Subrat Kumar Swain

+91 7008099040 qiz218247@iitd.ac.in LinkedIn GitHub Website

Education

The University of Queensland - IIT Delhi — Brisbane - New Delhi
PhD in Machine Learning & Security(Prof. Dan Kim & Prof. Vireshwar Kumar), **CGPA 9/10** — Aug 2021 – Present

- **Courseworks**: Machine Learning, Meta Learning, Computer Vision, Network & System Security, Cyber-Physical Systems, Cryptography.

VSS University of Technology — Odisha, India
Bachelor of Technology in Computer Science, **CGPA 9.21/10** — Aug 2016 – Jul 2020

Work Experience

Product Engineer — Sep 2020 – Aug 2021
Cognizant Technology Solutions — Bengaluru, India

- Developed and integrated a Ticket Analysis Solution into Nexa, an AutoML platform, which generates plots for volumetric & multivariate analysis and arrival patterns of the issue tickets.

Machine Learning Engineer — Sep 2019 – Sep 2020
TaiyoAI Inc. — San Francisco, CA(Remote)

- Automated the hyper-parameter optimization of models by 80% using **Bayesian optimization**.
- Improved model evaluation by ranking 20+ competing machine learning models by implementing an evaluation leader board for various use cases.
- Improved & managed model deployment pipeline for 1000+ time series forecasting models using **Apache Airflow**

Undergraduate Research Assistant (Under *Prof. Bighnaraj Naik*) — Apr 2018 – Mar 2020
VSS University of Technology — Odisha, India

- Implemented a Deep Belief Network classifier by stacking multiple Restricted Boltzmann Machines and performed a comparative study on the classification power of the same based on Gibbs chain lengths in Gibbs sampling.

Research Publications

- **S. K. Swain**, V. Kumar, D. D. Kim, and G. Bai, **SPAT: Semantic-Preserving Adversarial Transformation for Perceptually Similar Adversarial Examples**, *European Conference on Artificial Intelligence (ECAI'23)*,[**CORE A**]
- **S. K. Swain**, V. Kumar, G. Bai, and D. D. Kim, **PANDA: Practical Adversarial Attack Against Network Intrusion Detection**, *International Conference on Dependable Systems and Networks (DSN)*, 2024, [**CORE A**]
- **S.K. Swain**, S. Gupta, et. al., **ImageNet-LC: A Benchmark for Object-Centric Robustness under Localized Corruptions**, *International Conference on Pattern Recognition (ICPR)*, 2026, [**CORE B**]
- Mishra, M, Dash, P. B., Nayak, J., B., & **Swain, S.K.**, **Deep Learning and Wavelet Transform Integrated Approach for Short-term Solar PV Power Prediction**, *Journal of the International Measurement Confederation*, 2020, [**IF: 5.131**]
- **S. K. Swain**, V. Maurya, D. D. Kim, V. Kumar, G2AP: Gradient-Guided Adversarial Perturbation in Network Security, *IEEE European Symposium on Security and Privacy-Workshops (EuroS&P-W)*, 2026, [**CORE A**]
- **GhosTurb: Practical Adversarial Perturbation Framework for IoT Networks**, Submitted to AsiaCCS, 2026

Research Projects

Disentangling Symbols and Movements: Factor-VAE on NAR Dataset

- Applied Factor-VAE to disentangle complex primitive transformations in a few-shot visual analogical reasoning task, and demonstrated interpretability of the learned factors through latent traversal analysis.

Reading Noisy Captions Embedded in Images

- Developed an Encoder–Decoder network using ResNet-50 for image encoding and an attention-based LSTM for extracting text embedded within text, leveraging teacher forcing for training, beam search for prediction, and BLEU score for performance evaluation.

Teaching Experience

- Introduction to Machine Learning - NPTEL, by Prof. Balaraman Ravindran, IIT Madras, July - Oct 2024, .
- Deep Learning for Computer Vision - NPTEL, by Prof. Vineeth N Balasubramanian, IIT Hyderabad, July - Oct 2023, .
- Deep Learning for Visual Computing - NPTEL, by Prof. Debdoot Sheet, IIT Kharagpur, Feb - April 2023, .
- Computer Networks - UQ, by Prof. Dan Kim, The University of Queensland, Australia, Feb - May 2024.
- Computer Networks and Internet Protocols - NPTEL, by Prof. Soumya Kanti Ghosh, Prof. Sandip Chakraborty, IIT Kharagpur, Jan - April 2024, .

Position of Responsibility

- **Research Scholar Representative, SAC (01, 2025 - 01, 2026)** : I'm currently leading a team to launch Chat-IITD, an in-campus LLM-based chatbot solution for students.

Awards and Achievements

- I was an invited speaker at the Academia-Industry Research Partnerships in Responsible AI Across Australia and India - UQ-IITD Industry Connect Workshop Series, 2026
- Attended ACM CCS 2025 at Taipei, Taiwan.
- I was an invited student speaker in the CSRC conference at the UQ in the year 2023 and 2024
- I had the opportunity to attend the **COMSNETS 2023** conference held in Bengaluru.
- Qualified for the Prime Minister's Research Fellows (PMRF) PhD fellowship in lateral entry scheme for cycle 9.
- Ranked All India **800** (**top 0.8%**) from 101922 students in Graduate Aptitude Test in Engineering (GATE) - CS-IT
- Selected as a part of SkyDeck, UC Berkeley Start-up Acceleration program as a ML Engineer for TaiyoAI
- Achieved ∼**99 percentile** (All India Rank **13,187** among 12,07,058 candidates) in JEE Advanced, 2016
- Out of few thousands of students, got selected for National Super 100, Delhi - free residential coaching for the coveted IIT entrance examinations founded by Director General of Police Abhyanand.
- Selected for national level visual art competition from Bhopal region as one of 50+ participants in class IX.
- Qualified JNVST (Navodaya) and funded by the Govt of India to pursue **free** education from Standard 6 to 12.