

Kshitij Tapre

+91 9158639011 • [✉ kshitijtapre@gmail.com](mailto:kshitijtapre@gmail.com) • [🌐 https://cv.hznlabs.cc/](https://cv.hznlabs.cc/)
[in https://www.linkedin.com/in/kshitij-tapre-840422a9/](https://www.linkedin.com/in/kshitij-tapre-840422a9/)

Professional Summary

Cybersecurity professional with a foundational background in digital forensics, risk management, and security operations. Experienced in conducting vulnerability assessments (VAPT), evaluating compliance gaps, and developing remediation strategies. Proven track record in IT/ISMS policy development, risk assessment, and mapping controls to regulatory frameworks including ISO 27001, GDPR, and RBI guidelines.

Experience

Center for Cybersecurity and Forensics Education, IIT

Chicago, IL

Research Assistant

Aug 2025 – May 2026

- Developed Digital Twin architecture for IIoT security monitoring using Kubernetes and Docker, detecting MQTT-based anomalies with an 85% detection rate using machine learning models.
- Authored GRC policies for the acceptable use of Large Language Models (LLMs) aligned with the NIST AI Risk Management Framework (RMF).
- Co-authored research evaluating machine learning models for IIoT network intrusion detection, focusing on empirical security testing configurations.
- Designed a structured benchmarking framework to assess and audit LLM-based malware detection capabilities.

CPASS Foundation

Chicago, IL

Instructor for AI Foundations

Oct 2025 – Mar 2026

- Designed and delivered an introductory AI/ML curriculum for 9th–12th grade students, covering Python fundamentals, basic model structures, and data ethics.

LivingThings

Mumbai, MH

Project Lead & Senior Fullstack Developer

Nov 2022 – Dec 2023

- Led an engineering team designing a B2B IoT climate control network deployed across bank ATMs throughout India, ensuring alignment with physical and digital asset security needs.
- Performed Vulnerability Assessment and Penetration Testing (VAPT) across the application stack to identify, assess, and mitigate security risks.
- Audited and updated system architectures to satisfy internal risk management standards and regional financial sector deployment guidelines (RBI).
- Managed secure DevOps CI/CD pipeline migrations, ensuring continuous integration controls and container security protocols were met.

ParishOnNet

Mumbai, MH

Software Developer & Business Analyst

May 2025 – Oct 2025

- Conducted requirements gathering and gap analyses to translate stakeholder business workflows into secure technical specifications.
- Evaluated operational risks during the MVP development phase to verify data handling practices adhered to basic data protection principles.

Zyla Health

New Delhi, DL

Fullstack Developer (Internship)

Mar 2022 – Oct 2022

- Maintained features on a secure chatbot platform for healthcare data management, adhering to strict data privacy requirements.
- Developed secure data extraction pipelines used for behavior analysis while maintaining data integrity controls.

Certifications

EC-Council: Certified Security Analyst (ECSA)

ISC²: Certified in Cybersecurity (CC)

Microsoft: SC-200: Security Operations Analyst

Hack The Box: Certified Bug Bounty Hunter (CBBH)

Google: Cybersecurity Professional Certificate

DeepLearning.AI: Neural Networks and Deep Learning

Skills

Domains: IT Audit, GRC, Risk Assessment, ISO 27001, NIST RMF, VAPT, Application Security, OWASP Top 10, GDPR/DPDP

Tools: Wireshark, Burp Suite, Wazuh, Nmap, Metasploit, Nessus, Microsoft Entra, Git

DevOps/Cloud: AWS, Docker, Kubernetes, GCP, Azure, Terraform, CI/CD pipelines

Languages: Python, JavaScript, C++, Golang, R

Frameworks: React, Node.js, Django, Flask, FastAPI

Projects

DevSecOps Digital Twin: Designed an ontology-driven knowledge graph for semantic reasoning of security vulnerabilities in the SDLC.

AI for Malware Detection: Implemented a machine learning model for JavaScript code deobfuscation to aid in automated static analysis.

Secure LLM Integration: Developed a policy framework for mitigating compliance and data leakage risks when integrating LLMs into corporate environments.

APT Attack Analysis: Analyzed a nation-state cyber attack targeting critical infrastructure, mapping behaviors to the MITRE ATT&CK framework.

Publications

MDPI Applied Sciences (2025): AI-Powered Cybersecurity Models for Training and Testing IoT Devices

Education

Illinois Institute of Technology

MS in Applied Cybersecurity and Digital Forensics, GPA: 3.8 / 4.0

Excellence in Dissertation Research; Outstanding Student of the Year

Chicago, IL

2025

Xavier Institute of Engineering

BE in Computer Engineering, GPA: 7.75 / 10.0

Mumbai, MH

2022