VIBHA BELAVADI

email | portfolio | linkedin | 4694509896

EDUCATION

The University of Texas at Dallas, Richardson TX — GPA 3.71/4.00
MS/PhD Computer Science — May 2022
Focus: Adversarial Machine Learning, Deep Learning, Data Privacy & Security.

Birla Institute of Technology and Science, Pilani, Rajasthan, India
B.E. (Hons.) Computer Science — Aug 2014

EMPLOYMENT

Research Assistant, Data Security & Privacy Lab at UT Dallas, TX — Aug 2016 - present

- 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. It is a joint work with U.S. Army Research Lab.
- Attacking Machine Learning Models for Social Good; **GameSec 2020;** *Vibha Belavadi*, et al.
- Multi-concept adversarial attacks; **under submission;** *Vibha Belavadi*, et al.
- Reviewer for KDD, ACM CODASPY, IEEE TDSC, WebConf, PAKDD and SDM.

Data Scientist Intern, Swiss Re at Armonk, NY — May-Aug 2018

- Successfully predicted user's propensity for insurance enrollment 80+% of the times.
- Performed feature engineering, relevant causal feature extraction from customer health data, synthetic data generation & dictionary creation using NLP/data science methods.

Software Engineer Intern, **SAP Labs** at Bengaluru, India — Jul-Dec 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, R/R Studio, Scikit-Learn, OpenCV, MATLAB, SQL/NoSQL, Jupyter, Hadoop, HBase, Tableau, LaTex, Git.
- **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, Adversarial Machine Learning, Data Applications & Security, Semantic Web, Information Retrieval, Cloud Computing, Statistical Methods for Data Science, Statistical Methods in AI & ML.

ACADEMIC PROJECTS

- Improving Loan Acceptance: Designed a cost formulation framework using German Credit dataset that recommended the users to change certain attributes in their loan application and get loan approval, with 90+% attack success rate.
- Privacy Preservation of Sensitive Attributes: Generated adversarial artifacts on facial data to protect the Gender attribute. Successfully attacked 75+% of the male and female candidate gender images to preserve privacy.
- Differential Privacy based Access Control: Designed & implemented an access control system which is enabled by differential privacy based additive noise depending on the user's privacy clearance and data privacy risk.
- Data Modeling & Analytics: Implemented Monte Carlo Simulations, exploratory data analysis, data visualization, regression fitting, A/B Testing using null and alternate hypothesis, student-t test, and chi-square test, GBM and XGBoost models, K-Means clustering, PCA, One-hot encoding.
- Human Expressions Detection: Trained HAAR cascade classifiers in OpenCV to detect 'shh' and 'wink' expressions in images and live videos with 85+% accuracy.
- Top-based Web Search Engine: 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.