Rishav Chourasia

+65-97168493 | rishav@betterdata.ai | rishav1.github.io | Google Scholar

Objective

Veteran AI/ML researcher with a Ph.D. and over 6 years of experience with privacy engineering. Expert in differential privacy, multiparty computation, and cryptography with published works in venues like FORC, TPDP, and NeurIPS. Presently, my research focuses on Privacy-Preserving ML, Machine Unlearning, and Differential Privacy Auditing.

Experience

- **Betterdata.ai** *Dec 2025 - Present & Aug 2023 - Nov 2025*
  Head of Product (Earlier: Research Scientist / Privacy Engineer) Singapore
  - Lead development of the IRG1 platform; won IEEE S&P Distinguished Paper Award for auditing Apple's proprietary DP framework running on billions of devices.
  - Authored 4 papers on differential privacy quantification and auditing, with accepts at IEEE S&P, FMSD @ ICML, PPAI @ AAAI, FORC, and TPDP.
  - Coauthored grant proposal to secure US Department of Homeland Security's S&T Awards Contract.
- **Google Brain** *May 2022 - Aug 2022*
  PhD Student Researcher with Dr. Abhradeep Guha Thakurta and Dr. Krishnamurthy (Dj) Dvijotham Singapore
  - Derived high-confidence bounds on predictions for differentially private uncertainty estimation in Lasso regression.
- **Google Summer of Code** *May 2019 - Aug 2019*
  Student Developer with Preferred Networks Remote
  - Contributed to a Python-to-ONNX JIT compiler for Chainer ML framework.
  - Contributions enabled JIT compilation support for complex models like LSTMs, AlexNet and ResNet50.
- **Max-Planck Institute of Software Systems** *Nov 2018 - Feb 2019*
  Research Fellow with Dr. Adish Singla Saarbrücken, Germany
  - Studied how voting rules affect exploration/exploitation in multi-agent Q-learning, resulting in a NeurIPS paper.
- **Amazon Fraud Detection Team** *July 2018 - Nov 2018 & May 2017 - July 2017*
  Software Development Engineer & Software Development Intern Bangalore, India
  - Performance optimizations and bug fixes on the fraud detection ML platform (<800 ms latency with 99.9% SLA).
  - Developed tooling to track changes in pipeline configurations and raise alerts.

Education

- **National University of Singapore** *Aug 2019 - May 2025*
  Ph.D. in Computer Science with advisor Dr. Xiaokui Xiao Singapore
  - GPA: 4.83/5.00 - PhD Thesis
- **Indian Institute of Technology Guwahati** *July 2014 - June 2018*
  B.Tech in Computer Science and Engineering Guwahati, India
  - GPA: 9.26/10.00

Selected Projects

- **Privacy Auditing: Empirically Detecting Violations of Differential Privacy** *March 2023 - Aug 2025*
  Keywords: [Differential Privacy, Private Federated Learning, Reconstruction Attacks] [🌐]
  - Reverse-engineered Apple's DifferentialPrivacy.framework to find DP bugs affecting 87% of audited macOS Sonoma collection; IEEE S&P Distinguished Paper Award.
  - Pioneered a new operational interpretation of differential privacy, simplifying privacy analysis. This work received an oral acceptance at FORC, TPDP and PPAI, three of the most prestigious gatherings for privacy researchers.
- **Machine Unlearning: How to Guarantee Deletion in ML** *March 2022 - Feb 2023*
  Keywords: [Noisy Gradient Descent, Trustworthy Deletion] [🌐]
  - Built a rigorous and sound notion for quantifying data-deletion capacity of unlearning algorithms.
  - Proved that *unlearning via Noisy Gradient Descent* has optimal privacy-utility trade-offs with few training passes.
  - Results published at ICML 2023 and at FORC 2023 (20-minute oral presentation).
- **Privacy-Preserving ML: Maximizing Utility with Minimal Compute** *March 2020 - Feb 2022*
  Keywords: [Differential Privacy, Noisy Gradient Descent] [🌐]
  - Proved $O(1)$ privacy bound for Noisy Gradient Descent, a result that is regarded as a "breakthrough".
  - Collaborated with NEC researchers to develop the cross-distillation technique to enhance privacy.
  - Research works published in NeurIPS 2021 (spotlight) and PETS 2021.
- **Chainer Compiler: An experimental Python-to-ONNX converter** *May 2019 - Aug 2019*
  Tools: [ONNX, Chainer ML] [🐙, 🌐]
  - Developed Elichika, a compiler to convert Python source of a chainer.Chain object into ONNX computation graph.
  - Added core language features to the compiler, such as support for lambda functions, looping, and return.
  - Contributions were featured in NumFOCUS blog.

PUBLICATIONS

AUTHORSHIP ORDER BY CONTRIBUTION. C=CONFERENCE, W=WORKSHOP, T=THESIS

[C.1] Rishav Chourasia, Ergute Bao, Uzair Javaid, and Xiaokui Xiao. (2026). **Auditing Apple's DifferentialPrivacy.framework: Implementation Bugs, Misconfigurations, and Practical Risks**. In *IEEE S&P 2026*, pp. 1815–1834. Distinguished Paper Award.

[C.2] Rishav Chourasia, et al. (2025). **Laplace Transform Interpretation of Differential Privacy**. In *6th Symposium on Foundations of Responsible Computing (FORC 2025)* (pp 11:1–11:22).

[C.3] Rishav Chourasia and Neil Shah. (2023). **Forget Unlearning: Towards True Data-Deletion in Machine Learning**. In *International Conference on Machine Learning (ICML 2023)* (pp. 6028-6073). PMLR.

[C.4] Rishav Chourasia, et al. (2021). **Differential Privacy Dynamics of Langevin Diffusion and Noisy Gradient Descent**. In *Advances in Neural Information Processing Systems 34 (NeurIPS 2021)*, pp. 14771-14781.

[C.5] Rishav Chourasia, et al. (2021). **Knowledge Cross-Distillation for Membership Privacy**. In *Proceedings on Privacy Enhancing Technologies (PETS 2021)*, pp 362-377.

[C.6] Rishav Chourasia, et al. (2017). **Visualization of Two-Dimensional Interval Type-2 Fuzzy Membership Functions using General Type-2 Fuzzy Membership Functions**. In *17th World Congress of International Fuzzy Systems Association (IFSA-SCIS 2017)*, pp. 1-5.

[C.7] V Saxena, N Yadala, Rishav Chourasia, et al. (2017). **Type Reduction Techniques for Two-Dimensional Interval Type-2 Fuzzy Sets**. In *International Conference on Fuzzy Systems (FUZZ-IEEE 2017)*, pp. 1-6.

[W.1] Rishav Chourasia and Adish Singla (2019). **Unifying Ensemble Methods for Q-learning via Social Choice Theory**. In *Learning with Rich Experience workshop (LIRE 2019)* at NeurIPS 2019.

[W.2] Rishav Chourasia, et al. (2025). **One-Run Privacy Auditing for Structured Generative and Foundation Models**. In the 1st ICML Workshop on Foundation Models for Structured Data, Vancouver, Canada. 2025.

[T.1] Rishav Chourasia. (2025). **Learning and Unlearning via Noisy Gradient Descent**. Doctoral Dissertation, *National University of Singapore*.

[T.2] Rishav Chourasia. (2018). **Optimal Swarm RL: An Improved Deep-Exploration Strategy**. Bachelor Dissertation, *Indian Institute of Technology Guwahati*.

SKILLS

- **Programming Languages:** Python, C, C++, Objective C, Java
- **Machine Learning Frameworks:** JAX, PyTorch, Keras, ONNX, Fastai, Scikit-learn, XGBoost, Chainer
- **Cloud Technologies:** AWS, GCP, Docker, CI/CD
- **Mathematical & Statistical Tools:** Mathematica, MATLAB, SymPy, NumPy, Jupyter, Pandas, Polars
- **Database Systems:** MySQL,PostgreSQL,SQLite,MongoDB
- **DevOps & Version Control:** Git, CircleCI, Github Actions, Jenkins
- **Specialized Area:** Performance Optimization, ML Theory, Trustworthy AI Fundamentals
- **Other Tools & Technologies:** Weights & Biases, Comet ML, FastAPI, Flask
- **Research Skills:** Problem Formulation, Critical Thinking, Data Collection, Grant Writing, Presentation

HONORS AND AWARDS

- **SoC Research Incentive Award** *Oct 2023*
  National University of Singapore [🔗]
  ◦ Presented to students who have demonstrated good academic standing and research progress.
- **Research Achievement Award** *June 2022*
  National University of Singapore [🔗]
  ◦ Presented to PhD students who have achieved outstanding research performance over the past academic year.
- **1st Prize, CS6101 Deep Unsupervised Learning course** *Dec 2019*
  15th SoC Term Project Showcase, School of Computing
- **PhD Research Scholarship** *May 2019*
  National University of Singapore
  ◦ Awarded to promising PhD candidates accepted at NUS; 100% tuition fee-waiver and stipend for four years.
- **Research Fellowship** *Sept 2018*
  Max Planck Institute for Software Systems [🔗]
  ◦ Invited as a visiting scholar to work on a research project in the area of machine teaching.
- **Department Topper** *July 2015*
  Indian Institute of Technology, Guwahati
  ◦ Achieved highest GPA among freshman students in my department and was among top 8/440 students that year.
- **High School Matriculation Topper** *March 2012*
  DeNobili C.M.R.I, Dhanbad
  ◦ Achieved the highest percentage (96.4%) in ICSE matriculation among over 500 students.