SIDDHANT BHAMBRI

699 S Mill Ave, Tempe, AZ 85281 - United States of America

+1 (480)-227-4177 ◇ siddhantbhambri@asu.edu

Siddhant Bhambri ◇ sbhambr1 ◇ Siddhant Bhambri ◇ sbhambr1 ◇ siddhant.bhambri4

Research Objective: The goal of my research is to advance the field of Human-Aware Artificial Intelligence (HAAI). I aim to understand the interactions of robotic agents in settings where they have to closely collaborate and team with humans. My primary research interests lie in *planning*, *explainability* and *security in HAAI.*

EDUCATION

Ira A. Fulton School of Engineering, Arizona State University *2021 - Present*
PhD Student in Computer Science GPA: 4.0/4.0
Advised by *Dr. Subbarao Kambhampati*

Delhi Technological University, India *2016-2020*
B.Tech in Computer Science CGPA: 8.7/10.0

RESEARCH EXPERIENCE

Graduate Research Associate: ASU *Presently*
Mentored by *Dr. Subbarao Kambhampati*
Working on Human-Aware AI problem settings to formulate robust and seamless interaction between humans and AI agent/robot and particularly focusing on modeling the AI agent for compatibility with human behaviors.

Research Intern: IIIT-Delhi & IIT-Madras *2019-2020*
Mentored by *Dr. Arun Balaji Buduru (IIIT) & Dr. Chester Rebeiro (IIT)*
Conducted an empirical study of black-box adversarial attack technique to test robustness of such attacks on real-life classification tasks such as face-recognition systems and object-tracking systems.

Research Intern: IIIT-Delhi *2019-2020*
Mentored by *Dr. Sambuddho Chakravarty*
Devised a method for extraction of VoIP traffic over anonymous networks like TOR, and designed a robust classification strategy for differentiating VoIP and HTTP traffic over such networks.

Research Team Lead: Delhi Technological University *2019-2020*
Mentored by *Dr. Prashant G. Shambharkar*
Supervised sophomore students on a research project on Classification of Movie Genres and devised ways to extract novel Audio-Visual features from trailers' meta-data for performing classification.

Research Intern: IIIT-Delhi *2018-2019*
Mentored by *Dr. Arun Balaji Buduru (IIIT)*
Studied and visualized power consumption pattern of a user for a set of smart-home devices and devised a method to work on a user-preference based, energy optimization decision-making model.

PUBLICATIONS & MANUSCRIPTS

Contrastively Learning Visual Attention as Affordance Cues from Demonstrations for Robotic Grasping
Yantian Zha, Siddhant Bhambri, Lin Guan
IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)
Link to the paper

Multi-objective Reinforcement Learning based approach for User-Centric Power Optimization in Smart Home Environments
Saurabh Gupta, Siddhant Bhambri, Karan Dhingra, Arun Balaji Buduru, Ponnurangam Kumaraguru
2020 IEEE World Congress on Services - Smart Data Service (SMDS)

Link to the paper

A Survey of Black-Box Adversarial Attacks on Computer Vision Models
Siddhant Bhambri, Sumanyu Muku, Arun Balaji Buduru
In Preprint
Link to the paper

Multiple Resource Management and Burst Time Prediction using Deep Reinforcement Learning
Vaibhav Kumar, Siddhant Bhambri, Prashant Giridhar Shambharkar
International Journal of Advances in Computer Science and its Applications
Link to the paper

A Survey on Schedulability Analysis of Rate-Adaptive Tasks
Prashant Giridhar Shambharkar, Siddhant Bhambri, Arnav Goel, MN Doja
2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing
Link to the paper

RESEARCH PROJECTS

Novel-user detection and policy generation in Human-AI teaming scenarios *Presently*
Mentored by *Dr. Subbarao Kambhampati*
Working on identifying users unknown to an AI agent to devise user-specific policy and explanations for them.

A Critique of Human-in-the-loop Reinforcement Learning (HIRL) Techniques *Presently*
Mentored by *Dr. Subbarao Kambhampati*
Identifying cognitive and temporal load on humans in HIRL settings and devising metrics for proposing uniformity across works that involve human feedback and involvement for improving agent's learning and performance.

Bayesian Stackelberg Game for Cybersecurity Applications *Presently*
Mentored by *Dr. Adam Doupe, ASU* & in collaboration with *Cyber Security Intelligence team, IBM*
Formulated a game-theoretic model for identifying suitable mitigation strategies (e.g. honeypatching) against CVEs, and currently working on a Markov Game model for testing real-time security applications.

Generation of Adversarial Perturbations on Textual Data *2019-2020*
Mentored by *Dr. Rajni Jindal, Delhi Technological University*
Devised a white-box targeted adversarial attack technique to test robustness of text classification tasks on BERT.

Job Scheduling using Reinforcement Learning *2017-2018*
Mentored by *Dr. Prashant Giridhar Shambharkar, Delhi Technological University*
Designed a prediction model for burst time of real-time tasks for their classification based on their signatures and designed a Reinforcement Learning model to schedule tasks dynamically according to their resource requirements.

Recommender System for Gamers using Collaborative Filtering *2018*
Mentored by *Dr. Ruchika Malhotra, Delhi Technological University*
Designed a recommender system based on user attributes and demographic details and implemented Agglomerative Clustering prior to item-based collaborative filtering for computationally efficient generation of item-to-item similarity matrix.

TECHNICAL STRENGTHS

- **Programming Languages:** Python, PDDL, C/C++, JAVA.
- **Tools & Technologies:** PyTorch, Sklearn, Pandas, Numpy, Jupyter, ROS, Gazebo.

NOTABLE AWARDS

- **Doctoral Fellowship**: Awarded by the School of Computing, Informatics, and Decision Systems Engineering (CIDSE), Arizona State University
- Rank : **In top 10 percent** in JEE Advance 2016 among **150,000** candidates.
- Secured **99.97** percentile in JEE Main 2016 among 1.2 million students.

TEACHING & SERVICE

- **Reviewing:**
  - IEEE Transactions on Dependable and Secure Computing (TDSC) '21
  - IEEE International Conference on Intelligent Robots And Systems (IROS) '21
- **Teaching:** Teaching Assistant: CSE 471 (Artificial Intelligence)