# Adam Dziedzic

## Personal Details


| | |
|---|---|
| Phone: | +1 872 222 8183 |
| Email: | adam.dziedzic@sprintml.com |
| Personal web page: | https://adam-dziedzic.com/ |
| LinkedIn: | https://www.linkedin.com/in/adziedzic |
| GitHub: | https://github.com/adam-dziedzic |
| Twitter: | https://twitter.com/adam_dziedzic |


## Academic and Research Experience

**Current** — **CISPA Helmholtz Center for Information Security**, Germany
**September 2023** — *Assistant Professor in Computer Science*
*My research is focused on secure and trustworthy Machine Learning as a Service (MLaaS). I design robust and reliable machine learning methods for training and inference of ML models while preserving data privacy and model confidentiality.*
Group: SprintML Lab

**September 2023** — **Vector Institute & the University of Toronto**, Canada
**September 2020** — *Postdoctoral Fellow in Computer Science*
Group: CleverHans Lab
Advisor: Professor Nicolas Papernot
Research areas: Trustworthy & Collaborative Machine Learning

**September 2017** — **Google** (Madison, USA)
**June 2017** — *PhD Software Engineering Intern at Data Infrastructure and Analysis Team*
Mentor: Goetz Graefe

**June 2017** — **Microsoft Research** (Redmond, USA)
**March 2017** — *Research Intern at Data Management, Exploration and Mining (DMX)*
Mentors: Vivek Narasayya and Sudipto Das.

**June 2015** — **École Polytechnique Fédérale de Lausanne (EPFL)**, Switzerland
**October 2014** — *Research Intern at Data Intensive Applications and Systems*
Advisor: Professor Anastasia Ailamaki

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

## Education

**August 2020** — **University of Chicago**, USA
**July 2015** — PhD Program in Computer Science
Advisor: Professor Sanjay Krishnan
Research areas: Robust Machine & Deep Learning, Data Analysis and Database Systems
Gpa: 3.91/4

Teaching assistant: Fundamentals of Deep Learning, Introduction to Databases, Databases for Public Policy

September 2014 – October 2013 **Warsaw University of Technology**, Poland
Graduate Research Assistant
Major: Computer Information System Engineering
Main topic: Big Data
Advisor: Professor Jan Mulawka
Teaching assistant: Bioinformatics Algorithms

March 2013 – October 2011 **Warsaw University of Technology**, Poland
Master of Science in Computer Science
Major: Computer Information System Engineering
Thesis: "An analysis and comparison of non-relational (NoSQL) databases with an example of application using CouchDB."
Advisor: Professor Piotr Gawrysiak
Gpa: 4.93/5 (top 5%) The final grade: Excellent

September 2011 – February 2011 **Warsaw University of Technology**, Poland
Bachelor of Science in Computer Science
Major: Computer Information System Engineering
Thesis: "Document management system – application in three-tiered architecture."
Advisor: Ph.D. Eng Jarosław Dawidczyk
Gpa: 4.80/5 (top 5%) The final grade: Excellent

January 2011 – August 2010 **Technical University of Denmark**
Gpa: 11.71/12

June 2010 – October 2007 **Warsaw University of Technology**, Poland
Major: Computer Information System Engineering

## Work Experience

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

March 2012 – April 2012 **Mobile Startup**
Application providing aspects of music social interactions

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

September 2009 – July 2009 **Torn** Sp. z o.o. (Warsaw, Poland)
*Java and JavaScript software developer*
Financial and accounting system project

## Awards

| | |
|---|---|
| 2022 | Highlighted Paper on a new defense against model extraction at International Conference on Learning Representations (ICLR). |
| 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). |

## Publications

| | |
|---|---|
| PETs 2023 | Adam Dziedzic, Christopher A. Choquette-Choo, Natalie Dullerud, Vinith Suriyakumar, Ali Shahin Shamsabadi, Muhammad Ahmad Kaleem, Somesh Jha, Nicolas Papernot, Xiao Wang *Private Multi-Winner Voting for Machine Learning* |
| PETs 2023 | Franziska Boenisch, Christopher Mühl, Roy Rinberg, Jannis Ihrig, Adam Dziedzic *Individualized PATE: Differentially Private Machine Learning with Individual Privacy Guarantees* |
| EuroS&P 2023 | Franziska Boenisch, Adam Dziedzic, Roei Schuster, Ali Shahin Shamsabadi, Ilia Shumailov, Nicolas Papernot *When the Curious Abandon Honesty: Federated Learning Is Not Private* |
| EuroS&P 2023 | Franziska Boenisch, Adam Dziedzic, Roei Schuster, Ali Shahin Shamsabadi, Ilia Shumailov, Nicolas Papernot *Is Federated Learning a Practical PET Yet?* |
| ICLR Workshop 2023 | Adam Dziedzic, Franziska Boenisch, Mingjian Jiang, Haonan Duan, Nicolas Papernot *Sentence Embedding Encoders are Easy to Steal but Hard to Defend* (ICLR 2023 Workshop on Trustworthy ML) |
| ICLR 2022 | Adam Dziedzic, Muhammad Ahmad Kaleem, Yu Shen Lu, Nicolas Papernot *Increasing the Cost of Model Extraction with Calibrated Proof of Work* **SPOTLIGHT** (top 5% of accepted papers) |
| NeurIPS 2022 | Adam Dziedzic, Haonan Duan, Muhammad Ahmad Kaleem, Nikita Dhawan, Jonas Guan, Yannis Cattan, Franziska Boenisch, Nicolas Papernot *Dataset Inference for Self-Supervised Models* |
| ICML 2022 | Adam Dziedzic, Nikita Dhawan, Muhammad Ahmad Kaleem, Jonas Guan, Nicolas Papernot *On the Difficulty of Defending Self-Supervised Learning against Model Extraction* |
| 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* |

| | |
|---|---|
| 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) |
| 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* |
| 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* |

## Preprints

| | |
|---|---|
| ArXiv 2023 | Franziska Boenisch, Christopher Mühl, Adam Dziedzic, Roy Rinberg, Adam Dziedzic *Have it your way: Individualized Privacy Assignment for DP-SGD* |
| ArXiv 2022 | Stephan Rabanser, Anvith Thudi, Kimia Hamidieh, Adam Dziedzic, Nicolas Papernot *Selective Classification Via Neural Network Training Dynamics* |
| ArXiv 2022 | Adam Dziedzic, Stephan Rabanser, Mohammad Yaghini, Armin Ale, Murat A. Erdogdu, Nicolas Papernot *p-DkNN: Out-of-Distribution Detection Through Statistical Testing of Deep Representations* |
| 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* |
| 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 2020 | Adam Dziedzic, Sanjay Krishnan *Empirical Evaluation of Perturbation-based Defenses* |

## 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) |

## Talks

| | |
|---|---|
| 2023 | Presentation on our paper on Private Multi-Winner Voting for Machine Learning at PETS 2023 (July 12th). |
| 2023 | Talk on "Is this model mine? On stealing and defending machine learning models."for ML capstone class ECE697 from the University of Wisconsin-Madison (June 20th). |
| 2023 | Podcast Interview: On model stealing and defenses hosted by Matt Faltyn. https://traincheck.buzzsprout.com/ |

2023 Is this model mine? On stealing and defending machine learning models. CISPA, Germany.

2022 Is this Encoder Mine? On Stealing and Defending Self-Supervised Encoders
**AI Safety Unconference NeurIPS 2022**

2022 Stealing and Defending Self-Supervised Models. Invited talk on Dataset Inference for Self-Supervised Models at **ML Collective** (a nonprofit research organization) during their reading group "Deep Learning: Classics and Trends"which runs weekly, is fully virtual and is open to the public. They have 3000+ email subscribers and on average 100 weekly attendees.

2022 **Managing AI Risk - Cybersecurity & Data Risk Workstream at Vector Institute:** Is this Encoder Mine? On Stealing and Defending Self-Supervised Encoders

2022 Is this model mine? On stealing and defending machine learning models
**University of Michigan at Ann Arbor**

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.

USENIX — Program Committee Member: 2023.

CCS — Program Committee Member: 2023 in the Machine Learning and Security Track.

ICLR — Reviewer at the International Conference on Learning Representations: 2019, 2020, 2021, **2022 highlighted reviewer , top 5%**, 2023.

| | |
|---|---|
| ICML | Reviewer at the International Conference on Machine Learning: 2021, 2022, 2023. |
| NeurIPS | Reviewer at the conference on Neural Information Processing Systems: 2021, 2022, 2023. |

## References


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