Subhabrata (Subho) Majumdar

Responsible ML Scientist, Twitch | Founder, AI Vulnerability Database
e-mail: zoom.subha@gmail.com; web: shubhobm.github.io

Summary

- Technical leader in applied responsible machine learning who thrives in cross-functional collaborations.
- Pioneered the use of responsible ML methods in industry settings. Wrote a book, founded multiple nonprofit efforts in this area. Drove policy changes through successful collaborations in the data for good space.
- 10 years of R&D experience in ML, data science, and statistics with 30+ publications and 20+ filed patents (5 granted).

Core competencies

- Responsible ML: ML fairness, explainability, privacy, security, robustness.
- Predictive analytics, statistical machine learning: graphical models, feature selection, hypothesis testing.
- Technical leadership, cross-functional collaboration, strategic planning.
- Tools: Python (tensorflow, numpy, pandas, scikit-learn), R (data.table, ggplot, caret), SQL, Hadoop, Spark, Scala, AWS, C++.

Education

- PhD Statistics, University of Minnesota - Twin Cities, 2017. Advisor: Snigdhansu Chatterjee.
- MS Statistics, Indian Statistical Institute, 2012.
- BS Statistics, Indian Statistical Institute, 2010.

Experience

Twitch/Amazon, Dec 2022-Present

- First Applied Scientist in the newly formed Responsible AI team.
- Through a large-scale data audit, uncovered significant disparities against minority streamers. Created new bias metrics and detections, standardized them for broader use through a Python library.
- Led the creation of an internal Responsible AI science and engineering strategy.

AI Vulnerability Database (AVID), Sep 2022-Present

- Conceptualized and created AVID as an equivalent of MITRE ATT&CK and NIST CVEs in the AI world.
- Grew the leadership team to 8, formed its governing board, and incorporated its parent organization (501c3 pending).
- Wore multiple hats in the process: from engineering backend tools and datamodels to managing partnerships.
- AVID is now 140-strong on discord. We recently held 2 workshops (including MozFest), and are partnering with Hugging Face and a number of other organizations to release the MVP version of the AVID.

Splunk Security Content, Oct 2021-Oct 2022

- Led key projects developing cloud-native ML solutions: an AWS Glue-based ETL pipeline to enable for downstream ML work, Graph Neural Network-based counterfactual explanation of notable alerts, and auto-recommendation of tags (e.g., MITRE ATT&CK tactics) for novel threat detections.
- Played a critical role in shipping the largest-ever content update (v5.1) for Splunk User Behavioral Analytics (UBA).
- Partnered with engineering and product leadership to develop a long-term, customer-centric vision for ML research and development in security content.

AT&T Labs, Aug 2018-Sep 2021

- As a founding member of AI governance team implementing responsible ML practices across AT&T, proposed SIFT (System to Integrate Fairness Transparently) as an enterprise-level fairness monitoring and auditing framework.
- Technical lead for developing the internal SIFT platform, fairness analyses of business-critical use cases going through SIFT, and internal and external research collaborations.
- Work led to 15+ research papers and 15+ patent filings in 3 years.

University of Florida Informatics Institute, July 2017-Aug 2018

- As a postdoctoral researcher Developed novel machine learning methods for integrative analysis of multimodal biological Omics data. Work led to publication in the Journal of Machine Learning Research.

IBM Research, May 2016-Aug 2016

- Research fellow in the inaugural IBM Social Good program.
- Collaborated with scientists in the Data Science group, and Cary Institute of Ecosystem Studies to mine ecological data and devise cognitive algorithms that can determine which primates are carriers for the Zika virus in the wild.
- Work led to publication in the journal Epidemics.

Leadership

- Leading the long-term strategy and execution of AVID and its parent organization (AI Risk and Vulnerability Alliance).
- Founded and led execution in two other community efforts in responsible ML: Trustworthy ML Initiative, Bias Buccaneers.
- Managed a team of 4 data scientists to collaborate with UNICEF officials on a volunteer project in developing a ML platform for air-quality prediction. Work was presented in CHI-2021.

Selected publications (*see Google scholar for full list*)

- F.T. Brito, V.A.E. Farias, C. Flynn, J.C. Machado, **S. Majumdar**, D. Srivastava. Global and Local Differentially Private Release of Count-Weighted Graphs, SIGMOD 2023.
- (Book) Pruksachatkun, Y., McAteer, M., **Majumdar, S.** Practicing Trustworthy Machine Learning, 2023, O'Reilly Media.
- H. Raj, D. Rosati, **S. Majumdar**. Measuring Reliability of Large Language Models through Semantic Consistency, NeurIPS 2022 ML Safety workshop (Best Paper Award).
- C. Flynn, A. Guha, **S. Majumdar**, D. Srivastava, Z. Zhou. Towards Algorithmic Fairness in Space-Time: Filling in Black Holes, NeurIPS 2022 TSRML workshop.
- **Majumdar, S**. and Chatterjee, S. Feature Selection using e-values. ICML 2022.
- **Majumdar, S.**, Flynn, C., and Mitra, R. Evaluating Fairness in the Presence of Spatial Autocorrelation, NeurIPS 2021 AFCR workshop, PMLR 171, 6-18, 2022.
- **Majumdar, S.** and Michailidis, G. Joint Estimation and Inference for Data Integration Problems based on Multiple Multi-layered Gaussian Graphical Models, Journal of Machine Learning Research, 23(1), 1-53, 2022.
- *Derzsy, N., **Majumdar, S.**, Malik, R. An Interpretable Graph-based Mapping of Trustworthy Machine Learning Research, CompleNet 2021. **Alphabetical authors*.
- Farias, V., Timbo, F., Flynn, C., Machado, J., **Majumdar, S.,** Srivastava, D. Local Dampening: Differential Privacy for Non-numeric Queries via Local Sensitivity, PVLDB, 14(4), 521-533, 2020.
- Ghosh, A. and **Majumdar, S.** Ultrahigh-dimensional Robust and Efficient Sparse Regression using Non-Concave Penalized Density Power Divergence, IEEE Transactions on Information Theory, 66(12), 7812-7827, 2020.

Selected speaking engagements (*see my website for full list*)

06/2023 (Keynote) CVPR 2023 workshop on Fair, Data-efficient, and Trusted Computer Vision
11/2022 Open Data Science Conference *(*ODSC) West 2022
10/2022 ML:Integrity Conference 2022
07/2022 (Keynote) NAACL 2022 Workshop on Trustworthy Natural Language Processing
04/2022 University of Washington Responsibility in AI Systems and Experiences (RAISE) Lab
01/2021 (Plenary) All India Council for Technical Education Faculty Development Program
12/2020 Data Science Salon Virtual
11/2020 (3 talks) Indian Institute of Technology, Kanpur Data Science Seminar Series
02/2020 3rd NISS Virtual Industry Career Fair
03/2019 NYC Women in Machine Learning & Data Science meetup
05/2018 Savvysherpa, Inc., Minneapolis, MN

Major awards

- University of Minnesota (UMN) Martin-Buehler Award in Statistics 2016-2017, awarded by School of Statistics.
- UMN Interdisciplinary Doctoral Fellowship 2016-2017, awarded by the Graduate School.
- Best Student Paper in theory and methods, 2016 International Indian Statistical Association conference, Corvallis, OR.
- National Science Foundation (NSF) travel award for the 5th International Workshop on Climate Informatics, 2015.