ROHIT RAJARAM PAI

+1 858 214 9763 ◇ rohitpai.net ◇ ropai@ucsd.edu ◇ GitHub ◇ LinkedIn ◇ San Diego, California - 92037

EDUCATION

University of California San Diego, California, United States *September 2024 - June 2026*
Master of Science in Computer Science *CGPA: 3.962/4*
Sardar Patel Institute of Technology, Mumbai University, India *August 2018 - May 2022*
Bachelor of Technology in Computer Engineering *CGPA: 9.88/10*

RESEARCH EXPERIENCE

University of California San Diego *April 2025 - Present*
Graduate Student Researcher under Prof. Mihir Bellare *La Jolla, California*

- Performed the **end-to-end empirical evaluation** of a new generic committing AE transform, producing **rigorous and reproducible** performance comparisons against recent transforms.
- Built and refined the **benchmarking framework** in OpenSSL, C, and Python/Matplotlib to **reduce experimental noise** and generate clear, **data-driven evidence** of our transform's advantages.

TEACHING EXPERIENCE

University of California San Diego *July 2025*
Teaching Assistant under Adam Suhl (advised by Prof. Nadia Heninger) *La Jolla, California*

- Organized **10 discussion sections** and twice-weekly office hours for **CSE 107 Introduction to Modern Cryptography**, clarifying foundational concepts and solving additional problems.
- Acted as **primary grader for all assignments and exams**, ensuring timely and accurate evaluation of student work, and assisted the instructor with **course logistics**.

University of California San Diego *January 2025 - June 2025*
Teaching Assistant under Prof. George Porter *La Jolla, California*

- Collaborated with the professor to redesign the **CSE 124/224 Networked Services** course curriculum.
- Designed, implemented, tested and documented **10 new Golang-based programming assignments** covering Networking basics, Socket Programming, Remote Procedure Calls and Distributed Systems.

PROFESSIONAL EXPERIENCE

Deutsche India Pvt. Ltd., Deutsche Bank Group *July 2022 - August 2024*
Senior Analyst, Cryptography Engineering and Solutions Team *Pune, India*

- Increased security of **internal wide area networks** by designing multiple POCs and creating a **custom OpenSSHv9** package for RedHat Enterprise Linux 7 which processed over **5 million error-free network operations**.
- Developed a **post-quantum cryptography (PQC) CLI tool** using C, OpenSSL3, liboqs, and oqs-provider to assist **4,000+** internal applications in migrating to quantum-safe OpenSSL, enabling secure encryption without requiring direct library updates.
- Led the **vulnerability management** effort for a Java-based legacy application, patching over **200** critical and high-severity vulnerabilities to enhance security and stability.

PUBLICATIONS

1. **Pai, R.**, Purohit, M., & Vinayakray-Jani, P. (2023). **Strengthening Deep-Learning-Based Malware Detection Models Against Adversarial Attacks**. In ICDSAI 2022, Advances in Data Science and Artificial Intelligence, Springer Proceedings in Mathematics & Statistics, vol 403. 203 - 219. DOI
2. **Pai, R.**, Naik, A., Sandesara, H., & Dholay, S. (2022). **Vigila: Application for General Safety**. In ICAC3 2021, Intl. Conference on Advances in Computing, Communication, and Control, IEEE. DOI

PROJECTS

UCSOS: Rapid Response System for Students at Risk *April 2025 - June 2025*

- Led requirements gathering by **interviewing 3 individuals** supporting **at-risk community** members to identify essential features and security needs.
- Proposed a **secure SOS application** with one-click **emergency calling**, **rapid information dispersal** to response teams and emergency contacts, **panic-wipe** functionality, and a **camouflaged** interface.

EncryptedIoT: Analysing and Improving Ring's E2EE *September 2024 - December 2024*

- Performed a **detailed analysis of Amazon Ring's encryption** protocols, highlighting **trust issues** in the default mode and **the significant feature loss** introduced by **end-to-end encryption**.
- Proposed an **improved E2EE system** for Ring, enabling users to grant **timed access** to their IoT data and **restore previously unavailable features**, with security informally verified using Tamarin.

GAN-based Malware Detection Model *May 2021 - December 2021*

- Developed a robust malware detection system utilizing **Autoencoders and GANs**, capable of identifying **11 distinct classes** of malware by leveraging the dataset of over **100,000 samples**.
- Outperformed conventional neural network models by achieving a precision of **84.1%**, recall of **85.31%**, F1 Score of **84.7%** and a false positive rate of **4.49%**.

Vigila - A General Safety Application *August 2020 - April 2021*

- Designed a **community-based** safety application which sends **SOS messages** to all users in a **100m radius** along with the emergency contacts, using Geofencing Technique, Flutter and Cloud Firestore.

RELEVANT COURSEWORK

• Modern Cryptography • Applied Cryptography • Legacy of Cypherpunks • Private Information Retrieval • Lattice Algorithms • Computer Security • Computer Communication Networks • ML: Learning Algorithms • Cryptography and System Security • Cyber Security and Digital Forensics • Theoretical Computer Science • Advanced Data Structures • Design and Analysis of Algorithms • Operating Systems • Database Management Systems • Distributed Systems • Artificial Intelligence • Engineering and Applied Mathematics

TECHNICAL SKILLS

- **Languages** - Python, Golang, Java, C, Linux/Bash, SQL (MySQL), NoSQL (MongoDB), HTML, CSS
- **Libraries/Frameworks** - Flutter, Angular, Bootstrap, OpenSSL, TensorFlow, Keras, Pandas, Matplotlib, Numpy
- **Tools** - Google Cloud Platform, Git, OpenSSH, Docker, Firebase, Android Studio, Jupyter Notebook, VS Code

SOCIAL WORK

- Volunteered **60+ hours** under the **PlusYou** initiative of Deutsche Bank by assembling and distributing school kits for primary school students, creating awareness for children with developmental disabilities, and creating reusable paper bags. *(July 2022 - August 2024)*
- Mentored **10+ hours** under the **Abhyudaya Program** by coaching underprivileged 10th-grade students and solving their doubts. *(July 2019 - February 2020)*

ACHIEVEMENTS

- **Winner** of the **Code for Good** hackathon by JP Morgan and Chase. Designed a prototype for simplifying the **application process of government schemes** for the **labour class**. *(August 2020)*
- **18th out of 183** participants at the SANS South Asia Capture the Flag Competition. *(April 2021)*
- **94th out of 1320** teams at the Deloitte Hacky Holidays Competition. *(July 2021)*