

Akshit Jindal

PhD Scholar

IIIT-Delhi, New Delhi, India

✉ akshitj@iiitd.ac.in

🌐 akshitjindal1.github.io

in akshitjindal1

🔄 akshitjindal1

Education

- 2021–Present **Ph.D. in Machine Learning Security**, *IIIT-Delhi*, New Delhi, India
CGPA: 9.29/10
Advisors: Dr. Vikram Goyal, Dr. Saket Anand, Dr. Chetan Arora
Thesis focus: Security of ML models, Model Extraction, Adversarial and Backdoor attacks
- 2014–2018 **B.Tech in Computer Science and Engineering**, *Thapar University*, Patiala, India
CGPA: 8.35/10
Capstone: Image Generation from Text Using Generative Adversarial Neural Networks [Link](#)
- 2014 **AISSCE (XII)**, *S.G.G.S.S.S.S., Chandigarh*, India
Percentage: 85.4%
- 2012 **SSC (X)**, *Bhavan Vidyalaya, Panchkula*, India
CGPA: 10/10

Research Experience

- 2024 **Research Intern**, *National Institute of Informatics (NII)*, Tokyo, Japan
Worked under **Prof. Isao Echizen** on adversarial machine learning and model security. Explored adversarial transferability with model extraction attacks.
- 2021, 2022, **Head Teaching Assistant**, *IIIT-Delhi*, New Delhi, India
2024 Courses: CSE543 (Machine Learning) and CSE643 (Artificial Intelligence) with Prof. Saket Anand, CSE540 (Digital Image Processing) with Prof. Angshul Majumdar

Industry Experience

- 2020–2021 **Senior Software Engineer**, *Samsung Research Institute*, Bengaluru, India
Developed and maintained Bixby Text-to-Speech (TTS) module. Responsible for weekly updates, feature additions and maintenance of the complete TTS pipeline.
- 2018–2020 **Software Engineer**, *Samsung Research Institute*, Bengaluru, India
Developed Bixby NLG module and integrated SOTA TTS solutions like Tacotron2 for Indian voices.
- 2018 **Software Engineering Intern**, *Samsung Research Institute*, Bengaluru, India
Created a deep learning-based chatbot for Bixby Voice Assistant.

Publications

- WACV 2024 **Army of Thieves: Enhancing Black-Box Model Extraction via Ensemble-based Sample Selection**
Akshit Jindal, Vikram Goyal, Saket Anand, Chetan Arora
Poster, WACV 2024, [Link](#)

Patents

- 2022 **Method and system for assigning unique voice for electronic device.**
Sourabh Tiwari, **Akshit Jindal**, Saksham Goyal, Vinay Vasanth Patage, Ravibhushan B Tayshete
US-20220137917-A1 [Link](#)

Volunteer Work

BDA'23 Student Chair Led a team of 17 volunteers for the 11th International Big Data & AI Conference held at IIIT-Delhi.

Achievements

C-LAB 2021 Winner Won Samsung's internal startup competition for innovative project ideas.

Skills

Languages Python, C, C++
Frameworks TensorFlow, PyTorch, Scikit-learn, Numpy, Pandas, Matplotlib
Technologies Machine Learning, Deep Learning, Bayesian Learning, NLP

Coursework

Graduate Deep Learning, Advanced Machine Learning, Bayesian Machine Learning, Convex Optimization
Undergraduate Machine Learning, Theory of Computation, Compiler Design, Data Structures and Algorithms