

# Vinayak Banga

+91-9582945571 | [vinyakbanga22@gmail.com](mailto:vinyakbanga22@gmail.com) | [linkedin.com/in/vinayak-banga](https://linkedin.com/in/vinayak-banga) | [github.com/vinayakbanga](https://github.com/vinayakbanga)

Location: Noida, India

## PROFESSIONAL SUMMARY

AI Security Specialist and Cyber Risk Analyst with specialized expertise in \*\*Securing AI Systems\*\*, \*\*Public Cloud Security (AWS)\*\*, and \*\*AI Governance\*\*. Experience in designing controls for Generative AI adoption and engineering Python-based \*\*AI Agents\*\* to automate security workflows. Proficient in conducting AI risk assessments against \*\*ISO 42001\*\* and \*\*NIST AI RMF\*\*, while leveraging deep learning research to understand adversarial threats (Deep Fakes). Bridges the gap between AI development and security compliance to ensure safe adoption of emerging technologies.

## EDUCATION

### Indian Institute of Information Technology (IIIT)

*Master of Technology (M.Tech) in Cybersecurity*  
**Amity University**

*Bachelor of Technology (B.Tech) in Computer Science*

- **Specialization:** Cloud Computing | **CGPA:** 8.79
- **Key Focus:** AI Security, Cloud Security, Threat Modeling, GRC.

Sri City, Andhra Pradesh

2025 – 2027 (Expected)  
Noida, Uttar Pradesh

2020 – 2024

## EXPERIENCE

### Ultimate Kronos Group (UKG)

*Cyber Risk Analyst (Focus: AI & Cloud Risk)*

Noida, India

May 2024 – Present

- **AI Security Engineering:** Designed and deployed an automated "Background Check Agent" using Python and LLMs to enhance security vetting, reducing operational overhead by **70%**.
- **AI Risk Assessments:** Collaborated with Product Security teams to evaluate LLM-driven solutions, identifying risks related to data privacy, prompt injection, and model governance.
- **Cloud & Third-Party Security:** Assessed vendor security controls for public cloud applications against **ISO 27001** and **NIST CSF**, ensuring resilience against supply chain attacks.
- Mapped internal AI controls to **ISO 42001 (AI Management)** to support standardized risk scoring and mitigation planning.
- Automated continuous monitoring workflows using Process Unity, enabling faster incident response and evidence tracking.

### Alameda County Health Care Services Agency

*Software Developer Intern*

San Leandro, CA (Remote)

May 2023 – July 2023

- Built a secure healthcare data system, ensuring strict **IAM (Identity & Access Management)** and data integrity.
- Implemented secure application design principles, improving record access speed by **30%** while maintaining compliance with health data regulations.

Noida, India

### Sopra Steria

*Full Stack Intern*

June 2022 – Sep 2022

- Implemented **JWT (JSON Web Token)** encryption for secure user authentication, preventing session hijacking.
- Optimized web application security headers and API endpoints, reducing vulnerability surface area.

## KEY AI & SECURITY PROJECTS

### Deep Fake Detector (Adversarial AI Defense) | *IEEE Publication, Python, Deep Learning*

2024

- Published research in IEEE Xplore focusing on **AI Threat Detection** and media forensics.
- Developed a model to detect synthetic media usage, directly addressing the challenge of attacker exploitation of AI.

### Secure Serverless Cloud Architecture | *AWS Lambda, API Gateway, IAM, Encryption*

- Architected a secure microservice on AWS, implementing **Least Privilege IAM policies** to control access.
- Configured **Encryption at Rest** (DynamoDB) and In-Transit to secure sensitive data against exfiltration.

## SKILLS & TOOLS

**AI Security & Engineering:** AI Risk Assessment, LLM Security (OWASP Top 10), RAG, Agentic AI, Prompt Injection Defense, Python, TensorFlow

**Cloud Security:** AWS (IAM, Lambda, S3, DynamoDB), Secure SDLC, Encryption Standards, API Security

**Governance & Compliance:** ISO 27001:2022, ISO 42001 (AI), NIST AI RMF, NIST CSF, UK GDPR, Threat Modeling

**Tools:** Process Unity, BitSight, LogicGate, N8N, Burp Suite, Git, VS Code

## CERTIFICATIONS

- CompTIA Security+
- ISC2 Certified in Cybersecurity (CC)
- ISO 27001:2022 Lead Auditor
- AWS Certified Cloud Practitioner
- Cisco Certified Network Associate (CCNA)
- NPTEL: System and Usable Security