

YASH PARIKH

📍 San Diego, CA • ✉ yashpparikh@gmail.com • in/yashpparikh
🆔 0009-0008-2081-4198 • 🎓 Google Scholar • 🔗 illuminati1618

EDUCATION

High School Diploma | **Del Norte High School**

GPA: 4.00 unweighted, 4.44 weighted

Expected June 2027

San Diego, CA

Highest coursework: AP Computer Science A, AP Calculus BC, AP Physics C: Electricity and Magnetism (in progress), AP Statistics (in progress).

Dual Enrollment | **MiraCosta College**

Fall 2026 – Present

MATH 260, Calculus and Analytic Geometry III (in progress); CS 111, Introduction to Computer Science I: Java; CS 113, Basic Data Structures and Algorithms.

Extended Studies | **University of California San Diego**

Summer 2024

Machine learning coursework (4.0 GPA)

San Diego, CA

Python and Mathematics for Machine Learning; Machine Learning Algorithms; Deep Neural Networks.

Foundations in Data Science (FinDS) | **UCSD**

Summer 2024

NSF-funded summer program

San Diego, CA

Probability, graph theory, calculus and linear algebra, taught by faculty from UCSD, UCLA, UPenn and UT Austin.

RESEARCH EXPERIENCE

Student Intern | **San Diego Supercomputer Center, UCSD**

Sep 2026 – Present

Supervisor: Dr. Martin Kandes • [hpcgpt-cli](https://github.com/hpcgpt-cli)

San Diego, CA

- Building AI agents that help researchers perform supercomputer operations (e.g., loading environment modules, writing job scripts).
- Analyzing agent metrics such as token usage, task success, and the impact of modifying system privileges.

Research Intern | **Boston University Security Lab (SeclabU), RISE**

Jun 2026 – Aug 2026

Advisors: Prof. Gianluca Stringhini, Prof. Manuel Egele • Supervisor: Khosro Moeini

Boston, MA

- Conceived and built **VibeAuthBench (VAB)**, a benchmark that measures the vulnerabilities and misconfigurations AI coding agents introduce when adding a feature (Sign-In with Google) to existing open-source applications with Python, Go and Node.js backends.
- Designed a two-stage pipeline: functional verification of the sign-in flow, then an LLM-as-judge security review against OWASP and Google OAuth guidelines, scored with CVSS 4.0 weights.
- Served open-weight models (up to 480B parameters) with vLLM on BU's Shared Computing Cluster across 30 runs. Agents produced a working sign-in in only 5 of 30 runs; 163 of 172 security findings were introduced by the new code, and security varied by language.
- Presented at the BU RISE Symposium (Aug 2026). Selected as one of 85 interns from 3,800+ applicants (2.2%).

Research Intern | **San Diego Supercomputer Center, UCSD (REHS)**

Jun 2026 – Jul 2026

Mentor: Dr. Martin Kandes

San Diego, CA

- Benchmarked rule-based (Presidio), custom spaCy NER and LLM-based detection of personally identifiable information across 1,400+ annotated supercomputer support tickets on a 7-person research team.

Independent Researcher | **V2X Intrusion Detection**

Nov 2025 – Apr 2026

Self-directed • [Publications, 1]

San Diego, CA

- Designed a two-stage framework: an LSTM that flags malicious V2X message sequences (96.26% accuracy, ROC-AUC 0.976) and a Transformer that classifies 19 attack types (88.23% accuracy, 88.05% F1, up from a 70.81% baseline) using physics-based, vehicle-independent features.
- Split all data by vehicle so no vehicle appears in both training and testing, and built a sequential processor that classifies messages as they arrive (93.93% recall), with a ~142 KB model sized for vehicle onboard units.
- 1st Award, Greater San Diego Science and Engineering Fair; qualifier, CA Science & Engineering Fair (2026).

Research Student | COSMOS, UC Santa Cruz
Mentors: Prof. Alvaro Cardenas, Prof. Leilani Gilpin

Jul 2025 – Aug 2025
Santa Cruz, CA

- Developed a systematic testing framework identifying vulnerabilities in LLM-based autonomous drone safety decisions under adversarial weather conditions.
- Built an automated simulation pipeline testing 200 scenarios against FAA Part 107 regulations, finding 75% decision inconsistency in moderate weather conditions.

PUBLICATIONS

- [1] M. Bapat* and Y. Parikh*, “A Deep-Learning based Cascading Framework for Intrusion Detection and Attack Classification on V2X-based Autonomous Vehicles,” in *Proc. 2026 International Conference on Computer Networks and Inventive Communication Technologies (ICCNCT)*, IEEE, 2026, pp. 273–278.

[doi:10.1109/ICCNCT68477.2026.11590071](https://doi.org/10.1109/ICCNCT68477.2026.11590071)

*Equal contribution.

HONORS AND AWARDS

CyberPatriot National Champion | Air & Space Forces Association 2022, 2023, 2025
Open Division (2025): voted team MVP as Domain Controller security lead. Middle School Division (2022, 2023).

SoCal Cyber Cup Champion | National University & NDIA 2022, 2023, 2026
High School Division (2026); Middle School Division (2022, 2023).

MITRE Embedded Capture the Flag (eCTF) | Project Lead 2024, 2025
2nd Place, High School Division, and Top 30 overall (2024); Top 50 overall (2025).

iGEM Gold Medal (2025) | Software VP and Wiki Developer 2025 – Present

National Merit Semifinalist | National Merit Scholarship Corporation 2026

LEADERSHIP AND EXPERIENCE

President and VP of Windows | CyberAegis 2021 – Present
cyberaegis.tech San Diego, CA

- Lead a student-run cybersecurity training program for 100+ middle and high school students across 3 schools.
- Architect training environments of 7–8 interconnected Windows and Linux systems for live red vs. blue team exercises, and teach blue-team incident response for Active Directory/LDAP, DNS, IIS/Apache and SQL services.
- President’s Volunteer Service Award (Gold); Eisenhower Award for Inspired Leadership (twice).

VP and Director of Outreach | CyberCEO Aug 2023 – Present

- Taught digital and cyber safety to 1,600+ elementary school students and 50 senior citizens across San Diego through classroom and assembly presentations.

Systems Engineering Intern | Poway Unified School District Jan 2025 – Aug 2025

- Configured cloud workspaces providing Ubuntu, Kali Linux and Debian VMs for 200+ students without personal computers, including DNS migration and SSL/TLS management.
- Primary technical liaison for a 5-person engineering team; trained 8 district teachers on production workflows.

SKILLS

ML and AI	LSTM and Transformer models, scikit-learn, spaCy, Presidio, AutoGluon; LLM agents, vLLM model serving, LLM-as-judge evaluation
Security	Enterprise service hardening (Active Directory/LDAP, DNS, Apache/IIS web, MySQL and SQL databases, mail servers), incident response, red teaming, embedded firmware security
Systems	Linux, Windows Server, Docker, AWS (EC2, S3, Route 53), HPC clusters, Git