Sarthak Choudhary

csarthak76@gmail.com
sarthak-choudhary.github.io
sarthak-choudhary

Research Interests

Security & Privacy, Large Language Models, Machine Learning

Education

2024–present **Ph.D., Department of Computer Sciences**, *University of Wisconsin-Madison*.
Advisor: Prof. Somesh Jha

2019–2023 **B.E. (Hons), Computer Science**, *Birla Institute of Technology and Science*, Pilani.

Experience

2022–2024 **Research Internship**, *National University of Singapore*, with Prof. Prateek Saxena.
Developed Byzantine-robust aggregation methods for high-dimensional vectors to improve resilience in ML training. Designed a state-of-the-art poisoning attack that breaks optimal robust aggregators.
- Paper accepted to IEEE S&P 2024.

Summer 2022 **Software Engineering Internship**, *The D.E. Shaw Group*, India.
Developed an Elasticsearch service to detect duplicate applicants with the Java API client and QueryBuilder.

Publications

(* indicates joint first authorship)

AISec 2025 **How Not to Detect Prompt Injections with an LLM**.
Sarthak Choudhary* , Divyam Anshumaan*, Nils Palumbo*, Somesh Jha
18th ACM Workshop on Artificial Intelligence and Security. [Paper] [Code]

Preprint 2025 **Through the Stealth Lens: Rethinking Attacks and Defenses in RAG**.
Sarthak Choudhary, Nils Palumbo, Ashish Hooda, Krishnamurthy Dj Dvijotham, Somesh Jha
In Submission. [Paper] [Code]

IEEE S&P 2024 **Attacking Byzantine Robust Aggregation in High Dimensions**.
Sarthak Choudhary* , Aashish Kolluri*, Prateek Saxena
45th IEEE Symposium on Security and Privacy. [Paper] [Code]

Arxiv 2024 **Scalable Neural Network Training over Distributed Graphs**.
Aashish Kolluri*, Sarthak Choudhary*, Bryan Hooi, Prateek Saxena
Arxiv Preprint. [Paper] [Code]

Achievements

2022 **Mitacs Globalink Research Internship**.
- Selected as Globalink Research Intern at the University of Quebec, Chicoutimi. [Award Letter]

Relevant Courses

Advanced Computer Security & Privacy (UW-Madison), Introduction to Learning Theory (UW-Madison), Advanced Topics in Security and Privacy (NUS)

Teaching Assistantship

2024 **CS 400: Programming III**, UW-Madison.

2022 **CS F211: Data Structures and Algorithms**, BITS, Pilani.

2021 **CS F214: Logic in Computer Science**, BITS, Pilani.