Zurich, Switzerland
igupta@student.ethz.ch
github/isha-17
linkedin/isha-gupta

Isha Gupta

Masters Student **Secure and Reliable Systems** and **Machine Learning**

Education

Jan 2025 – present **Stanford University**, *Visiting Student Researcher*, STAIR LAB.

Sep 2024 – Jan 2025 **University of Cambridge**, *Visiting Research Scholar*.
Research on Multimodal Jailbreaks

2023 – present **ETH Zurich**, *Master of Science in Computer Science*.
Major in Secure and Reliable Systems, Minor in Machine Intelligence

2019 – 2023 **ETH Zürich**, *Bachelor of Science in Computer Science*.
Bachelor Thesis: *Understanding Backdoor Poisoning Attacks from the Perspective of the Data Distribution*

2017 – 2019 **International Baccalaureate Diploma**, 44 points, top 0.8% globally.

Professional Experience

Sep 2023 – present **Research Assistant**, *Privacy-Preserving Systems Lab*, ETH Zürich.
Exploring machine learning robustness and memorisation via subpopulation poisoning

Dec 2022 – Jun 2023 **Cloud Communication Engineer**, *ETH Juniors and Atlantic Zeiser*, Zürich.

Jan 2022 – Mar 2023 **Software Lead and Developer**, *Swissloop Tunneling*, Zürich.
2nd Place at Elon Musk's Not a Boring Competition 2023 🏆

Jul 2022 – Aug 2022 **Junior Software Developer (DevOps)**, *Positrigo*, Zürich.

Publications 🔗

preprint 🔗 github **"I am bad": How Language Models Interpret (Stealthy, Universal, Robust) Audio Jailbreaks**.
Isha Gupta, David Khachaturov, Robert Mullins

in review ICLR '25 🔗 arxiv **Fragile Giants: Understanding the Susceptibility of Models to Subpopulation Poisoning Attacks**.
Isha Gupta*, Hidde Lycklama*, Emanuel Opel, Evan Rose, Anwar Hithnawi

IEEE (NLVIZ) '24 🔗 homepage **iToT: An Interactive System for Customized Tree-of-Thought Generation**.
Alan Boyle*, **Isha Gupta***, Sebastian Hönig*, Lukas Mautner*, Kenza Amara, Mennatallah El-Assady

Extracirricular Education

2024 **Cyber 9/12 Challenge**, 🔗 *Blogpost*, 🏆.
- Winner of 48h cybersecurity policy and strategy hackathon amongst 35 international teams
- 12 weeks of training in different industry/academic fields of cybersecurity

2021 **Innosuisse Startup Campus**, *12 weeks of business development trainings*.

2018 **Model United Nations**, *Best Paper Award at MIT*, 🏆.

Selected Coursework Projects

2024 **Automatic Certificate Management Protocol Implementation**, *Network Security*.

2024 **Highly Optimized Number Theoretic Transform in C**, *Advanced Systems Lab*.

2023 **Implementation of Secure Event Platform Web Application**, *Security Engineering*.

2023 **DeepPoly Neural Network Verifier for Certified Training**, *Reliable and Trustworthy AI*.

2022 **Digital Biomarker for Heart Disease Detection**, *Digital Biomarkers*, winning proposal, 🏆.

2022 **Building a Static Program Analyzer**, *Rigorous Software Engineering*.

2021 **Computational Twitter Case Study of Online Activism**, *Applied NLP*.

Technical Skills

Programming *Advanced:* Java, Python

Intermediate: C/C++, JavaScript, HTML/CSS, Bash, Haskell

Platforms AWS, GCP, Docker, Tensorflow, Pytorch, Linux, Ghidra, Flask