

# Ayush RoyChowdhury

Austin, United States | ayushrc0914@gmail.com | (469) 994 8424 | ayush-roychowdhury.github.io

## Objective

---

I'm passionate about AI security and engineering, with a **B.S. in Electrical and Computer Engineering** and currently pursuing my **M.S. in the same field**. I bring **hands-on experience across AI, cloud, security, and software engineering**, and I've been **fortunate to present my research at top venues like DefCon 32, ASPLOS '24, Microsoft SLG Security and Compliance, and the ACE Center**. My work has also been **featured on Security Magazine, Data Breach Today, Secure World, CYBR Monk and Dark Reading**.

I'm excited to bring my skills to a **full-time role in Security, AI, or Software Engineering**. **Flexible and eligible to work all locations in US**.

## Education

---

### M.S. Electrical and Computer Engineering, UT Austin

August 2024 — May 2026

- Cumulative GPA: 3.83/4.0
- Track: Architecture, Computer Systems, and Embedded Systems
- Thesis: Improving the Reliability and Security of Compound AI systems for Enterprise Use
- TA for Enterprise Network Security, Software Engineering II and Multithreading Prog/Arch/Tools

### B.S. Electrical and Computer Engineering, UT Austin

- Cumulative GPA: 3.61/4.0, Business Minor
- Track: Software Engineering and Systems
- TA for Introduction to Embedded Systems

## Research Achievements

---

### Confused Deputy Risks in RAG-based LLMs

January 2024 — August 2025

- Confused Deputy Risks in Production Level Rag-Based Systems such as Copilot for M365: [spark.ece.utexas.edu/confusedpilot](https://spark.ece.utexas.edu/confusedpilot)
- **Presented ConfusedPilot at DefCon 32 AI Village.**
- **Presented Emerging AI Threats to Microsoft SLG Security and Compliance Webinar.**
- **Featured on Security Magazine, Data Breach Today, Secure World, CYBR Monk, and Dark Reading.**

### Learning-based Detection of Microarchitectural Attacks

January 2024 — April 2024

- SoK (Systemization of Knowledge) on learning-based detection of microarchitectural attacks: [ut-ldma.github.io](https://ut-ldma.github.io)
- Reinforcement learning-based detection of microarchitectural attacks, **presented at ASPLOS '24 workshop & ACE Symposium.**

## Experience

---

### Security R&D Intern, Zenity, Austin

September 2025 — December 2025

- Creating a red teaming **framework** for **assessing LLM robustness to indirect prompt injections and jailbreaks**.
- **Penetration Testing of Agentic AI Systems** across platforms such as **Copilot for Microsoft 365, ChatGPT, Cursor, and Salesforce**.

### Security Development Engineer Intern, Nvidia, Santa Clara

May 2025 — August 2025

- **Red-teaming AI agents** to identify **issues with privacy and knowledge integrity**.
- **Built and analyzed different jailbreak classifiers** (LR, XGBoost, Neural Network, CNNs etc.) based on **collected activation that can hook into open-source models at inference time for improved model security**.

### Security R&D Intern, Zenity, Austin

September 2024 — April 2025

- Helping **red-team Copilot for M365 and Copilot Studio Agents**, with a focus on **data exfiltration and privacy**.
- Contributed to the development of **open-source Pentesting Tool PowerPwn** for **assessing security of Copilot Chatbots in the Wild and Copilot for M365**: <https://github.com/mbrg/power-pwn>
- Contributed by **identifying vulnerabilities and implementing solutions for enhanced security measures to an open-source Gen AI Matrix**: [https://tpts.ai/entity/ayush\\_roychowdhury.html](https://tpts.ai/entity/ayush_roychowdhury.html)

## Software Engineering Intern, Cox Automotive, Austin

May 2024 — August 2024

- Set up infrastructure for RAG-based systems with sparse retrieval in AWS. Researched performance improvements in routing vs. non-routing for OpenSearch clusters. Automated data refresh using Lambda.
- Developed a secure backend-for-frontend to track dealership activity using C# and AWS.
- Built a secure Copilot tool to assess Rally epics, features, and stories for sprint planning, focusing on clarity and completeness. Used Purview and Azure Active Directory for governance and identity access management.

## Cloud IoT R&D Intern, Trend Micro, Austin

June 2023 — August 2023

- Developed an application to automate the software delivery and bug fix pipeline for Security Management System using AWS IoT and middleware.
- Used OpenAI API to create a bug resolution system that leveraged gpt-3.5-turbo to suggest bug fixes based on code, testing and Jira context.

## Cloud Automation R&D Intern, Trend Micro, Austin

June 2022 — August 2022

- Proposed and implemented a cloud feature that would automate client's network appliance management in Trend Micro's Cloud One service.
- Implemented an app to invoke a Lambda with KMS integration for network security filters offered to network appliances by Trend Micro's Cloud One service.

## Technical Skills

---

**AI/ML:** Security for Large Language Models and Compound AI Pipelines, Tensorflow, PyTorch, Scikit-learn, Pandas, Numpy, CUDA

**Security Tools:** VMWare, VirtualBox, Linux, Kali Linux, Ghidra, Wireshark, nmap, tcpdump, Scapy, Netcat, Metasploit, Web Application Security Testing, Microsoft Purview, Azure Active Directory

**Languages:** Python, C/C++, Java, Ruby, SQL, Bash, React, ARM Assembly, PHP, C#, Go, R, Javascript, HTML, CSS

**Cloud Infrastructure:** AWS, Azure, Docker, Kubernetes, microk8s

## Featured Projects

---

### Web Application Security

- Performed network reconnaissance using nmap and Wireshark, analyzed packet handshakes.
- Syn Flood Attack using scapy on implemented Server-Client in C.
- Deployed a website using Docker and Kubernetes, ran administration using microk8s.
- Applied Command Injection, PHP Injection, SQL Injection, CSP Bypass Attack, and Forkbomb Attack.

### RSA & AES-128 Implementation and DPA

- Implement RSA and AES-128 (Counter-Mode) in C/C++ using basic arithmetic functions.
- Implemented a Differential Power Analysis attack in Python by analyzing power traces from hardware and using Pearson Correlation to guess the encryption key.

### Lingobin

- Developed an application to help translate code-switches in communication by leveraging OpenAI Whisper.
- Automated testing of the application on collected datasets from Kaggle and Hugging Face.

### GSTAgri

- Capstone project focusing on Edge AI and IoT and leverages the ST150M, a Globalstar satellite modem, to create an asset monitoring and management system that predicts crop risk.
- Reducing overall data usage and cost by implementing Edge AI to alert clients based on metrics set by subject matter experts.

### Meals on Wheels Delivery App

- A delivery application similar to DoorDash made using React, JS, HTML, CSS, Python, SQL and Salesforce for Meals on Wheels volunteers who deliver meals to the elderly.
- Lead a team of engineers and corresponding research group to deliver this project successfully to Meals on Wheels.