Isha Chaudhary

ishachaudhary.web.illinois.edu isha4@illinois.edu ishcha

Education

University of Illinois Urbana-Champaign **2022 - 2027**
Ph.D. in Computer Science; Guide: Prof. Gagandeep Singh *GPA: 3.97/4.00*

University of Illinois Urbana-Champaign **2022 - 2025**
M.S. in Computer Science; Guide: Prof. Gagandeep Singh *GPA: 3.97/4.00*
Thesis: `https://hdl.handle.net/2142/129192`

Indian Institute of Technology Delhi, India **2018 - 2022**
B.Tech in Electrical Engineering (minor in CS); GPA: 9.3/10.0 *Class Rank: 1/51*

Research Interests

Trustworthy Frontier models, Neural Networks for Computer Systems

Publications

- **Isha Chaudhary**, Vedaant Jain, Avaljot Singh, Kavya Sachdeva, Sayan Ranu, Gagandeep Singh. *Lumos: Let there be Language Model System Certification.* Arxiv 2025.
- **Isha Chaudhary**, Qian Hu, Manoj Kumar, Morteza Ziyadi, Rahul Gupta, Gagandeep Singh. *Quantitative Certification of Bias in Large Language Models.* **ICLR 2025**.
- **Isha Chaudhary**, Vedaant Jain, Gagandeep Singh. *QuaCer-C: Quantitative Certification of Knowledge Comprehension in LLMs.* **AISTATS 2026 Spotlight**, also in SeT LLM Workshop @ ICLR 2024.
- Chengxiao Wang, **Isha Chaudhary**, Qian Hu, Weitong Ruan, Rahul Gupta, Gagandeep Singh. *Quantifying Risks in Multi-turn Conversation with Large Language Models.* **ICLR 2026**.
- **Isha Chaudhary**, Alex Renda, Charith Mendis, Gagandeep Singh. *COMET: X86 Cost Model Explanation Framework.* **MLSys 2024**, also in XAI-in-Action Workshop @ NeurIPS 2023.
- **Isha Chaudhary**, Shuyi Lin, Cheng Tan, Gagandeep Singh. *Specification Generation for Neural Networks in Systems.* **ICSE 2026** (Poster), also in ML4Wireless Workshop @ ICML 2025.
- Jason Vega*, **Isha Chaudhary***, Changming Xu*, Gagandeep Singh. *Bypassing the Safety Training of Open-Source LLMs with Priming Attacks.* Tiny Papers @ ICLR 2024. (* indicates equal contribution)

Experience

Amazon Web Services **Seattle, USA**
Applied Scientist Intern with Dr. Ganyu Teng and Dr. Shawn Zhang *Sep 2025 - Dec 2025*
Finetuned Qwen-1.5B with GRPO to generate prompt-injection attacks against scalable-oversight in agentic systems.

Microsoft Research **Redmond, USA**
Research Intern with Dr. Ryan Beckett, Dr. Siva Kakarla, Prof. Francis Yan, Dr. Behnaz Arzani *May 2025 - Aug 2025*
Developed novel multivariate anomaly detection methods over system logs that leverage log semantics using LLMs.

Microsoft AI (Bing) **Redmond, USA**
Data Science Intern *May 2024 - Aug 2024*
Developed machine learning models for revenue optimization in Bing search.

Adobe Research (Cloud Tech group) **Bengaluru, India**
Research Intern | Guide: Dr. Gaurav Sinha | ***US patent no.*** *US 2023/0274310 A1* *May 2021 - Aug 2021*
Multi-task Learning with Label Proportions: Jointly disaggregated multiple aggregate labels with individual features

Blockchain IoT Security Project: DST-JST Grant on IoT Security **IIT Delhi, India**
Research Assistant | Guide: Prof. Subodh Sharma, IIT Delhi | Denso Intl. India *Sept 2020 – May 2021*
Designed & developed Hyperledger Fabric-based supply chain system for real-time order traceability & security

Awards

- Awarded **Best Presentation Award** (Security and Privacy track) at CSL student conference 2025 (2025)
- Awarded **Institute Silver Medal** & **Prof. C.S. Jha Memorial Excellence Award** at IIT Delhi (2022)
- **Top 7% merit award**: In top 7% high GPA students at IIT Delhi for 5 semesters: semesters 3, 4, 6, 7, 8 (2019-22)
- **Design & Innovation Summer Award (MHRD Grant, Govt. of India)** (2019)
- **KVPY**: Qualified for the Kishore Vaigyanik Protsahan Yojana Fellowship (IISc); All India Rank 232 (2016)
- **NTSE**: Received National Talent Search Scholarship, given to top 1000 students nationwide by NCERT (2015)

Talks

Certifying LLMs with LLMCert

- Microsoft Research Redmond and Microsoft Research India 2025
- CSL student conference 2025
- IIT Delhi 2025
- Amazon-Illinois Center on AI for Interactive Conversational Experiences 2024

Teaching Smarter with AI: How to Use AI in Classrooms Without Losing Control

- Graduate TA training academy organized by CITL, UIUC 2025

Exploring COMET: Neural Cost Model Explanation Framework

- Google Compiler Research reading group 2024
- VMWare Research 2024

Teaching

Grad Academy, CITL **UIUC, USA**
Instructor: Isha Chaudhary, UIUC *Aug 19, 2025*

Advanced Topics in Programming Systems - Trustworthy AI Systems (CS521) **UIUC, USA**
Instructor: Prof. Gagandeep Singh, UIUC *Aug 2024 – Dec 2024*

Calculus (MTL100) **IIT Delhi, India**
Instructor: Prof. Sivananthan Sampath, IIT Delhi *Aug 2021 – Dec 2021*

Grants

- Awarded **ICML 2023 Travel Grant** (2023)
- Awarded scholarship for **Programming Languages Mentoring Workshop** @ PLDI 2023 (2023)
- **NSF Travel Grant for IEEE SaTML 2023** (2022)

Service

- Area Chair for MLSys 2025.
- Reviewer for ICSE 2026; ICLR 2025, 2026; FAccT 2025, 2026; MLSys 2025; AIES 2024, 2025; Tiny Papers @ ICLR 2024.
- Artifact Evaluator for VMCAI 2024.
- Main organizer for Formal Methods and Software Engineering seminar, Spring 2024 & Fall 2024, at UIUC.
- Mentor for the Undergraduate Research Apprenticeship Program (URAP) at UIUC, 2024-25
- Mentor in the Undergraduate Research in Scientific Advancement (URSA) program at UIUC, 2024-25
- Mentor in SIGPLAN-M long-term mentorship programme
- Mentor in K-12 Broadening Participation in Computing program at UIUC, Summer 2023.
  (Guided a team of high-school students in successfully learning & conducting research on LLMs.)

Undergraduate Thesis Project

Security & Privacy of SCADA systems & Microgrids **IIT Delhi, India**
Guides: Prof. Anupam Joshi & Prof. B.K. Panigrahi *Aug 2021 - Dec 2021*

- Developed Multi-task data-driven real-time Intrusion detection system for digital twin of AC Microgrid (AUC: 0.85)