


## Education

### Georgia Institute of Technology

 Ph.D. in Computational Science and Engineering

 M.S. in Computational Science and Engineering

> GPA: 3.91/4.0

> Advisor: Prof. Duen Horng Chau

> Research concentration: Adversarial ML, ML security, Explainability and Interpretability in Deep Learning

2015 - present

currently pursuing

Fall 2015 - Spring 2017

### Netaji Subhas Institute of Technology, University of Delhi


 B.E. in Instrumentation and Control Engineering

> Thesis: Automatic Speaker Recognition using Student's T-Mixture Model

2010 - 2014

## Work Experience

### Alexa Brain, Amazon

 Applied Scientist Intern

> Explored generative regularization and implemented several weakly supervised deep learning models for name-free skill invocation on the Alexa voice interface.

> Proposed an attention-based, low-rank approximation that learns a shared embedding space for high-level application domains and low-level word tokens.

May 2018 - Aug 2018

### Alexa Natural Language Understanding, Amazon

 Software Development Engineer Intern

> Developed, evaluated and visualized semantic representations for automatic ontology alignment of knowledge graphs.

May 2017 - Aug 2017

### Amazon Web Services, Amazon

 Web Development Engineer Intern

> Developed a data pipeline to accelerate the execution time of CloudWatch Logs Search.

> Designed and integrated visualizations in the CloudWatch console to enable quick analysis of AWS metrics.

May 2016 - Aug 2016

### Indraprastha Institute of Information Technology, Delhi (IIITD)

 Research Associate

> Developed from ground-up, a platform for realtime tracking, analysis and visualization of social media data. This is actively being used by several federal and state security agencies in India.

> Developed the TweetCred credibility API and the TweetCred browser extension, which were also covered by popular news outlets including The Washington Post and The New Yorker.

Sep 2013 - Aug 2015

### Google Summer of Code 2013

 Software Developer Intern - ThinkUp

> Developed the data model for analyzing and generating insights from social media data, designed visualizations.

Jun 2013 - Sep 2013

### mLabs

 Software Engineer

> Developed the complete software and hardware interface for a patented web-enabled electronic prototyping device.

Sep 2012 - May 2013

## Publications

### Conference Papers

#### **ADAGIO: Interactive Experimentation with Adversarial Attack and Defense for Audio**

N. Das, M. Shanbhogue, S. T. Chen, L. Chen, M. E. Kounavis, D. H. Chau  
*European Conference on Machine Learning & Principles & Practice of Knowledge Discovery in Databases (ECML-PKDD)*, 2018.

#### **SHIELD: Fast, Practical Defense and Vaccination for Deep Learning Using JPEG Compression**

N. Das, M. Shanbhogue, S. T. Chen, F. Hohman, S. Li, L. Chen, M. E. Kounavis, D. H. Chau  
*ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD)*, 2018.  
🏆 Audience Appreciation Award (runner-up)

#### **PASSAGE: A Travel Safety Assistant with Safe Path Recommendations for Pedestrians**

M. Garvey, N. Das, J. Su, M. Natraj, B. Verma  
*ACM International Conference on Intelligent User Interfaces (IUI)*, 2016.

### Workshop Posters & Papers

#### **Compression to the Rescue: Defending from Adversarial Attacks Across Modalities**

N. Das, M. Shanbhogue, S. T. Chen, F. Hohman, S. Li, L. Chen, M. E. Kounavis, D. H. Chau  
*KDD Workshop - Project Showcase*, 2018.

#### **Defense against Adversarial Attacks using JPEG Compression**

N. Das, M. Shanbhogue, S. T. Chen, F. Hohman, L. Chen, M. E. Kounavis, D. H. Chau  
*NIPS Workshop - Women in Machine Learning (WiML)*, 2017.

#### **Training a Generative Agent Grounded in Cooperative Visual Dialog with Deep Reinforcement Learning**

A. Kalia, N. Das, M. Shanbhogue, V. Parthasarathy  
*NIPS Workshop - Women in Machine Learning (WiML)*, 2017.

### Preprints and Technical Reports

#### **GOGGLES: Automatic Training Data Generation with Affinity Coding**

N. Das, S. Chaba, S. Gandhi, D. H. Chau, X. Chu  
*arXiv preprint arXiv:1903.04552*, 2019.

#### **Keeping the Bad Guys Out: Protecting and Vaccinating Deep Learning with JPEG Compression**

N. Das, M. Shanbhogue, S. T. Chen, F. Hohman, L. Chen, M. E. Kounavis, D. H. Chau  
*arXiv preprint arXiv:1705.02900*, 2017.

## Academic Reviewing

**ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD)**

2019

**Deep Learning and Security Workshop at IEEE S&P (DLS)**

2018

## Teaching

### **CSE 6242: Data & Visual Analytics**

• Graduate Teaching Assistant (451 students)

*Georgia Institute of Technology*

Fall 2018

- Head Teaching Assistant (215 students)
- Graduate Teaching Assistant (187 students)

Fall 2016  
Spring 2016

## Grants and Funding

### ★ Amazon AWS Research Grant

2018

*Adversarial Re-Training and Model Vaccination for Robust Deep Learning*

Co-PI's: H. Park, S. Freitas, D. H. Chau

Funded \$5,000 in AWS cloud credits

### ★ NVIDIA GPU Grant

2018

*Defending Adversarial Attacks by Robust, Inference-time Local Linear Approximation*

Co-PI's: S.T. Chen, S. Freitas, F. Hohman, D. H. Chau

Funded NVIDIA Titan V GPU worth \$3,000

## Honors and Awards

### ☆ Audience Appreciation Award (runner-up) at ACM SIGKDD Conference

2018

For "SHIELD: Fast, Practical Defense and Vaccination for Deep Learning Using JPEG Compression"

### ☆ KDD Student Travel Award

2018

For participation at the ACM SIGKDD International Conference on Knowledge Discovery & Data Mining.

## Projects

### GOGGLES: Learning Interpretable Representations of Semantic Concepts [[github.com/chu-data-lab/GOGGLES](https://github.com/chu-data-lab/GOGGLES)]

*Class project for GaTech CS 8803: Data Management for Machine Learning*

Fall 2018

> Proposed a novel learning framework that encapsulates high-level semantic concepts as visually grounded prototype embeddings, which serve as labelling functions for inferring class labels for image datasets.

### Image Segmentation using CRFs and Conditional Image Generation using VAE

*Class project for GaTech CS 8803: Probabilistic Graphical Models*

Spring 2018

> Experimented with CNNs and CRFs to evaluate DeepLab, a state-of-the-art model in image segmentation.

> Given image segmentation and class labels for the segments, implemented a conditional generative model using VAE.

### Neuroevolutionary Gait Simulation of Quadruped Robots [[bit.ly/cse6730-gait-videos](https://bit.ly/cse6730-gait-videos)]

*Class project for GaTech CSE 6730: Modeling and Simulation*

Spring 2016

> Developed a simulation framework wherein quadruped robots were evolved to learn walking gaits through a neuroevolutionary mechanism using a genetic algorithm.

### baudcast [[github.com/nilakshdas/baudcast](https://github.com/nilakshdas/baudcast)]

*Independent open-source project*

2014

> Developed a socket-based, realtime messaging library for the internet of things paradigm.

> This has been downloaded and used in over 1,000 Node.js projects.

## Technical Skills

**Programming:** Python, Java, C++, C, Matlab, Scala, SQL

**Big Data:** Apache Storm, Apache Hadoop and MapReduce, Apache Spark, Pig, Apache Lucene

**Machine Learning:** TensorFlow, PyTorch, DyNet, Caffe, scikit-learn, Weka, Microsoft Azure ML Studio

**Web Development:** JavaScript ES7, Node.js, Ruby on Rails, PHP, Django, D3, jQuery