Pandu Ranga Reddy Konala

pandurangareddy414@gmail.com | pandukonala.github.io

Personal Statement

I'm a cybersecurity researcher working at the crossroads of AI code generation and modern DevSecOps. My PhD research focuses on identifying code quality issues in Infrastructure as Code, resulting in a framework that detects vulnerabilities ranging from misconfigurations to cyber attacks by tracing how security smells diffuse through metadata patterns. More recently, I've been building agentic pipelines that generate, validate, and self-repair security-hardened infrastructure against regulatory frameworks, reducing manual compliance effort from weeks to minutes and costs by over 99%. I've also designed distillation and fine-tuning pipelines to bring these capabilities to smaller, cost-efficient open-source AI models. I am looking for roles where I can apply and extend my knowledge at the intersection of AI, security, and software infrastructure.

Academic Progress

The University of Waikato — *Hamilton, New Zealand*

PhD in Computer Science — *April 2022 - February 2026*

- Fully funded by MBIE, New Zealand, through the AI for Human-Centric Security Catalyst project scholarship
- Thesis: *A Code Quality Framework for Infrastructure as Code in the Modern DevSecOps Era*
- Published 3 first-author papers at peer-reviewed venues (IEEE CSR, DBSec, IWSEC) with 2 under review

Lancaster University — *Lancaster, United Kingdom*

Masters in Cyber Security — *September 2019 - September 2020*

- Fully funded by Lancaster University through the Cyber Security Scholarship program
- NCSC-certified programme by the National Cyber Security Centre, UK

Amrita Vishwa Vidyapeetham — *Coimbatore, India*

Bachelor of Technology in Computer Science and Engineering — *June 2015 - April 2019*

- Specialized in Cyber Security
- Published 2 first-author research papers on cloud security and decentralized file systems

Work Experience

Research Associate — *Hamilton, New Zealand*

School of Computing & Mathematical Sciences, The University of Waikato — *April 2022 - February 2026*

- Engineered an end-to-end automated pipeline integrating multi-turn LLM repair loops, containerised Docker/EC2 testing infrastructure, and a reporting interface for continuous IaC quality-compliance validation.
- Designed a teacher-student distillation pipeline for supervised fine-tuning of smaller open-source models, incorporating a custom reward function for quality and compliance-aware IaC generation.
- Built metadata extraction and clone detection tooling to analyse 27,000 Ansible Galaxy repositories at scale, supporting my empirical research across multiple publications.

Software Developer — *Lancaster, United Kingdom*

Quantum Base — *June 2020 - September 2020*

- Designed and implemented secure system architectures to integrate quantum PUFs with IoT devices, bridging the gap between quantum technology and everyday applications.

Security Analyst Intern — *Lucknow, India*

Infosec Future Pvt Ltd — *May 2018 - June 2018*

- Conducted website penetration testing, vulnerability scanning, and risk analysis using automated tools and manual techniques during an eight-week internship.
- Performed detailed information gathering to identify security risks and vulnerabilities.

Red Hat System Administrator Intern — *Hyderabad, India*

Complete Open Source Solutions (COSS) — *May 2017 - June 2017*

- Gained hands-on experience in managing and maintaining Red Hat Enterprise Linux systems during a four-week internship.
- Handled system installation, configuration, performance monitoring, security management and maintained system documentation.

Ethical Hacker Intern — *Vizag, India*

Star Computers — *May 2016 - May 2016*

- Gained hands-on experience in penetration testing and vulnerability assessments over a four-week period.
- Identified potential vulnerabilities and security risks in client systems and applications through various tests and assessments.

Professional Certifications

Red Hat Certified Engineer (RHCE) by Red Hat, License No. 170-138-911

Red Hat Certified System Administrator (RHCSA) by Red Hat, License No. 170-138-911

Certified Ethical Hacker (CEH) by EC-Council, License No. ECC022209621222

Skills

Cyber Security Tools Metasploit Framework, Nessus, Burp Suite, Wireshark, CIS-CAT

Programming Python, Bash/Shell, Java, SQL, Node.js, R

Platforms & Infrastructure AWS (EC2), Red Hat Linux, Kali, Docker, Podman, Ansible, Terraform

Miscellaneous LaTeX, SAST, DAST, LLM/GenAI Integration, TensorFlow, PyTorch, Hack The Box

Peer-Reviewed Research Publications

Tracking Security Smell Diffusion Patterns in Ansible Playbooks Using Metadata *Published*

Research Paper (First-Author) *November 2025*

- International Workshop on Security (IWSEC) 2025, Japan
- Analysed security smell propagation across Ansible Galaxy repositories, revealing 38–54% code overlap that facilitated diffusion of 3 CWEs and 3 CVEs affecting millions of downstream users, including CVE-2017-7550 (CVSS 9.8), with cloned repositories downloaded at 100× higher rates than their fork-visible counterparts.

Metadata Assisted Supply-Chain Attack Detection for Ansible *Published*

Research Paper (First-Author) *June 2025*

- Conference on Data and Applications Security and Privacy (DBSec), Norway
- Proposed a quality-based approach using metadata for detecting supply-chain attacks in Ansible Galaxy repositories, identifying 2 CVEs and 3 CWEs affecting millions of downstream users.

SoK: Static Configuration Analysis in Infrastructure as Code Scripts *Published*

Research Paper (First-Author) *August 2023*

- IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy
- Systematised 24 analysis tools (SAST & DAST) for IaC scripts, categorising detection capabilities and identifying research gaps.

Access mechanism using inter planetary file system *Published*

Research Paper (First-Author) *April 2019*

- International Journal of Engineering and Technology, Volume 7, No 4, ISSN: 2227-524X
- Designed a decentralized access control mechanism leveraging IPFS for secure and distributed control of IoT devices.

Securing Data in Cloud – A Physical Cyber System *Published*

Research Paper (First-Author) *December 2017*

- Journal of Computer Science Engineering, Volume-3, Issue-12, ISSN-2456-1843
- Proposed a priority-based encryption method for secure data sharing in cloud storage, incorporating user priority levels to defend against known-ciphertext and known-plaintext attacks.

A Policy-Driven Framework for Measuring the Code Quality of Ansible Roles: An Empirical Study *Under Review*

Research Paper (First-Author) *2026*

- Journal of Systems and Software (JSS)
- Designed a policy-driven quality framework for Infrastructure as Code that analyses IaC code across 9 quality categories unique to IaC, identifying security vulnerabilities, maintenance risks, and monitoring gaps, with large-scale empirical validation on 27,000 open-source repositories.

Evaluating and Preventing Security Smells in AI-Generated Ansible Code *Under Review*

Research Paper (First-Author) *2026*

- Evaluated 16 state-of-the-art AI foundation models for generating secure and compliant Ansible code, finding none natively capable of meeting CIS benchmarks, and proposed a prompt engineering framework that enables full compliance with standards such as HIPAA, SOC 2, and PCI-DSS.

Projects

AI for Human Centric Security *PhD Project*

The University of Waikato *April 2022 - February 2026*

- Part of a trans-Tasman cyber security research collaboration between New Zealand universities and CSIRO Data61, Australia, funded by MBIE.
- Proposed a policy-driven quality framework that analyses IaC code across 9 categories unique to Infrastructure as Code, identifying misconfigurations, security vulnerabilities, and maintenance risks.

Cryptographically Secure On-Line Identity System *Masters Project*

Lancaster University *June 2020 - September 2020*

- Developed a framework leveraging quantum computer-generated identities (PUFs) for device authentication and validation, targeting resource-constrained IoT and mobile devices. Funded by Quantum Base and The Royal Society, UK.

Secure communication using IPFS with IoT *Under Graduate Project*

Amrita Vishwa Vidyapeetham *June 2018 - April 2019*

- Used the Interplanetary File System (IPFS) protocol for secure, direct communication between users and IoT devices, eliminating the need for third-party vendors. Funded by Amrita Vishwa Vidyapeetham, India.

Voluntary Activities

New Zealand Cyber Security Challenge *cybersecuritychallenge.org.nz*

2022 - 2025

- Organized and facilitated Capture The Flag (CTF) events for the New Zealand Cyber Security Challenge, engaging over 500 participants, including high school students, university students, and industry professionals, to enhance their cybersecurity skills and awareness.

Cyber Security Workshop *Amrita School of Engineering, India*

February 2016

- Organized and led a two-day workshop on Ethical Hacking and Cyber Security at Amrita School of Engineering, India, aimed at inspiring students from underprivileged backgrounds to explore opportunities in cybersecurity.