

VIBHA BELAVADI

[email](#) | [portfolio](#) | [linkedin](#) | 469-450-9896

EDUCATION

The University of Texas at Dallas, Richardson TX GPA 3.71/4.00

PhD Computer Science

Summer 2022

Masters Computer Science

Spring 2016

Focus: Adversarial Machine Learning, Deep Learning, Data Privacy & Security.

Birla Institute of Technology and Science (BITS-Pilani), Rajasthan, India

B.E.(Hons.) Computer Science

Spring 2014

PUBLICATIONS AND RESEARCH WORK

- Developing novel systems and methods to preserve data security, privacy, and fairness.
- [MultiModal Deception Detection: Accuracy, Applicability, Generalizability](#); **IEEE TPS 2020**; *Vibha Belavadi*, et al. (UT Dallas & U.S. Army Research Lab).
- [Attacking Machine Learning Models for Social Good](#); **GameSec 2020**; *Vibha Belavadi*, et al.
- [Multi-Concept Adversarial Examples](#); **preprint**; *Vibha Belavadi*, et al.
- Reviewer for KDD, ACM CODASPY, IEEE TDSC, WebConf, PAKDD and SDM.

EMPLOYMENT

Data Scientist Intern, Swiss Re at Armonk, New York

Summer 2018

- Extracted relevant causal features that helped successfully predict the user's propensity for insurance enrollment more than 80% of the times.
- Performed feature engineering, synthetic data generation and dictionary creation using NLP and data science methods.

Software Engineer Intern, SAP Labs at Bengaluru, India

Fall 2013

- Designed & developed web services for SAP BusinessObjects and released in production.
- Wrote automation testing framework for BOUM2 backend to improve product quality.

SKILLS

Technologies: TensorFlow, Keras, PyTorch, Python, Pandas, Spark, Java, Scala, Hive, R, Scikit-Learn, OpenCV, MATLAB, SQL/NoSQL, Hadoop, HBase, Tableau, LaTeX, Git, RESTful web-services.

Methodologies: Object Oriented Programming, Functional Programming, Agile/Scrum.

Courses: Deep Learning, Machine Learning, Data Structures & Algorithms, Databases, Computer Vision, Natural Language Processing, Data Science, Big Data, Generative Adversarial Networks (GANs), Adversarial Machine Learning, Data Applications & Security, Semantic Web, Information Retrieval, Cloud Computing, Statistical Methods for Data Science, Statistical Methods in AI & ML, Recommendation Systems.

PROJECTS

- **Improving Loan Acceptance for social good:** Designed a cost formulation framework for the loan data that recommended users change specific attributes in their loan application to get loan approval, with a 90.4% success rate.
- **Multi-concept attack of Sensitive Attributes:** Generated adversarial artifacts on facial data to protect a set of attributes (e.g., Gender) while attacking others (e.g., Glasses). The accuracy of the Glasses model dropped to 17.22% (compared to 98.69% original accuracy). The Gender model accuracy increased to 99.09% (compared to 93.76% base accuracy).
- **Recommendation System:** Implemented a recommendation system using collaborative filtering, content-based filtering, matrix factorization, and hybrid methods and compared their performances using precision@k, recall@k, and ndcg@k as metrics.
- **Differential Privacy-based Access Control:** Implemented an access control system with differential privacy-based additive noise based on user's privacy clearance and data privacy risk.
- **Human Expressions Detection:** Trained HAAR cascade classifiers in OpenCV to detect 'shh expression' and 'wink expression' in images and live video with 85%+ accuracy.
- **Web Search Engine for food:** Developed topic-based web search engine using Apache Nutch, Apache Solr, Apache Lucene Page rank/HITS, query expansion & clustering.
- **Probabilistic graphical modeling:** MCMC sampling, Bethe Free energy approximation, Loopy Belief Propagation, Approximate MAP inference, Gibbs Sampling, MLE & Bayesian Structure Learning using MATLAB.
- **Data Modeling and Analytics:** Implemented Monte Carlo Simulations, exploratory data analysis, data visualization, regression fitting, A/B Testing using null and alternate hypothesis, student t-test, chi-square test, GBM, and XGBoost models, K-Means clustering, PCA, One-hot encoding.