Jimmy Z. Di

jimmy.di@uwaterloo.ca
LinkedIn, GitHub, Google Scholar
1-647-962-3506

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

Experience

JD Development Group **Jan 2023 - Aug 2023**
Data Analyst *Markham, ON*

- Prepared investor packages using Tableau dashboards to visualize current and future housing market trends in the GTA area; 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 10%

Bank of America Merrill Lynch **Sep 2020 - Dec 2020**
Software Engineer Intern *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

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

Publications

Machine Unlearning Fails to Remove Data Poisoning Attacks **Jun 2024**

- Implemented Instruction Poisoning on IMDb dataset by instruction-tuning an pre-trained GPT-2 Model using **HuggingFace transformer**; achieved 60% poisoning success rate with a 20% poison budget
- Published the spotlight paper as co-first author at ICML'24 GenLaw Workshop, introducing a new evaluation method for Machine Unlearning using poisoning attacks against image classifiers and language models such as GPT-2. In submission to ICLR 2025

Hidden Poison: Machine Unlearning Enables Camouflaged Poisoning Attacks **Dec 2023**

- Implemented the **gradient matching** algorithm to generate poison and camouflage examples using PyTorch Autograd for the poisoning attack, achieving 90% camouflage success rate against CNN architectures such as Resnet-18
- Published the paper as the first author at NeurIPS'23, 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

Education

University of Waterloo **Sep 2023 - Apr 2025**
Master of Mathematics in Computer Science, GPA: 3.98/4.0 *Waterloo, ON*

- Supervisor: Professor Gautam Kamath
- Graduate Student Representative on the Undergraduate Academic Plans Committee

Awards

Vector Scholarship in Artificial Intelligence $17,500
2023

David R. Cheriton Graduate Scholarship $20,000
2023