Jimmy Z. Di

LinkedIn, GitHub, Google Scholar

jimmy.di@uwaterloo.ca
1-647-962-3506

Publications

Machine Unlearning Fails to Remove Data Poisoning Attacks
Martin Pawelczyk*, Jimmy Z. Di*, Ayush Sekhari, Yiwei Lu, Gautam Kamath, Seth Neel
Spotlight paper at ICML' 2024 Workshop on Generative AI and Law (GenLaw '24)
In Submission to ICLR 2025

Hidden Poison: Machine Unlearning Enables Camouflaged Poisoning Attacks
Jimmy Z. Di, Jack Douglas, Jayadev Acharya, Gautam Kamath, Ayush Sekhari.
Advances in Neural Information Processing Systems 36 (NeurIPS 2023)

Compound Drop Shape Analysis with the Neumann Number
Guangle Li, Gabriel Robles Del Hierro, Jimmy Z. Di, Yi Y. Zuo
Langmuir 36 (2020) 7619-7626

Education

University of Waterloo — **Sep 2023 - Apr 2025**
Master of Mathematics in Computer Science, GPA: 4.0/4.0 — *Waterloo, ON*

- Representative on the Undergraduate Academic Plans Committee (UAPC)

University of Waterloo — **Sep 2016 - Oct 2022**
Bachelor of Computer Science, Minor: Physics, GPA: 3.5/4.0 — *Waterloo, ON*

- Graduated with Distinction

Teaching

CS 350: Operating System — Summer 2024
Teaching Assistant & Instructional Apprentice

- Conducted both in-person and remote office hours to assist students in debugging coding assignments focusing on implementing core and auxiliary features such as user program arguments copying, thread scheduling, and semaphores in CastorOS
- Reviewed, assessed difficulty, and corrected typographical errors in early versions of students midterm exams
- Proctored and graded student's written midterm / final exams

CS 451: Data-Intensive Distributed Computing — Winter 2024
Instructional Apprentice

- Led tutorial sessions demonstrating code snippets in Java and Scala for Hadoop MapReduce and Apache Spark, covering functionalities such as Spark SQL, Page-Ranking, and Spark Streaming
- Addressed students' questions on the online forum Piazza regarding to Assignment specifics and debugging
- Coordinated TA activities including assignment grading and office hour schedules throughout the semester

CS 245: Logic and Computation — Fall 2023
Teaching Assistant

- Graded and provided feedback on students' written assignments
- Proctored and graded student's midterm / final exam

Awards

Vector Scholarship in Artificial Intelligence — $17,500
2023

David R. Cheriton Graduate Scholarship — $20,000
2023

Skills

Languages: Python, Scala, TypeScript, C#, C++, SQL
Frameworks/Libraries: PyTorch, Apache Spark, OpenCV, Angular 9, ASP.NET, scikit-learn, HuggingFace
Tools/Technologies: HDFS, Tableau, Oracle Database

Work Experience

JD Development Group — Jan 2023 - Aug 2023

Data Analyst — *Markham, ON*

- Prepared investor packages using Tableau dashboards to visualize housing market trends in the GTA; presented to the senior leadership including the CEO and CFO of the company
- Retrieved current housing market data from real estate sites including Altus and Realtor.ca; applied **logistic regression** to analyze unit prices and enhanced the accuracy of price forecasts by 15%

University of Waterloo — May 2021 - Aug 2022

Research Assistant — *Waterloo, ON*

- Published a paper as the first author at NeurIPS, introducing a novel poisoning vector called the **camouflaged data poisoning attack**, which targets deep neural networks to misclassify a target image after unlearning specific images
- Implemented the **gradient matching** algorithm to generate poison and camouflage examples using PyTorch Autograd for the poisoning attack, achieving a high camouflage success rate against CNN architectures such as Resnet
- Fine-tuned hyperparameters including learning rate and batch size using grid and random search; achieved 100% attack success and state-of-the-art validation accuracy on **CIFAR-10** and **ImageNet** datasets

Bank of America Merrill Lynch — Sep 2020 - Dec 2020

Software Engineer — *Remote*

- Created a responsive front-end application with **Angular 9** and reformatted API to monitor position reconciliations with real-time visualization, enabling analysts to resolve trading inconsistencies with more frequent and granular data
- Designed a dashboard UI utilizing **ngx-charts** to visualize metrics like trading volumes and discrepancy counts; applied data binding and interactive filtering to ensure a consistent pattern

University of Hawaii at Manoa — Jan 2020 - Apr 2020

Research Assistant - C++ Developer — *Honolulu, HI*

- Implemented algorithms to model compound axis-symmetric droplets by numerically solving **the Young-Laplace equation**, enhancing understanding of fluid dynamics in microgravity environments, as detailed in our publication
- Designed a robust edge detection algorithm with **OpenCV** to monitor changes in droplets' shape in real-time footage using Gaussian filtering/Canny edge detection; increased detection accuracy of noisy water droplet samples by **7x**
- Incorporated a serial port driver with a UI using **locks and mutexes**, allowing users to set up and control multiple linear actuators simultaneously using the MVC architecture

TAO Solutions — Sep 2018 - Apr 2019

Software Engineer Intern — *Toronto, ON*

- Developed scalable components and services to enhance the company's web application, including calculations and displays for loan amortization and repayment schedules, using **ASP.NET** and **Angular**
- Participated in daily stand-up meetings to ensure timely delivery of assigned work items ahead of sprint deadlines

Telus Communications — Jan 2018 - Apr 2018

Business Analyst — *Toronto, ON*

- Performed topics and sentiment analysis on textual customer survey data using **tokenization** and **Naive Bayes** to identify key areas that needed improvement; reduced project timeline from 3 weeks to 1 and selected as **"Featured Project"** in quarterly department meeting
- Built a modular, lightweight data ETL pipeline with a GUI to visualize and export Excel data to an Oracle database using PyQt and pandas; leveraged error handling and asynchronous processing to enhance UI responsiveness