control Systems: Assessing Challenges and Opportunities from the Operators' Perspective

SOUPS 2025

Seattle, WA, USA

Clement Fung, Eric Zeng, Lujo Bauer.

*21st Symposium on Usable Privacy and Security.*

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

IROS 2024

Abu Dhabi, UAE

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

*2024 IEEE/RSJ International Conference on Intelligent Robots and Systems.*

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

NDSS 2024

San Diego, CA, USA

Clement Fung, Eric Zeng, Lujo Bauer.

*31st Network and Distributed System Security Symposium.*

#### 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.

*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

Ljubljana, 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*

## OTHER PUBLICATIONS

### Attacking Autonomous Driving Agents with Adversarial Machine Learning: A Holistic Evaluation with the CARLA Leaderboard

ArXiv 2025

Henry Wong, Clement Fung, Weiran Lin, Karen Li, Stanley Chen, Lujo Bauer.

ArXiv Preprint: 2511.14876

### 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

## INVITED TALKS

### Adopting AI to Protect Industrial Control Systems: Assessing Challenges and Opportunities from the Operators' Perspective

- CyLab Partners Conference. October 2025.
- RSTCON 2025. October 2025.
- Symposium on Usable Privacy and Security (SOUPS). August 2025.

### Approaches for More Effective ML-based Anomaly Detection in Industrial Control Systems

- Secure Cyber-Physical Systems Group, CISPA Helmholtz Center for Information Security. October 2024.
- SysNets Seminar, Max Planck Institute for Software Systems. October 2024.
- Artificial Intelligence and Security Group, Karlsruhe Institute of Technology. October 2024.
- CAE-R Research Symposium, National Cybersecurity Education Colloquium. October 2024.

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

- RSTCON 2025. October 2025.
- Network and Distributed System Security Symposium (NDSS). February 2024.

### Perspectives from a Comprehensive Evaluation of Reconstruction-based Anomaly Detection in Industrial Control Systems

- CAE-R Seminar, April 2023.
- European Symposium on Research in Computer Security (ESORICS). September 2022.

### Detecting and Explaining Anomalies in Industrial Control

- Bosch Center for Artificial Intelligence. June 2023.
- Accountable Systems Lab, Carnegie Mellon University. November 2022.
- CyLab Partners Conference. October 2022.

### Towards a Lightweight, Hybrid Approach for Detecting DOM XSS Vulnerabilities with Machine Learning

- The Web Conference. April 2021.

### The Limitations of Federated Learning in Sybil Settings

- Symposium on Research in Attacks, Intrusions and Defenses (RAID). October 2020.

### Brokered Agreements in Multi-Party Machine Learning

- Asia-Pacific Workshop on Systems (APSys). August 2019.

### Dancing in the Dark: Private Multi-Party Machine Learning in an Untrusted Setting

- UBC Cybersecurity Summit. May 2018.
- Computer Systems Lab Seminar, University of Toronto. December 2017.

## Teaching and Mentoring

---

### TEACHING

#### Carnegie Mellon University

##### TEACHING ASSISTANT

- |   |           |
|---|-----------|
| • 17-331: Information Security, Privacy, and Policy<br>Instructor: Norman Sadeh                         | Fall 2024 |
| • 11-667: Large Language Models Methods and Applications<br>Instructors: Daphne Ippolito, Chenyan Xiong | Fall 2023 |

##### FUTURE FACULTY PROGRAM, EBERLY CENTER FOR TEACHING EXCELLENCE AND EDUCATIONAL INNOVATION

- |   |      |
|---|------|
| • Completed a program that prepares graduate students for teaching in future faculty careers        | 2024 |
| • Designed a course syllabus, taught two guest lectures, and participated in nine teaching seminars |      |

## **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 Oveis Fall 2017
- CPSC 210: Software Construction  
Instructors: Norman Hutchinson, Ryan Vogt, Jonatan Schroeder Fall 2016

### MENTORING

#### **Carnegie Mellon University**

##### ADVISED RESEARCH ASSISTANTS

- Alexa Lowe Fall '25, Spring '26
- Denis Wambold KIT MS Thesis, visited Fall '25
- Henry Wong Summer '24, Fall '24, Spring '25
- Karen Li Fall '23, Spring '24
- Stanley Chen Spring '23
- Sneha Rander Fall '22
- Jeneel Mashru Fall '22
- Kevin Li Fall '22
- Shreya Srinarasi Summer '21

#### **University of British Columbia**

##### ADVISED RESEARCH ASSISTANTS

- Chris J.M. Yoon Summer '18, Fall '18
- Syed Mubashir Iqbal Summer '17
- Jaime Koerner Spring '17

## **Professional Experience**

---

### **Bosch Center for Artificial Intelligence**

Pittsburgh, PA, USA

05/2023 - 08/2023

#### MACHINE LEARNING RESEARCH INTERN

- Research on applications of diffusion models to improve the performance of visual anomaly detection.
- A paper describing our results was published at IEEE TAI 2025.

### **Oasis Labs**

Berkeley, CA, USA

01/2019 - 07/2019

#### SOFTWARE ENGINEER

- Developing a secure, private, data-sharing platform for an early-stage blockchain startup.
- A paper describing a use case of this platform was published at an ICML 2019 workshop.

### **LinkedIn Corporation**

Sunnyvale, CA, USA

06/2015 - 08/2015

#### SOFTWARE ENGINEERING INTERN

- Search, Network, and Analytics Team: Building infrastructure for online ML-based relevance scoring at scale

### **LinkedIn Corporation**

Mountain View, CA, USA

09/2014 - 12/2014

#### SOFTWARE ENGINEERING INTERN

- Distributed Data Systems Team: Designed and prototyped a derived-data serving system, Venice

### **Voicebox Technologies**

Bellevue, WA, USA

01/2014 - 04/2014

#### SOFTWARE ENGINEERING INTERN

- Server and Tools Team: Developed concurrent database access layer for a mobile voice-assistant service

### **Ontario Institute for Cancer Research**

Toronto, ON, Canada

05/2013 - 08/2013

#### SOFTWARE DEVELOPER INTERN

- Developer for the Boutros Lab: a bio-informatics research group

# Service

---

## External Service

### PROGRAM COMMITTEE

- VehicleSec 2026
- ACM SoCC 2026
- CPSS 2026
- ISC 2025
- RAID 2025
- 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. Dependable and Secure Computing 2025
- IEEE Trans. Information Forensics & Security 2025 (2x)
- Springer Machine Learning 2025
- 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

- SCS Graduate Application Support Program, 2025
- Student Representative for Faculty Meetings, 2024–2025
- 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 Sports Committee, 2021–2023

### UBC DEPARTMENT OF COMPUTER SCIENCE

- Computer Science Graduate Student Association (President), 2017
- Department Strategy Committee, 2017
- Space and Safety Committee, 2017

## Awards and Recognitions

---

2025	<b>PhD Student Research Award</b>	RSTCON 2025
2024	<b>Best Poster Award (\$300)</b>	IAP CMU Workshop: AI and Security in the Cloud
2024	<b>AI Net 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