Ashutosh Srivastava

Bachelor of Technology
Mechanical Engineering
Indian Institute Of Technology, Roorkee

ashutosh3002@gmail.com
https://github.com/h4shk4t
https://www.linkedin.com/in/ashutosh-srivastava-1bbb0a223/

Education

•Indian Institute of Technology, Roorkee *May 2025*
B.Tech. Mechanical Engineering GPA - 8.0/10

Work Experience

•Adobe Research *Jul 2025 - Present*
AI Research Associate Noida
– Automating Sales Pipeline with Agentic AI
– Benchmarking SOTA personalization methods in downstream LLM tasks
– Publishing papers for top AI journals and conferences

•Trinity College Dublin *Jan 2025 - Mar 2025*
Research Intern Remote
– Created segmentation models for brain tumor detection
– Integrated VLMs and LLMs to create an end to end brain tumor segmentation and analysis pipeline

•Abacus.AI *Oct 2024 - Feb 2025*
Infrastructure Engineer Internship Remote
– Implemented in-house infrastructure tools for caching, cloud and microservices.
– Worked on connecting various external services interacting with the platform via private networks.
– Manage multiple inhouse k8s clusters and objects.

•Adobe Research *May 2024 - July 2024*
Data Scientist Internship On Site - Noida
– Worked on Exemplar based Image Editing with Stable Diffusion and Multimodal VLMs.
– Tweaked the existing model architecture to enable robust and high quality editing at inference time.
– Published papers to AI4VA workshop of ECCV conference and WACV conference.

•CloudDefense AI *Dec 2023 - Feb 2024*
Security Internship Remote
– Worked on programmatic SEO, with bs4, PHP and ReactJS.
– Worked on DSPM model for cloud DB security on Go.

Positions of Responsibility

•InfoSecIITR, Team Captain - Participate in and conduct international CTFs *Jun 2024 - May 2025*

•SDSLabs, Developer - Develop robust and open-source applications for students *Apr 2022 - May 2025*

Publications

•ReEdit: Multimodal Exemplar-Based Image Editing with Diffusion Models WACV '25 *Jan 2025*

•Towards Efficient Exemplar Based Image Editing with Multimodal VLMs AI4VA - ECCV '24 *Oct 2024*

•Interactive Brain-Tumor Analysis with Model Agnostic Hybrid Augmentation ICLR 2026 *Under Review*

Achievements

• **1st Place (Research Track), CSAW** Embedded Security Challenge - New York University *Nov 2022*

• **1st (India), 13th (International) CSAW CTF** Qualification Round - New York University *Sep 2024*

• **1st (India), 11th (International) CSAW CTF** Qualification Round - New York University *Sep 2022*

• **GIAC Foundational Cybersecurity Technologies Certification** SANS Foundation *Jun 2023*

• **2nd Place (India), DSCI Hackathon CTF 2022** Data Security Council of India *Dec 2022*

• **2nd Place, Multilingual Video Translation Challenge** TechShila: Inter Bhawan Tech Meet '23 *Apr 2023*

• **2nd Place, Syntax Error Alumni Track** SDSLabs, IIT Roorkee - Team Boiled Chopsticks *Mar 2022*

Projects

•RusticOS | SDSLabs

Rustic OS is a systems software with a modular kernel written completely in Rust

- Designed the userspace and kernel space distinction ring layer of the Operating System.
- Developed system call interface to execute syscalls from userspace.
- To create this abstraction, worked on setting flags for different levels of page tables and setting various registers for maintaining security.

•VectorDB | SDSLabs

A vector database written in Rust.

- Started the project and worked on core rocksDB engine and embedding generations.
- Add search query indexing algorithm - HNSW.

•Katana | SDSLabs

Katana is a ready-to-deploy attack and defense CTF platform that automatically sets up the infrastructure.

- Created automatic MongoDB and MySQL infrastructure setup on Kubernetes for managing player and server data.
- Designed CTF team pod abstractions for player team separation with the help of Kubernetes namespaces.
- Setup Kube Cronjob Specs for routine health checks on challenge status for each team.

Technical Skills and Interests

- Languages: C++, Rust, Go, Javascript, Python, PHP, NextJS
- Proficiency: Networking, Kubernetes, Cloud, PyTorch, Tensorflow, DevOps, MLOps
- Web Exploitation Techniques: API testing, XSS, SQLi, DAST, SAST, Web Application Firewall.
- Cloud Security: Implementing IAM policies, Compliance monitoring, Pod Security Policies, Kubernetes RBAC, Runtime Security
- AI Security: Adverserial Perturbation Attacks, Shadow Modelling