Adam Dziedzic

Personal Details

Phone:	+1 872 222 8183
Email:	adam.dziedzic@utoronto.ca
Personal web page:	https://adam-dziedzic.com/
LinkedIn:	https://www.linkedin.com/in/adziedzic
GitHub:	https://github.com/adam-dziedzic

Education

Current 2022 Postdoctoral Fellow in Computer Science
September 2020 **The Vector Institute** & **the University of Toronto**, Canada
Advisor: Professor Nicolas Papernot
Research areas: Trustworthy & Collaborative Machine Learning
I lead a project on Collaborative Learning. We enable multiple participants to collaborate and improve their local machine learning models while preserving the privacy and confidentiality of their data. I also work on attacks and defenses for ML models. Our defenses make model stealing more difficult by requiring users to complete a calibrated proof-of-work before they can read predictions from a model exposed via a public API.

Current 2020 PhD Program in Computer Science
July 2015 **The University of Chicago**, USA
Advisor: Professor Sanjay Krishnan
Research areas: Machine & Deep Learning, Data Analysis and Management, Databases, Systems
I worked on input and model compression for adaptive and robust convolutional Neural Networks. We explored FFT-based convolution with compression to control resource usage, retain high accuracy, and create more robust models. I also designed declarative interfaces for deep learning and compression of inputs and filters in the frequency domain for the FFT-based convolution. We investigated how the Band-Limited Convolutional Neural Networks can be leveraged to create a robust defense against adversarial attacks. Additionally, I researched the recommendation of indexes and hybrid physical designs for SQLServer, as well as the data loading and migration framework for the BigDAWG project.
Courses: Fundamentals of Deep Learning, Mathematical Foundations of Machine Learning, Machine Learning, Mathematical Toolkit (Linear Algebra & Probability), Convex Optimization, Discrete Mathematics, Algorithms & Data Structures, Databases, Topics in Databases, Operating Systems, Distributed Systems, Computer Architecture, Networks.
GPA: 3.91/4
Teaching assistant: Fundamentals of Deep Learning, Introduction to Databases, Databases for Public Policy

June 2015 Research Internship
October 2014 **École Polytechnique Fédérale de Lausanne (EPFL)**, Switzerland
Group: Data Intensive Applications and Systems
Advisor: Professor Anastasia Ailamaki
I built an automated testing infrastructure to benchmark the loading performance of several commercial and open-source databases, performed in-depth analysis to identify bottlenecks of the process and investigated novel techniques that could be used to accelerate DBMS data loading.

September 2014	Graduate Research Assistant
October 2013	**Warsaw University of Technology**, Poland
	Major: Computer Information System Engineering
	Main topic: Big Data
	Advisor: Professor Jan Mulawka
	Teaching assistant: Bioinformatics Algorithms
March 2013	Master of Science in Computer Science
October 2011	**Warsaw University of Technology**, Poland
	Major: Computer Information System Engineering
	Thesis: "An analysis and comparison of non-relational (NoSQL) databases with an example of application using CouchDB."
	Technologies: CouchDB, Riak, HBase, Python, Django, jQuery, sphinx
	Advisor: Professor Piotr Gawrysiak
	Gpa: 4.93/5 (top 5%) The final grade: Excellent
September 2011	Bachelor of Science in Computer Science
February 2011	**Warsaw University of Technology**, Poland
	Major: Computer Information System Engineering
	Thesis: "Document management system – application in three-tiered architecture."
	Advisor: Ph.D. Eng Jarosław Dawidczyk
	Technologies: PostgreSQL, Java, JEE, Hibernate, Dojo, PowerDesigner ObjectLedge, TestNG, JUnit, OO Design, Apache Tomcat
	Gpa: 4.80/5 (top 5%) The final grade: Excellent
January 2011	**Technical University of Denmark**, Copenhagen, Denmark
August 2010	Erasmus Programme
	Courses: Logical Systems and Logic Programming, Advanced Databases, Applied Statistics and Statistical Software, Web 2.0 and Mobile Interaction, Java Programming
	Gpa: 11.71/12
June 2010	**Warsaw University of Technology**, Poland
October 2007	Major: Computer Information System Engineering
June 2007	**Stefan Żeromski's High School in Kielce**, Poland
September 2004	Extended curriculum in mathematics and physics

Publications and posters

ICLR 2022	Adam Dziedzic, Muhammad Ahmad Kaleem, Yu Shen Lu, Nicolas Papernot *Increasing the Cost of Model Extraction with Calibrated Proof of Work* **SPOTLIGHT**
ICLR 2021	Christopher A. Choquette-Choo, Natalie Dullerud, Adam Dziedzic, Yunxiang Zhang, Somesh Jha, Nicolas Papernot, Xiao Wang *CaPC Learning: Confidential and Private Collaborative Learning*

Intel 2021	Ahmad-Reza Sadeghi, Ferdinand Brasser, Markus Miettinen, Thien Duc Nguyen, Thomas Given-Wilson, Axel Legay, Murali Annaaram, Salman Avestimeh, Alexandra Dmitrienko, Farinaz Koushanfar, Buse Gul Atli, Florian Kerschbaum, Lachlan J. Gunn, N. Asokan, Matthias Schunter, Rosario Cammarota, Adam Dziedzic, Nicolas Papernot, Virginia Smith, Reza Shokri *Private AI Collaborative Research Institute: Vision, Challenges, and Opportunities*
ArXiv 2021	Franziska Boenisch, Adam Dziedzic, Roei Schuster, Ali Shahin Shamsabadi, Ilia Shumailov, Nicolas Papernot *When the Curious Abandon Honesty: Federated Learning Is Not Private*
ArXiv 2021	Adelin Travers, Lorna Licollari, Guanghan Wang, Varun Chandrasekaran, Adam Dziedzic, David Lie, Nicolas Papernot *On the Exploitability of Audio Machine Learning Pipelines to Surreptitious Adversarial Examples*
ACL 2020	Dan Hendrycks, Xiaoyuan Liu, Eric Wallace, Adam Dziedzic, Rishabh Krishnan, Dawn Song *Pretrained Transformers Improve Out-of-Distribution Robustness*
JOR 2020	Arnold Wong, Garrett Harada, Remy Lee, Sapan D. Gandhi, Adam Dziedzic, Alejandro Espinoza-Orias, Mohamad Parnianpour, Philip Louie, Bryce Basques, Howard S. An, Dino Samartzis *Preoperative paraspinal neck muscle characteristics predict early-onset adjacent segment degeneration in anterior cervical fusion patients: a machine-learning modeling analysis*
OJVT 2020	Adam Dziedzic, Vanlin Sathya, Monisha Ghosh, Sanjay Krishnan *Machine Learning for Fair Spectrum Sharing in Dense LTE Wi-Fi Coexistence*
ICNC 2020	Vanlin Sathya, Adam Dziedzic, Monisha Ghosh, Sanjay Krishnan *Machine learning-based detection of multiple Wi-Fi BSSs for LTE-U CSAT*
Ph.D. 2020	Adam Dziedzic *Input and Model Compression for Adaptive and Robust Neural Networks* (Ph.D. Thesis)
ArXiv 2020	Adam Dziedzic, Sanjay Krishnan *Empirical Evaluation of Perturbation-based Defenses*
ICML 2019	Adam Dziedzic, Ioannis Paparrizos, Sanjay Krishnan, Aaron J. Elmore, Michael Franklin *Band-limited Training and Inference for Convolutional Neural Networks* (paper) code: https://github.com/adam-dziedzic/bandlimited-cnns
SIGOPS 2019	Sanjay Krishnan, Aaron J. Elmore, Michael Franklin, Ioannis Paparrizos, Zechao Shang, Adam Dziedzic, Rui Liu *Artificial Intelligence in Resource-Constrained and Shared Environments*
CIDR 2019	Sanjay Krishnan, Adam Dziedzic, Aaron J. Elmore *DeepLens: Towards a Visual Data Management System*
SIGMOD 2018	Adam Dziedzic, Jingjing Wang, Sudipto Das, Bolin Ding, Vivek R. Narasayya, Manoj Syamala *Columnstore and B+ tree – Are Hybrid Physical Designs Important?*

UChicago 2017	Adam Dziedzic *Data Loading, Transformation, and Migration for Database Management Systems* (Master's thesis)
CIDR 2017	Tim Mattson, Vijay Gadepally, Zuohao She, Adam Dziedzic, Jeff Parkhurst *Demonstrating the BigDAWG Polystore System for Ocean Metagenomic Analysis*
VLDB ADMS 2016	Adam Dziedzic, Manos Karpathiotakis, Ioannis Alagiannis, Raja Appuswamy, Anastasia Ailamaki *DBMS Data Loading: An Analysis on Modern Hardware*
HPEC 2016	Adam Dziedzic, Aaron J. Elmore, Michael Stonebraker *Data Transformation and Migration in Polystores* (paper) code: https://github.com/bigdawg-istc/bigdawg
HPEC 2016	John Meehan, Stan Zdonik, Shaobo Tian, Yulong Tian, Nesime Tatbul, Adam Dziedzic and Aaron J. Elmore *Integrating Real-Time and Batch Processing in a Polystore*
GCASR 2016	Adam Dziedzic, Aaron J. Elmore *Portage: A Data Migrator for a Polystore in the Database Deluge Era*
NEDBDAY 2016	Adam Dziedzic, Aaron J. Elmore *Portage: A Data Migrator for a Polystore in the Database Deluge Era*
IEEE VIS DSIA 2015	Adam Dziedzic, Jennie Duggan, Aaron J. Elmore, Vijay Gadepally, Michael Stonebraker *BigDAWG: a Polystore for Diverse Interactive Applications*
SPIE 2014	Adam Dziedzic, Jan Mulawka. *Analysis and Comparison of databases with an introduction to consistent references in big data storage systems*

Work Experience

September 2017 – June 2017 | **Google (Madison, The US)**

PhD Software Engineering Intern at Data Infrastructure and Analysis team

Mentor: Goetz Graefe

Eliminated a performance cliff in the F1 database for the aggregation queries.

Researched and designed different methods of incremental spilling and skew-awareness for graceful aggregation.

Contributed to the low-level data structures and made changes that were crucial to achieving robust performance in F1.

Coded in C++, wrote tests, and performed code reviews.

Participated and presented a poster during the internal Google PIRC 2017 conference for PhD interns.

June 2017 – March 2017 | **Microsoft Research (Redmond, The US)**

Data Management, Exploration and Mining (DMX) group

Mentors: Vivek Narasayya and Sudipto Das.

Worked on analysis and acceleration of query execution for mixed (OLTP and OLAP) workload.

Carried out research on hybrid physical structures for diverse workloads.

August 2013 – June 2013 | Barclays Investment Bank (London, The UK)
Analyst at Equities Derivatives Technology

Technologies: Java, Spring, Maven, Velocity, Jetty, JIRA, JUnit, JMock
The goal of the project was to validate current underlyings and suggest new underlyings for a given product, for example, a reverse convertible instrument. I created a system that went into production and brought value to the business.

December 2012 – April 2012 | CERN (Geneva, Switzerland)
Technical Student at IT Department and CERN Computer Center

I worked on NoSQL and NewSQL databases.

Technologies: NoSQL, CouchDB, Python, Django, tastypie, jQuery, sphinx, MapReduce, git, REST
My role involved developing a project to store information on the configuration and management of non-host devices at CERN Computer Centre. This began with gathering requirements from internal users and continued through design, implementation, testing, and deployment. The data was stored in the CouchDB database and exposed via REST-ful API.

March 2012 | Mobile Startup (app providing aspects of music social interactions)

Technologies: Python, Django, PostgreSQL, JavaScript, jQuery, Android
My mobile start-up provided aspects of music social network interaction. The application was based on rich user experience and heavily used social media API-s such as last.fm and youtube.com. My team took part in Startup Sauna program.

July 2010 | Tekten Sp. z o.o. (Warsaw, Poland)
Database designer, Java and PL/SQL software developer

Internal system project
Technologies: Java, PL/SQL
Database: Oracle 10g

September 2009 – July 2009 | Torn Sp. z o.o. (Warsaw, Poland)
Java and JavaScript software developer

Financial and accounting system project
Technologies: HTML, CSS, JavaScript, Java
Database: Oracle 10g

References

Nicolas Papernot	Assistant Professor at the University of Toronto and the Vector Institute email: nicolas.papernot@utoronto.ca
Sanjay Krishnan	Assistant Professor at the University of Chicago email: skr@uchicago.edu
Somesh Jha	Lubar Professor at the University of Wisconsin, Madison email: jha@cs.wisc.edu
Xiao Wang	Assistant Professor at Northwestern University email: wangxiao@cs.northwestern.edu
Vivek Narasayya	Principal Researcher at Microsoft Research, Redmond email: viveknar@microsoft.com
Michael Franklin	Liew Family Chairman of Computer Science at the University of Chicago email: mjfranklin@uchicago.edu

Teaching

Deep Learning	*TTIC-31230: Teaching assistant for the course on Fundamentals of Deep Learning taught by Prof. David McAllester* (Winter 2020)
Database Systems	*CS23500/33550: Teaching assistant for the course on Database Systems taught by Prof. Aaron J. Elmore* (Autumn 2015, Spring 2016, Winter 2017, Winter 2018, Spring 2018)
Bioinformatics Algorithms	*MBI: Teaching assistant for the course on Methods in Bioinformatics taught by Prof. Robert M. Nowak* (Spring 2014)

Technical Skills

Programming languages	C++, Java, Python (advanced), C, Bash, JavaScript, PowerShell PL/SQL (intermediate), C#, Prolog, R, Octave, Haskell, Scala (basic)
Frameworks	PyTorch, TensorFlow, Django, Spring
Databases	PostgreSQL 8.4-9.6 (advanced), NoSQL databases (CouchDB, Riak), MonetDB, Oracle 10g/11g/12c, SQL Server, Vertica (intermediate), VoltDB, S-Store, MariaDB (basic)

Awards

2022	Highlighted Reviewer at International Conference on Learning Representations (ICLR).
2019	Travel Award at International Conference on Machine Learning (ICML).
2018	Travel Award at SIGMOD (Special Interest Group on Management of Data).
2011-2012	The scholarship of the Rector of the Warsaw University of Technology for

	my achievements during the Master's program.
2007-2011	The academic scholarship for the best faculty students (granted on a yearly basis and based on GPA).

Talks

2022	Collaborative Machine Learning. **Vector Talk Series**
2021	Confidential and Private Collaborative Learning. **Scotia Bank - Research Frontier Talk Series**
2021	CaPC Learning: Confidential and Private Collaborative Learning. **Vector School: AI Model Governance**
2021	CaPC Learning: Confidential and Private Collaborative Learning. **Invited Speaker for the Third Workshop on Privacy in Natural Language Processing.**
2021	CaPC Learning: Confidential and Private Collaborative Learning. **The MLFL series, hosted by the Center for Data Science, UMass Amherst.**
2021	CaPC Learning: Confidential and Private Collaborative Learning. **Flow Seminar**
2021	CaPC Learning: Confidential and Private Collaborative Learning. **Intel Labs**
2020	CaPC Learning: Confidential and Private Collaborative Learning. **Vector Institute**
2018	Columnstore and B+ tree – are hybrid physical designs important? **University of California, Berkeley**
2018	Columnstore and B+ tree – are hybrid physical designs important? **Imperial College London**
2018	Columnstore and B+ tree – are hybrid physical designs important? **Oracle**
2018	Columnstore and B+ tree – are hybrid physical designs important? **Microsoft Research**
2018	Columnstore and B+ tree – are hybrid physical designs important? **MemSQL**

Service and Volunteering

Vector	Served on the Research Adjudication Committee for the Vector Scholarship in Artificial Intelligence: 2022.
ICLR	Reviewer at the International Conference on Learning Representations: 2019, 2020, 2021, 2022 (highlighted reviewer).
ICML	Reviewer at the International Conference on Machine Learning: 2021, 2022.
NeurIPS	Reviewer at the conference on Neural Information Processing Systems: 2021, 2022.

Languages

Polish	Mother tongue
English	Fluent
French	Basic Knowledge

Interests and Activities

Guitar	I finished a 5-year music school in classical guitar class.
Geography and traveling	Traveling is my passion. I won a Polish Olympiad of Geography 2004, the main topic of which were Asian countries.
Sports	I am an amateur basketball player. I was a member of my high school basketball team. I attended martial-art courses at the University of Chicago.