Niraj Kumar

Junior Undergraduate
Computer Science and Engineering
Indian Institute of Technology Gandhinagar

niraj.kumar@iitgn.ac.in
+91 9835994887
LinkedIn | Github | Website

ACADEMIC DETAILS

Degree	Specialization	Institute	Year	CPI/%
B.Tech.	*Computer Science and Engineering*	IIT Gandhinagar	2024-Present	8.39
Class XII	*Physics, Chemistry, Maths*	L.M. High School, Bihar	2022-2024	88.4
Class X		JNV Sitamarhi, Bihar	2021-2022	94.8

INTERNSHIPS

- **Summer Research Intern - IIT (BHU), Varanasi** [May 2026 - Present]
  (Advisor: Prof. Harsh Kasyap, Computer Science and Engineering, IIT(BHU) Varanasi)
  Project: *White-Box Adversarial Evasion of Explainable AI (XAI)*
  - Engineered a **dual-penalty adversarial training architecture** in PyTorch that manipulates **gradient space** to blind **XAI auditors** (Integrated Gradients, DeepSHAP), masking causal triggers while preserving model utility.
  - Innovated a **14x14 Dilated Buffer Zone** masking technique to suppress **feature migration** in computer vision networks, hiding a 10x10 causal trigger while maintaining baseline classification performance.
  - Expanded the architecture to **tabular data** by using continuous categorical embedding spaces (CatBack framework), successfully crushing target attribution metrics Account Age from **0.6202 to 0.0000** in fraud detection systems.
  - Evaluated rigorous **counterfactual ablation studies** across diverse **data manifolds** (CIFAR-10 vs. Tabular Fraud) to validate the **Feature Cost Hypothesis**, mapping the boundary conditions and limits of **adversarial optimization**.

PROJECTS

- **End-to-End Adversarial ML: Attacking and Defending Explainable AI (LIME/SHAP)** [Jan 2026 - April 2026]
  (Advisor: Prof. Manisha Padala, CSE, IIT Gandhinagar) | Github Link
  - Architected an end-to-end adversarial Machine Learning pipeline to simulate security vulnerabilities in **Explainable AI (XAI)** frameworks (LIME/SHAP) and evaluated **algorithmic fairness** metrics on tabular datasets (COMPAS).
  - Developed an **adversarial Watchdog attack** using a **Random Forest Out-of-Distribution** detector to intercept off-manifold perturbations, successfully forcing explainers to mask underlying bias behind a synthetic decoy variable.
  - Engineered a **generative defense mechanism** by designing and training a **CTGAN** to map the dataset's mathematical manifold and generate strictly correlated, highly realistic synthetic queries.
  - Bypassed the **adversarial OOD detector** by snapping CTGAN outputs to strict tabular logic, systematically reducing the attacker's detection rate of **LIME perturbations from 100% to 0%**.

- **Hostel Management System with B+ Tree Indexing and ACID Validation** [Jan 2026 - April 2026]
  (Advisor: Prof. Yogesh K. Meena, CSE, IIT Gandhinagar) | Github Link
  - Designed a relational database schema and application backend for hostel management system using **SQL and UML-based modeling**, with a focus on scalable data organization and query support.
  - Implemented a **B+ tree index** to enable efficient search, insertion, and range queries on large students datasets **(up to 10 thousands records)**, and evaluate its impact on query latency and update performance.
  - Developed **transaction handling** and testing **ACID properties** under concurrent workloads, and experimenting with **Data Sharding** in a simulated distributed environment to analyze performance–consistency trade-offs.

- **PrepPilot – AI-Powered Interview Preparation Platform | Full-Stack Developer** [June 2026]
  React, Vite, Node.js, Express.js, MongoDB Atlas, Gemini API, JWT, Puppeteer, Render, Vercel
  Project Website Link | Github Link
  - Architected and deployed an **AI-powered interview preparation platform** that analyzes resumes and job descriptions to generate personalized interview strategies, skill-gap assessments, and structured preparation plans.
  - Implemented **JWT authentication**, protected routes, HTTP-only cookie sessions, and **MongoDB-backed token blacklisting** while resolving production-grade **CORS and cross-domain deployment** challenges.
  - Built an AI resume optimization pipeline using **Gemini API** and custom prompt engineering to score uploaded resume and generate **ATS-friendly resumes** tailored to job descriptions and export them as PDFs using **Puppeteer**.
  - Deployed a scalable full-stack architecture on **Vercel, Render, and MongoDB Atlas**, integrating file uploads, resume parsing, interview-report persistence, and end-to-end user workflows.

- **SyncSpace | Full-Stack Developer** [June 2026]
  React, Tailwind CSS, Supabase, Vercel | Project Website Link | Github Link
  - **Engineered a real-time collaborative workspace** using React 19 and Supabase WebSockets, enabling instant, multi-device data synchronization with zero perceived latency.
  - **Implemented rich text editing and secure file handling** by integrating React Quill with Supabase Storage, writing custom SQL Row-Level Security (RLS) policies to safely process and instantly convert anonymous 5MB uploads into clickable UI hyperlinks.
  - **Designed a mobile-first, responsive interface** utilizing Tailwind CSS flexbox layouts and custom viewport breakpoints, ensuring a flawless UX across desktop and mobile devices.
  - **Established a continuous deployment pipeline (CD)** linking GitHub to Vercel, enabling automated edge-network builds and routing management for single-page application (SPA) paths.

- **Personal Portfolio Website** [March 2025]
  HTML, CSS, JavaScript | Project Website Link | Github Link
  - Designed and developed a **responsive personal portfolio website** to showcase projects, skills, and professional details, with **well-structured** sections like About, Skills, Projects, and Contact for clear navigation.
  - Applied responsive design principles to ensure **compatibility** across devices, while strengthening skills in **frontend development, UI design**, and overall website structuring through hands-on implementation.

- **GUI-Based Real-Time Weather Application using Python** [March 2025]
  Python, API, Tkinter | Project Link
  - Developed a GUI-based Weather Application using Python and Tkinter, integrating the **OpenWeatherMap API** to fetch real-time data using **HTTP requests** with proper **error handling** for invalid inputs.
  - Implemented a **CSV-based system** to store and manage search history, while gaining hands-on experience in **API integration**, file handling, and modular Python development.

TECHNICAL SKILLS

- **Programming Languages and Web:** Python, C++, C, JavaScript, HTML, CSS, Node.js, React
- **ML / Data and Tools:** PyTorch, NumPy, Pandas, Scikit-Learn, Matplotlib, Xilinx Vivado, Git, Github

ACHIEVEMENTS

- Ranked in the top 3.24% out of 250,000+ candidates in the AlgoUniversity Tech Fellowship (ATF) 2025.
- Won Gold Medal in mathematics conducted by Science Olympiad Foundation (SOF) at zonal level and school level.

POSITIONS OF RESPONSIBILITY

- **EII IIT Gandhinagar - Technical Coordinator & Events Lead** [July 2025 - April 2026]
  - Led development, deployment, and maintenance of the official EII website, supporting registrations, announcements, and participant engagement for **9+ entrepreneurship events**, workshops, and speaker sessions.
  - Spearheaded planning and execution of entrepreneurship-focused workshops, guest lectures, hackathons and flagship events, coordinating logistics, stakeholder communication, and on-ground operations.
  - Partnered with organizers, speakers, and technical teams to implement digital event workflows, schedules, streamlining registrations, content updates, and information dissemination for participants.
  - Led a team of **30+ people** and directed cross-functional coordination across technical and event teams, ensuring timely execution of deliverables and successful completion of multiple institute-wide initiatives.