Abhishek Saini

CONTACT INFORMATION

14 Orris Ave
Piscataway, NJ 08854

abhishek.saini@rutgers.edu
Personal Homepage

EDUCATION

Rutgers University, New Brunswick, NJ
Ph.D. Student in Computer Engineering — Sep 2024 – present
Relevant Coursework: Advanced Computer Architecture, Hardware and Systems Security, Distributed and Parallel Computing, Linear Algebra and Applications, Distributed Deep Learning

University of Washington, Seattle, WA
M.S. in Data Science, GPA: 3.94/4.00 — Sep 2021 – Mar 2023

Indian Institute of Technology, Madras, India
B.Tech. + M.Tech. in Electrical Engineering, Minor in Physics — Aug 2011 – Jul 2016

PUBLICATIONS

Abhishek Saini, Haolin Jiang, and Hang Liu. ”Vulnerabilities in Partial TEE-Shielded LLM Inference with Precomputed Noise.” Submitted to EuroSys, 2026.

RESEARCH EXPERIENCE

Dept of ECE, Rutgers University, New Brunswick, NJ
Graduate Research Assistant, HPDA Lab (Advisor: Prof. Hang Liu) — Sep 2024 – present

- **Vulnerability Discovery in TEE-Shielded Inference:** Uncovered a critical ”static secret basis” vulnerability in TEE-Shielded LLM/ML inference protocols. Devised novel algebraic attacks achieving a 100% success rate in compromising state-of-the-art systems.
- **Security for Tool-Using Agents:** Developing a planner-agnostic security framework to mitigate indirect prompt injection in LLM agents.

Dept of ECE, University of Washington, Seattle, WA
Research Assistant, EMIT Lab (Advisor: Prof. Sajjad Moazeni) — May 2023 – Mar 2024

- Developed a novel framework to train cascade classifiers using Genetic Algorithms and LightGBM for feature selection that reduced the training time by 50x.
- Extended open-source EDA tools to generate Cadence SKILL code, streamlining the transition from netlist to physical layout.

PROFESSIONAL ACTIVITIES

Artifact Evaluator, SOSP — Summer 2025

Program Committee, IEEE ICDM GTA^3 — Fall 2025

TEACHING AND MENTORSHIP

ECE 333: Computer Architecture Laboratory — Sep – Dec 2025
Rutgers University, Teaching Assistant

AMATH 550: Linear Algebra and Applications — Sep – Dec 2025
Rutgers University, Grader

ECE 252: Programming Methodology I — Jan – May 2025
Rutgers University, Teaching Assistant

Dept of ECE, University of Washington, Seattle, WA — Sep – Dec 2023
Research Assistant, EMIT Lab
Mentored high school student interns on customizing open-source Python EDA libraries

EL2100: Computer Aided Design Lab Aug – Dec 2015
Indian Institute of Technology, Madras, Teaching Assistant

EE1101: Signals and Systems Jan – May 2016
Indian Institute of Technology, Madras, Teaching Assistant

Industry Experience

Bosch Research, Sunnyvale, CA
Research Intern Jun 2022 – Sep 2022

- Engineered a real-time predictive maintenance framework for high-dimensional time-series data. Rectified data leakage in legacy baselines by formulating a rigorous, interpretable supervised learning pipeline with temporal validation, resulting in a filed patent.

OpsMx, Bengaluru, India
Software Engineer Dec 2020 – Sep 2021

- Conducted R&D on a risk analysis framework to automate software development lifecycle. Applied statistical models for metrics analysis and clustering algorithms for log error pattern recognition, while architecting a scalable distributed backend to process high-volume telemetry.

Palpx, Bengaluru, India
Software Engineer Mar 2020 – Dec 2020

- Developed computer vision solutions for diverse industrial and educational applications. Addressed data scarcity and deployment constraints by leveraging synthetic data generation and optimizing lightweight models for client-side inference.

Xiaomi, Bengaluru, India
Business Analyst Aug 2016 – Mar 2020

- Spearheaded analytics initiatives across E-commerce and Retail verticals, formulating statistical models for multi-warehouse inventory optimization, customer lifecycle management, and fraud mitigation. Selected technical implementations included utilizing time-series forecasting for demand planning (95% accuracy) and connected components analysis to detect anomalous reseller networks.

Skills

Languages: Python, C, C++, R, SQL
Frameworks & Libraries: CUDA, PyTorch, Intel SGX SDK, Scikit-learn, Pandas, Docker
Research Interests: LLM Security, Trusted Execution Environments (TEE), Agentic AI, Formal Verification, AI for Systems, AI for Science.

Honors and Awards

Secured **All India Rank 597** in IITJEE (top 0.12%)	2011
Winner of Sustainability Network Event at Techsoc, IIT Madras	2012
Awarded Merit-cum-Means (MCM) Scholarship	2011–2016
Gold Medal, Inter-Hostel Football Competition	2013
Quarterly Superhero Award, Xiaomi	2019
Awarded Rutgers ECE Graduate Certificate of Appreciation for Service	2025