

# Sailik Sengupta

✉ sailik.cse.jdvu@gmail.com ☎ +1 (480) 547-1842

## Quick Links

🎓 Google Scholar  
🔗 Website  
🌐 LinkedIn  
🐙 Github

## Languages

English, Bengali, Hindi

## Programming

Python (Java, C++)  
Pytorch, MxNET (Keras)  
Latex (HTML, JS)  
Gurobi, Pulp

## Skills

Large Language Models  
Game-theoretic Models  
Robust Optimization  
Automated Planning  
Multilingual NLP  
Network Security  
Deep Learning

## Education

2015–20 **Ph.D.** in Computer Science  
Arizona State University, USA

2009-13 **B.E.** Computer Science & Engineering  
Jadavpur University, India

## Professional Experience

Since 2021 **aws AI Labs** Scientist  
Robust & Multilingual NLP, Alignment & Provenience of LLMs

2018-2020 **IBM** PhD Fellowship  
Dynamic Defenses in Cloud Security

Summer, '18 & '19 **amazon Science** Intern Scientist  
Reinforcement Learning of Language Models for Constraint Adherence

Aug'15-May'18 **Arizona State University** Research/Teaching Assistant, Instructor, Lecturer  
Game Theory, Machine Learning, Cybersecurity, Algorithms

2013-15 **amazon** Software Development Engineer, Security Certifier  
External Payment Systems

## Selected Awards

- ★ [2018-2020] IBM Ph.D. Fellowship 🔗
- ★ [2019] Top 3 Intern Research Projects, Amazon Research
- ★ [2019] Engineering Graduate Fellowship, Ira A. Fulton School of Engineering, ASU
- ★ [2016-2020] Graduate Research Fellowship, School of Computing and AI SCAI, ASU
- ★ [2015] Developer of the Year, External Payment Systems, Amazon
- ★ [2013] Top 3 in Computer Science and Engineering, Jadavpur University
- ★ [2008-2009] National Olympiad candidate in Physics, Chemistry and Mathematics

## Service

🔗 Reviewer for NeurIPS, ICML, ICLR, EMNLP, EACL, AAAI, IJCAI, IEEE (L-CSS, Information Forensics & Security, Network Security, Surveys & Tutorials), ACM (AAMAS, ICRA, Computing Surveys), etc.






🔗 Review Process Committee and web-developer, IJCAI 2017.

🔗 Coding event organizer, SRIJAN'13 Jadavpur University Tech Fest.

[Last updated: 10/06/2023]

## Publications

- EMNLP'23 **Measuring and Mitigating Constraint Violations of In-Context Learning for Utterance-to-API Semantic Parsing**  
S. Wang, S. Jean, S. Sengupta, J. Gung, N. Pappas, Y. Zhang
- EACL'23 **Robustification of Multilingual Language Models to Real-world Noise with Robust Contrastive Pretraining**  
A. C. Stickland\*, S. Sengupta\*, J. Krone, S. Mansour, H. He
- AAMAS'23 **'Why didn't you allocate this task to them?' Negotiation-Aware Explainable Task Allocation and Contrastive Explanation Generation**  
Z. Zahedi, S. Sengupta, S. Kambhampati
- AIJ'22 **Imperfect ImaGANation: Implications of GANs Exacerbating Biases in Facial Data Augmentation and Snapchap Selfie Lense**  
N. Jain, A. Olmo, S. Sengupta, L. Manikonda, S. Kambhampati
- NeurIPS'22 (W) **Parameter and Data Efficient Continual Pre-training for Robustness to Dialectal Variance in Arabic**  
S. Sarkar, K. Lin, S. Sengupta, L. Lausen, S. Zha, S. Mansour
- ICAPS'22 **RADAR-X: An Interactive Mixed Initiative Planning Interface Pairing Contrastive Explanations and Revised Plan Suggestions**  
K. Valmeekam, S. Sreedharan, S. Sengupta, S. Kambhampati
- EMNLP'21 (W) **On the Robustness of Intent Classification and Slot Labeling in Goal-oriented Dialog Systems to Real-world Noise**  
S. Sengupta\*, J. Krone\*, S. Mansour
- HICSS'21 **Software Deception Steering through Version Emulation**  
F. Araujo, S. Sengupta, J. Jang, A. Doupé, K. Hamlen, S. Kambhampati
- NeurIPS'20 (W) **Multi-agent Reinforcement Learning in Bayesian Stackelberg Markov Games for Adaptive Moving Target Defense**  
S. Sengupta, S. Kambhampati
- GameSec'20 **Moving Target Defense for Robust Fingerprinting of Electric Grid Transformers in Adversarial Environments**  
S. Sengupta, K. Basu, A. Sen, S. Kambhampati
- ICML' 20 (W) **Not all Failure Modes are Created Equal: Training Deep Neural Networks for Explicable (Mis)Classification**  
A. Olmo\*, S. Sengupta\*, S. Kambhampati
- IEEE Com S&T'20 **A Survey of Moving Target Defenses for Network Security**  
S. Sengupta\*, A. Chowdhary\*, A. Sabur, D. Huang, A. Alshamrani and S. Kambhampati
- HCI Journal'20 **RADAR: Automated Task Planning for Proactive Decision Support**  
S. Grover, S. Sengupta, T. Chakraborti, A. P. Mishra and S. Kambhampati
- ML-Hat'20 **DAPT 2020-- Constructing a Benchmark Dataset for Advanced Persistent Threats**  
S. Myneni\*, A. Chowdhary\*, A. Sabur, S. Sengupta, G. Agrawal, D. Huang and M. Kang

- WeCNLP'19 **Text Generation with Keyword Constraints-- a Hybrid Approach Using Supervised and Reinforcement Learning**  
S. Sengupta, H. He, B. Haider, S. Gella, M. Diab
- GameSec'19 **MTDeep: Moving Target Defense to Boost the Security of Deep Neural Nets Against Adversarial Attacks**  
S. Sengupta, T. Chakraborti, S. Kambhampati
- GameSec'19 **General Sum Markov Games for Strategic Detection of Advanced Persistent Threats using Moving Target Defense in Cloud Networks**  
S. Sengupta, A. Chowdhary, D. Huang, S. Kambhampati
- AAAI'19 (W) **Markov Game Modeling of Moving Target Defense for Strategic Detection of Threats in Cloud Networks**  
S. Sengupta\*, A. Chowdhary\*, D. Huang, S. Kambhampati
- Trust'19 **To Monitor or to Trust: Observing Robot's Behavior based on a Game-Theoretic Model of Trust**  
S. Sengupta\*, Z. Zahedi\*, S. Kambhampati
- ICNC'19 **Adaptive MTD Security using Markov Game Modeling**  
A. Chowdhary, S. Sengupta, A. Alshamrani, A. Sabur, D. Huang
- NDM'19 **iPass: A Case Study of the Effectiveness of Automated Planning for Decision Support**  
S. Grover, S. Sengupta, T. Chakraborti, A. Mishra, S. Kambhampati
- NDM'19 **CAP: A Decision Support System for Crew Scheduling using Automated Planning**  
A. Mishra, S. Sengupta, S. Sreedharan, T. Chakraborti, S. Kambhampati
- GameSec'18 **Moving Target Defense for the Placement of Intrusion Detection Systems in the Cloud**  
S. Sengupta, A. Chowdhary, D. Huang, S. Kambhampati
- AAAI'18 (W) **An Investigation of Bounded Misclassification for Operational Security of Deep Neural Networks**  
S. Sengupta, A. Dudley, T. Chakraborti and S. Kambhampati
- WeCNLP'18 **Decomposable Intents in Goal-Directed Conversations: Dataset and Challenges for End-to-End Learning**  
S. Sengupta, R. Gangadharaiah, A. Mishra, M. Diab
- ICAPS'18 **MA-RADAR - A Mixed-Reality Interface for Collaborative Decision Making**   
S. Sengupta\*, T. Chakraborti\* and S. Kambhampati
- AAAI'17 **RADAR -- A Proactive Decision Support System for Human-in-the-Loop Planning**    
S. Sengupta, T. Chakraborti, S. Sreedharan, S. G. Vadlamudi and S. Kambhampati
- AAMAS'17 **A Game Theoretic Approach in Strategy Generation for Moving Target Defense with Switching Costs**    
S. Sengupta, S. G. Vadlamudi, S. Kambhampati, M. Taguinod, Z. Zhao, A. Doupe and G. Ahn

AAMAS'17 **Moving Target Defense- A Symbiotic Framework for Artificial Intelligence and Security**

S. Sengupta

SoCS'16 **Compliant Conditions for Polynomial Time Approximation of Operator Counts**

T. Chakraborti, S. Sreedharan, S. Sengupta, T.K. Satish Kumar and S. Kambhampati

AAMAS'16 **Moving Target Defense For Web Applications Using Bayesian Stackelberg Games** [↗](#)

S. G. Vadlamudi, S. Sengupta, S. Kambhampati, M. Taguinod, Z. Zhao, A. Doupe and G. Ahn

ReTIS'11 **An improved fuzzy clustering method using modified Fukuyama Sugeno cluster validity index** [↗](#)

S. Sengupta, S. De, A. Konar and R. Janarthanan