

# Shaheer Saud

[shaheersaud.internship@gmail.com](mailto:shaheersaud.internship@gmail.com) | [linkedin.com/in/shaheer-saud](https://www.linkedin.com/in/shaheer-saud) | [github.com/shaheersaud2004](https://github.com/shaheersaud2004) | [cipherconsulting.net](https://cipherconsulting.net)

## EDUCATION

Rutgers, the State University of New Jersey - New Brunswick  
*B.S. in Computer Science, Minor in Data Science and Criminology*

**May 2026**  
**3.69 GPA**

## WORK EXPERIENCE

### AT&T — Cyber Security Data Analytics Team

*Cyber AI Engineering Intern*

**Middletown, NJ**  
*May 2025 – Present*

- Rebuilt the AT&T RAG LLM document pipeline with new data sources and automation, cutting retrieval time from weeks to seconds and improving IAM/PAM query accuracy by 23%
- Programmed a benchmarking tool to evaluate LLM configurations, reducing testing time by 78%, increasing model iteration speed, and enabling faster deployment of optimized models across use cases
- Tuned LLM performance by reengineering core prompts, chunking logic, and embedding strategies — increasing output reliability and optimizing token usage across AT&T's internal AI models

### Colgate - Palmolive

*Security Engineer Intern*

**Piscataway, NJ**  
*Feb 2024 - Present*

- Developed an AI-powered chatbot for advanced PAM queries, reducing a week-long support process to minutes and cutting help desk resolution time by 98% with instant, accurate answers
- Executed end-to-end log analysis with Splunk (SIEM), Okta (identity), and Tanium (endpoint) to uncover unauthorized access, anomalies, and misconfigurations — enhancing detection and response speed
- Automated migration of over 1,000 IT profiles using PowerShell, Python, and Colgate-Palmolive's API, cutting manual effort by 80% and securely transferring credentials and secrets at scale

### Rutgers Office of Information Technology

*Information Technology Supervisor*

**New Brunswick, NJ**  
*Apr 2023 - Present*

- Deployed a secure Python automation script with Selenium to streamline data aggregation across multiple platforms, reducing caller wait times by 86% and enhancing data integrity
- Leveraged expertise in OSI Layer 1 to 7 configurations, including secure IP address management, TCP/IP protocols, and DNS security, to resolve network challenges and ensure uninterrupted, secure data flow
- Led and trained 200 consultants, resolving over 300 IT tickets via ServiceNow, focusing on mitigating security breaches and preventing network interruptions, significantly improving incident response times

## PROJECTS

### Smart Home Honeypot Dashboard | *Python, Flask, SQLite, WebSockets, GeoIP, Telnet, Jinja2*

- Built a full-stack IoT honeypot simulating a smart home, using fake login portals, Telnet exploits, and firmware traps to capture attacker behavior — visualized threats in real time via a custom dashboard

### Sensitive Data Exposure Crawler | *Python, FastAPI, Asyncio, NLP, Chart.js, Uvicorn, WebSockets*

- Created a real-time web crawler that scans public URLs for exposed personal data using NLP filters and visualizes scan results through a live dashboard with 100+ concurrent scanning workers

### Brute-Force Attack Simulation System | *Python, Flask, Asyncio, Web Security*

- Coded an asynchronous brute-force testing framework with concurrency limits, randomized delays, and CAPTCHA/MFA resistance to evaluate and document modern authentication defenses

## SKILLS & ACTIVITIES

**Languages:** Python, Java, JavaScript, HTML/CSS, C/C++, PowerShell, SQL

**Certifications:** Cisco Intro to Cybersecurity, TryHackMe Jr. Pen Tester, Pursing CCNA

**Involvement:** Cipher Consulting, MSA Treasurer, HackRU (2023/2024/2025), HackTheBox