

Kanishka Sahoo

Software Engineer | Security Engineer

Email: hello@ksahoo.com **Location:** Bengaluru, Karnataka, India

Portfolio: ksahoo.com **LinkedIn:** linkedin.com/in/kanishka-sahoo **GitHub:** github.com/kanishka-sahoo

2026 Computer Science graduate with security and software engineering internship experience building Python/FastAPI services and security tooling, supporting production incident response, and maintaining automated tests and CI/CD workflows. CompTIA Security+ certified.

Work Experience

Software Engineer Intern

Aug 2026 – Present

Seceon Inc. | Bengaluru, Karnataka, India

- Develop software for Seceon's cybersecurity products across backend systems and Linux infrastructure supporting security operations.

Intern, Security Engineering

Jan 2026 – Jul 2026

GoTo Technologies India Pvt. Ltd. | Bengaluru, Karnataka, India

- Reduced incident triage time by up to 75% with RAG search over thousands of past Jira incidents and tickets, using pgvector and Azure.
- Reduced vendor-risk assessment time by 90% with a new AI-assisted scanner (React, FastAPI) that has assessed dozens of vendors.
- Built a configuration-management REST API using FastAPI and PostgreSQL for an internal incident platform used by approximately 1,000 engineers.
- Supported production incident response by analyzing logs, diagnosing application and container failures, and rolling back Kubernetes deployments.
- Wrote and maintained automated tests, and maintained GitHub Actions CI/CD workflows across build, test, and deployment stages.

SOC Intern

Jun 2025 – Jul 2025

PESU-ISFCR | Bengaluru, Karnataka, India

- Built a real-time email threat-detection filter that flags phishing, spoofed-sender, and malicious messages before inbox delivery.
- Investigated phishing and account-takeover activity in red-team and blue-team exercises, and triaged and escalated incidents during SOC monitoring.

Research Trainee

Jun 2024 – Jul 2024

PESU-ISFCR | Bengaluru, Karnataka, India

- Developed a repeatable workflow to collect, compare, and report Google Drive Desktop forensic artifacts across the application lifecycle.

Technical Skills

Languages: Python, C, C++, Bash, SQL, Go

Backend & Cloud: FastAPI, Flask, REST APIs, PostgreSQL, AWS, Docker, Kubernetes, Linux, WebSockets, React

Tools: Burp Suite, Nmap, Kali Linux, GitHub Actions, Git, pgvector, pytest

Engineering: CI/CD, Backend Development, API Design, Data Structures & Algorithms, Object-Oriented Programming, Infrastructure as Code, Applied Machine Learning

Security: Application Security, API Security, Security Engineering, Vulnerability Assessment, Incident Response, Threat Detection, Penetration Testing, Authentication & Authorization, IAM, OWASP Top 10, Secure SDLC, Cloud Security, Container Security, Digital Forensics

Projects

Multi-Agent Penetration Testing Workspace

github.com/kanishka-sahoo/pentest

- Built a FastAPI and React workspace that coordinates reconnaissance, exploitation, and post-exploitation agents and persists events in PostgreSQL.
- Ran security tools in isolated Kali Linux containers and streamed output over WebSockets with replay of persisted events.
- Enforced target allowlisting and exploit-proof requirements, added pgvector retrieval, and tested agents, tools, and authorization with pytest.

Linkify — Secure Link Shortener and Analytics Platform

github.com/kanishka-sahoo/linkify

- Built a full-stack link platform (TanStack Start, React, Neon Postgres, Drizzle ORM) whose redirects enforce expiry, click-cap, and password rules.
- Secured a REST API with scoped, expiring bearer keys and role-based access, and Postgres-backed rate limits and brute-force lockouts.
- Added TOTP and passkey authentication, CSP and HSTS headers, CSV formula-injection protection, bot detection, and privacy-mode analytics.

IoT Honeypot and ML Anomaly Detection

github.com/kanishka-sahoo/iot-honeypot

- Deployed an SSH honeypot and used CICFlowMeter to generate labeled network-flow data for attack-pattern analysis.
- Trained a CatBoost classifier with 96% benign-versus-malicious classification accuracy and automated IP blacklisting for positive detections.

s3-ducky — ESP32-S3 HID Security Research Tool

github.com/kanishka-sahoo/s3-ducky

- Built ESP32-S3 firmware for a BadUSB HID research device that emulates keyboard and mouse input, with a separate boot mode for uploading payloads and manual execution controls that prevent accidental runs during testing.

Education

B.Tech. Computer Science and Engineering — PES University | Specialization: Cyber Security and Connected Systems | GPA: 8.7/10 | 2022 – 2026

Certifications

CompTIA Security+ | CompTIA | Aug 2026

Achievements

Top 10, Terrathon 24-hour hackathon, IoT anomaly-detection challenge (Mar 2025) • Top-10 team finishes, ISFCR CTF events, PESU (2022–2024)