High-Income Career with Cybersecurity + AI Skills

(Designed for learners who commented “Cyber Ankur” — from the desk of @ankurdecodes)

1.Why Cybersecurity + AI Is the Highest-Paying Skill Combination Today

In 2025 and the coming decade, the biggest challenge companies face is:

"Who will protect our AI models, data, and systems?"

AI systems are powerful but vulnerable to:

- Data poisoning attacks
- Model theft
- Prompt injection
- Jailbreaking attempts
- Malware created using AI
- Deepfake fraud

Because of this, companies are hiring engineers who understand both AI and cybersecurity — a rare combination.

Salary Range for AI + Cybersecurity Engineers

- India: ₹15 LPA – ₹45 LPA
- USA: $140,000 – $280,000/year
- Remote Global: $90,000 – $220,000/year

These roles are in massive demand in:

- FinTech
- EdTech
- Banks
- AI startups
- Cloud companies
- Cybersecurity firms
- Government & defense

This roadmap will help you become one of these high-income engineers.

2. First Learn the Core Foundations

To protect AI systems, you must understand how AI works and how cyber attacks work.

AI Fundamentals You Must Know

- Machine Learning basics
- Neural networks
- Large Language Models (LLMs)
- Model training & inference
- Embeddings
- RAG systems
- AI deployment basics

Cybersecurity Fundamentals You Must Know

- Networking basics (TCP/IP, DNS, ports)
- Linux commands
- Firewalls & proxies
- Web vulnerabilities (XSS, SQLi, CSRF)
- Authentication & encryption
- OWASP Top 10

These foundations give you the perfect base for advanced learning.

3. Step-by-Step Roadmap to Become an AI Security Specialist

STEP 1: Learn AI + ML Basics (1–2 Months)

Learn:

- Python
- Pandas, NumPy
- ML algorithms
- Neural networks
- Deep learning basics
- Transformers & LLMs

Build mini projects:

- Sentiment model
- Image classifier
- Chatbot

STEP 2: Learn Cybersecurity Fundamentals (1–2 Months)

Study:

- Network security
- Linux/Kali basics
- Vulnerability scanning
- Encryption
- API security

Practice labs on:

- TryHackMe
- HackTheBox
- PortSwigger Academy

STEP 3: Learn AI Security (The Real Skill!) (1–2 Months)

This is where high-paid roles exist.

Learn about attacks on AI models:

- Data poisoning
- Model evasion attacks
- Adversarial attacks (image/text)
- Prompt injection attacks
- Jailbreak vulnerabilities
- Model extraction (stealing model weights)

Learn defenses:

- Red teaming for LLMs
- Prompt hardening
- Secure vector databases
- Safe RAG design

Build mini projects:

- Sentiment model
- Image classifier
- Chatbot

STEP 4: Learn AI Deployment & MLOps (1–2 Months)

To secure AI, you must understand how it is deployed.

Learn:

- Docker
- Kubernetes
- Model pipelines
- API security
- Cloud (AWS / Azure / GCP)

Build:

- A secure LLM API
- A containerized ML model

STEP 5: Master AI + Cybersecurity Tools (1 Month)

AI Tools:

- ChatGPT, Claude, Gemini
- OpenAI Studio
- Vector DBs (FAISS, Chroma)

Cyber Tools:

- Burp Suite
- Nmap
- Wireshark
- Metasploit

Bonus Tip:

Explore all trending AI tools in one place using platforms like Techyuni.com or their Chrome extension — helps you discover free and paid tools instantly.

4. Career Paths for Cybersecurity + AI Engineers

These are the fastest-growing roles in the world right now.

1. AI Security Specialist

Protect AI systems from attacks.

2. LLM Red Team Engineer

Attempt to break AI models to improve safety.

3. AI Security Analyst

Monitor and defend LLM-based applications.

4. AI Risk & Compliance Engineer

Ensure ethical and safe AI deployments.

5. MLOps + Security Engineer

Secure ML pipelines during deployment.

6. AI Product Security Architect

Design secure AI systems for enterprises.

5. Projects You Should Build (Very Important!)

Create projects that prove your value.

- Secure RAG chatbot (defense against prompt injection)
- Adversarial attack detector
- Secure AI API with rate limiting + auth
- LLM behavior monitoring dashboard
- AI red teaming manual + test cases
- AI-based fraud detection system

Upload everything to:

- GitHub
- Portfolio website
- LinkedIn posts

6. Where You Can Get Jobs

Target:

- AI startups
- Cybersecurity companies
- Cloud companies (AWS, Azure, GCP)
- Banks
- FinTech
- Big tech (Google / Meta / OpenAI / Anthropic)

Apply via:

- LinkedIn
- Naukri
- Wellfound (AngelList)
- RemoteOK
- ZipRecruiter

7. 6-Month Fast-Track Learning Timeline

- Month 1: Python + ML basics + networking
- Month 2: Deep learning + Linux + security basics
- Month 3: LLMs + prompt injection + adversarial attacks
- Month 4: MLOps + API security + cloud basics
- Month 5: Real projects + cyber labs
- Month 6: Portfolio + job applications

8. Tips from @ankurdecodes

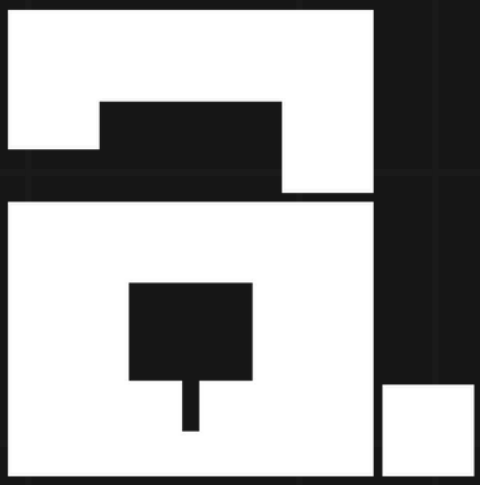
- Don't choose only cybersecurity or only AI — combine both
- Keep practicing on real datasets & cyber ranges
- Study case studies of AI system hacks
- Build projects that show real defense skills
- Stay updated — AI security evolves monthly

9. Your Next Step

You received this roadmap because you commented “Cyber Ankur”. Follow this roadmap with consistency and you can build one of the most powerful and high-paying careers of the future — a skill set that ONLY a few people in the world have.

For more deep insights on AI, cybersecurity, tech careers, and smart tools — follow @ankurdecodes.

Stay safe. Stay smart. Your AI-Cyber journey starts now. 🔐🤖🚀



ANKUR CHANDRAKANT

For more such Valuable Resources

Follow @ankurdecodes