Shanto Roy

346-308-4424 — shantoroy@ieee.org — linkedin.com/in/shanto-roy — github.com/shantoroy — credly.com/users/shantoroy

Summary

AI Security Engineer — PhD in Cybersecurity **Status: Green Card**

AI Platform Security Engineer with a PhD in cybersecurity and a strong background in academic security research and enterprise SRE operations. Focused on securing enterprise AI platforms through guardrail and policy design, OWASP AI risk assessment, AI traffic and agent monitoring, etc. Brings a rare blend of research-driven security analysis, hands-on infrastructure operations, and vendor product evaluation to drive secure, observable, and governed AI systems at scale.

Skills

AI Security	LLM Security, AI Guardrails, Agentic Security, MCP Security, AI Governance
Sec Ops	SIEM, SOAR, EDR, Security Monitoring, Threat Detection
Platforms	CrowdStrike, Zscaler, Google Chronicle, ExtraHop, Grafana, Splunk
Cloud	GCP, AWS, Kubernetes, Docker, Terraform
Programming	Python, Bash, SQL

Certifications

- AWS AI Practitioner (2025)
- RHCSA in Open Stack (2017)
- RHCSA (2016)
- Red Hat Certified Engineer (2016)
- GCP Associate Cloud Eng. (2024)
- Professional Scrum Master I (2025)

Experience

Charles Schwab (TX, USA) **FTE: Jan 2026 – Present**
AI Platform Security Engineer

Shadow AI & MCP Security Control

- Managed Shadow AI and Agentic (harness, agents, MCPs, skills, etc.) visibility and guardrails across SaaS applications, endpoints, and enterprise infrastructures
- Evaluated 10+ industry-leading vendor products for AI security, provided recommendation

AI Guardrail Architecture

- Designed policies for LLM/MCP/Agent guardrails covering input validation and output evaluation/filtering
- Enforced controlled Agent/MCP access and context boundaries aligned with enterprise security policies

AI Traffic Monitoring, Detection & Response

- Monitored AI API traffic using centralized logging pipelines and SIEM/Zero-trust platforms
- Collaborated with the Data Leak Prevention (DLP) and Insider Risk teams to ensure better enterprise security posture

AI Governance & Platform Security

- Supported AI governance initiatives covering access control, auditability, and data boundaries
- Assisted with secure onboarding and lifecycle management of enterprise AI applications/tools
- Ensured alignment with security, privacy, and compliance requirements for AI platforms

Charles Schwab (TX, USA) **FTE: Jun 2024 – Jan 2025**
Site Reliability Engineer *Intern: Jun 2023 – Aug 2023*

Infrastructure Resiliency & Security

- Managed Red Hat and Windows servers across dev, non-prod, and production environments of 50+ applications
- Conducted regular vulnerability assessments and applied patches to secure systems
- Conducted disaster recovery, load testing, and capacity planning, etc., and provided on-call support
- Mentored interns and juniors and helped them with their projects/onboardings

Visibility, Documentation, and Automation

- Created and maintained comprehensive documentation for operational procedures, runbooks, and troubleshooting
- Configured monitoring and logging tools to track system performance and troubleshoot issues proactively
- Automated routine tasks using Python, Shell, PowerShell, and Salt scripts to reduce manual effort

University of Houston (TX, USA) **Aug 2019 – May 2024**
Research/Teaching Assistant

- Researched cyber deception/reconnaissance to enhance threat detection/defense and published 6* relevant manuscripts
- Collaborated in 5+ research projects involving MITRE ATT&CK, cloud data security, and IoT security
- Utilized REST APIs and Postgress for 10+ large-scale IoT ecosystem projects and Grafana for monitoring

Education

University of Houston (TX, USA) **Aug 2019 - May 2024**

- **MS** and **Ph.D.** in Computer Science (Concentration: Cyber Security)
- **Labs**:
  - Resilient Network and Systems Lab (Dr. Aron Laszka)
  - Networked Systems Laboratory (Dr. Omprakash Gnawali)
- **Scholar Publications**: https://scholar.google.com/citations?user=OMGYMbwAAAAJ

Awards at Charles Schwab

- Participated Cyber Range (Cybersecurity Hackathon) in 2025 & 2024, and ranked within top 10 out of 70+ teams
- Received quarterly org-wise recognition two times and team monthly shoutouts 7 times

SRE Projects

Infrastructure Security **Jun 2024 – Present**

- Implemented data center and cloud migration strategies to move 5+ applications from one data center to another
- Developed an infra inventory for the team that tracked service accounts, NAS locations, app/env-wise server list, etc.
- Provided a calendar (yearly/monthly/daily) view of infra-team activities, e.g., patching, release, deployment, etc.
- Provided compliance insights of the platforms of 50+ applications based on non-/overdue risk-level vulnerabilities

AI Chatbot for Operations **Nov 2024 – Present**

- Developed an RAG AI chatbot PoC for SREs to access critical information faster from documentation and log data
- Offers SREs to focus more on process than data source and reduces mean time to resolution (MTTR) during an incident

Specialized Security/AI Projects

Privacy and Security **2019-2025**

- **MITRE ATT&CK:** Explored use-cases of the ATT&CK framework in threat intelligence, intrusion detection, offensive security, and cyber risk assessments.
  Manuscript Link: https://arxiv.org/pdf/2304.07411.pdf
- **Cyber Reconnaissance:** Developed a taxonomy of cyber reconnaissance where we categorized different techniques attackers use to obtain valuable information for future attack planning.
  Manuscript Link: https://arxiv.org/pdf/2105.04749.pdf.
- **Cyber Deception:** Developing a deception framework that combines semi-indistinguishable honeypots and attacker redirection to mitigate adversarial reconnaissance and to investigate attacker behavior.
  Book Link: https://uh-ir.tdl.org/items/8b74b15c-4489-4c41-b3c2-fa5bea6fdd13
- **IoT Remote Attestation and Security Game:** Applied game theory to practical experimentation performed in a controlled IoT environment for ARM-based vulnerability, exploitation, and attestation analysis.
  Manuscript Link: https://arxiv.org/pdf/2109.07724.pdf.
- **Privacy:** Developed a privacy-aware Mobile and Fog computing-based E-governance framework to trace and mitigate COVID-19 community transmission.
  Manuscript Link: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9204791.

AI Concept Projects **2024-Present**

- **RAG-based Chatbot:** A RAG (Retrieval Augmented Generation) based question-answering prrof-of-concept (PoC) system that allows a user to query target documents using natural language. The system uses local LLMs through Ollama for privacy and performance and provides a chat interface for easy interaction.
  Repo Link: https://github.com/shantoroy/rag-chatbot-python-fullstack-template
- **Model Context Protocol (MCP):** Hands-on use of local MCP servers for tool integration, context retrieval, and secure interaction patterns

Data Science/AI/ML in Security **2020-2024**

- **Strategic Cyber Camouflage:** Explored the usage of autonomous intelligent cyber defense agents by using game theory to optimize decoys and signal modification; by modifying features of real and fake objects, and applying machine learning to scale feature modifications for effective deception.
  Manuscript Link: https://aronlaszka.com/papers/kiekintveld2023strategic.pdf
- **Cyber Recon Modeling:** Developed a probability-theory-based model for adversary belief formation to more realistically capture key aspects of cyber reconnaissance that can serve as a basis for developing practical deception games.
  Manuscript Link: https://arxiv.org/pdf/2306.06769
- **OS Fingerprinting:** Tested the accuracy of different ML-based classifiers applied over network traffic features.
  Repo Link: https://github.com/shantoroy/OS_fingerprinting_using-ML
- **Smart Contract Security Trend:** Scraped community posts from *Medium* and analyzed/modeled trends of cyber attacks and usage of security tools behind smart contract development.
  Manuscript Link: https://arxiv.org/pdf/1905.08833.pdf