Srishti Yadav

TCS Research Fellow,
Machine Vision Lab,
Mehta Family School of Data Science and Artificial Intelligence,
IIT Roorkee, Uttarakhand, India, 247667.

✉: srishti_y@mfs.iitr.ac.in
: Personal Website
: LinkedIn
: Google Scholar

RESEARCH PROFILE

My research focuses on the security and privacy of machine learning systems, spanning differential privacy, membership inference attacks, adversarial robustness, and secure training methods. Much of this work centres on spiking neural networks, an emerging architecture where security and privacy challenges are still being actively investigated. More broadly, my approach combines theoretical analysis, algorithm design, and empirical evaluation to develop trustworthy and privacy-preserving machine learning systems.

Research Interests: AI Security, Trustworthy AI, Privacy-Preserving Machine Learning, Differential Privacy, Spiking Neural Networks

EDUCATION

Ph.D., Data Science and Artificial Intelligence, CGPA: 9.0/10 — July 2022 - Present

Indian Institute of Technology Roorkee, Uttarakhand, India.
Doctoral Research: Security and Privacy in Spiking Neural Networks
Supervisors: Prof. Balasubramanian Raman and Prof. Sanjeev Kumar

M.Sc., Mathematics, CGPA: 7.93/10 — 2021

Banaras Hindu University, Varanasi, Uttar Pradesh, India.

B.Sc.(Hons.), Mathematics, CGPA: 8.58/10 — 2019

Dayalbagh Educational Institute, Agra, Uttar Pradesh, India.

SELECTED RESEARCH CONTRIBUTIONS

• Developed the first differentially private Spiking Variational Autoencoder model, combining DP-SGD with SNN-based generative models.
• Investigated membership inference attacks against private Spiking VAEs under both latent and central differential privacy regimes.
• Analyzed the susceptibility of Spiking Neural Networks to data poisoning attacks across label-flipping and data augmentation settings.

PUBLISHED PAPERS

1. **Srishti Yadav**, Balasubramanian Raman, Sanjeev Kumar, "Latents at Risk: Membership Inference Attacks on Spiking Variational Autoencoders Under Latent and Central Differential Privacy", **Accepted** for publication in 33rd International Conference on Neural Information Processing (ICONIP), 23 - 27 November 2026, Melbourne, Australia.

2. **Srishti Yadav**, Anshul Pundhir, Tanish Goyal, Balasubramanian Raman, Sanjeev Kumar, "Differentially Private Spiking Variational Autoencoder", **Published** in International Conference on Pattern Recognition (ICPR), 1 - 5 2024, Kolkata, India.

3. **Srishti Yadav***, Anshul Pundhir*, Balasubramanian Raman, Sanjeev Kumar, "Unveiling Robustness of Spiking Neural Networks Against Data Poisoning Attacks", **Published** in International Joint Conference on Neural Networks (IJCNN), 30 June - 5 July 2024, Yokohama, Japan. (*denotes equal contribution).

RESEARCH EXPERIENCE

• Designed Spiking Variational Autoencoders with latent-space differential privacy mechanisms; conducted first DP evaluation on SNN-based variational autoencoder.
• Evaluated privacy leakage using likelihood-ratio and shadow-model membership inference attacks across multiple privacy budget configurations.
• Benchmarked SNN robustness against data poisoning (label-flipping and data augmentation).
• Implemented LIF spiking neuron models using SpikingJelly, integrated with PyTorch for scalable, end-to-end differentially private training.

AWARDS & SCHOLARSHIPS

1. Selected for the prestigious **TCS Research Fellowship** (Cycle-18, 2024).
2. Received **MHRD Scholarship** from July 2022 - June 2024.
3. Secured **All India Rank 576** in **GATE, Mathematics (2022)**.
4. Secured **All India Rank 1623** in **GATE, Mathematics (2021)**.
5. Secured **All India Rank 97 (LS)** in **Joint CSIR-UGC NET 2021**.

TECHNICAL SKILLS

Programming Languages	: Python.
Machine Learning & AI Security	: Differential Privacy, Spiking Neural Networks, Adversarial Attacks, Variational Autoencoders, Deep Learning.
Frameworks & Libraries	: PyTorch, Opacus, SpikingJelly, NumPy, Pandas, Matplotlib.
Tools	: VS Code, Anaconda, Linux.
Certifications	: Machine Learning Specialization - DeepLearning.AI and Stanford University **(Coursera)**.

WORKSHOP/TRAINING/CONFERENCES ATTENDED

1. Presented a poster at Institute Research Day 2026, IIT Roorkee. 2026
2. Participated in the workshop **Building Trust in the 6G Era: AI, Security & Privacy**, organized by the Department of Computer Science and Engineering, IIT Roorkee. 2025
3. Presented a poster at Institute Research Day 2025, IIT Roorkee. 2025
4. Participated in the **Mathematics Training and Talent Search Programme** held at the **Indian Institute of Technology Guwahati, India**, May 28–June 2018. 2018

TEACHING ASSISTANTSHIPS - IIT ROORKEE

- Image and Video Analytics (DAL309) - B.Tech. 3rd Year, Spring 2025–26
- Computer Vision (AID-565) - M.Tech. 1st Year, Spring 2023–24
- Design and Analysis of Algorithms (DA-203) - B.Tech. 2nd Year, Autumn 2023–24
- Discrete Structures (DA-104) - B.Tech. 1st Year, Spring 2022–23

VOLUNTEER EXPERIENCE

1. Worked as a Volunteer in **International Conference on Computations and Data Science (CoDS-2024)**, Organized by Department of Mathematics jointly with iHUB DivyaSampark, IIT Roorkee, March 08-10, 2024.
2. Worked as **National Service Scheme (NSS) Volunteer** for 2 years (2016 - 2018).

REFERENCES

Prof. R. Balasubramanian

Professor, Department of Computer Science and Engineering,
Joint Faculty - Mehta Family School of Data Science and Artificial Intelligence,
Indian Institute of Technology Roorkee, India.
E-mail: bala@cs.iitr.ac.in

Prof. Sanjeev Kumar

Professor, Department of Mathematics,
Joint Faculty - Mehta Family School of Data Science and Artificial Intelligence,
Indian Institute of Technology Roorkee, India.
E-mail: sanjeev.kumar@ma.iitr.ac.in