भारतीय सांकेतिक विज्ञान संस्थ हैदराबाद
भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

Program Partner
CyberAI

Secure your seat today to lead the digital frontier

Course Starts on	Course Duration	Registration Ends
02 May 2025	**16 Weeks**	**15 Apr 2025**

Certification Program in AI and Cybersecurity by IIT Hyderabad

The Certification Program in AI and Cybersecurity by IIT Hyderabad is a premier educational offering designed for professionals aiming to excel in the rapidly evolving landscape of cybersecurity and artificial intelligence. This program blends academic rigor with practical industry insights, equipping participants with the knowledge and skills to address real-world challenges in the cybersecurity domain.

In-Person Campus Immersion Experience at IITH

Experience physically the IIT-H campus and AI Dept. over a **2-days itinerary.**

- Network, meet and connect with the faculty members, fellow peers and industry leaders.
- Participate in Ask-Me-Anything (AMA) session with leading experts in cybersecurity and AI.
- Receive the formal certificate during a convocation ceremony at IITH.

www.aicybercourse.ai.iith.ac.in

Program features
Why Choose This Program?

This program stands out for its focus on bridging the gap between theoretical foundations and practical applications. Participants will benefit from:

Practical Applications

Gain hands-on experience with real-world scenarios to build actionable expertise.

Case Studies

Learn through detailed case studies that provide insights into the challenges and solutions implemented by leading organizations.

Live Industry Applications

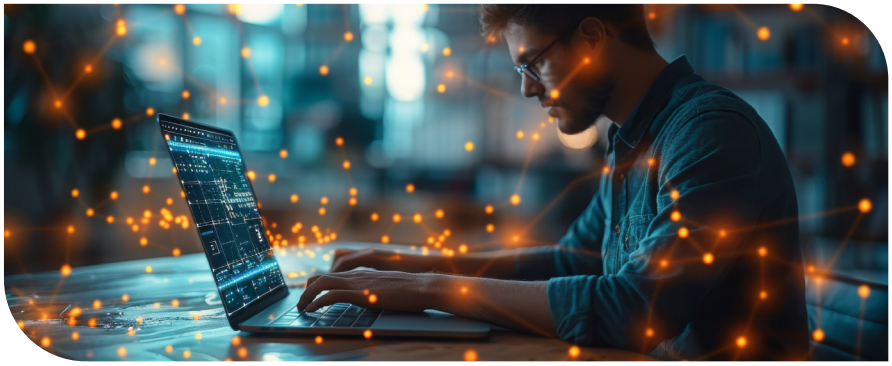
Engage with live applications from top industry experts, enabling you to stay ahead in this dynamic field.

Comprehensive Curriculum

A meticulously curated syllabus that covers key areas of cybersecurity and AI, including threat detection, predictive analytics, and ethical hacking.

Guidance from Renowned Faculty

Learn from esteemed IIT Hyderabad faculty and industry leaders who bring a wealth of knowledge and expertise to the program.



Program Duration

The program spans **4 months**, providing a structured learning experience.

Delivery Mode

The course is delivered **online**, allowing flexible learning from anywhere.

Certification

Upon completion, you will receive a **certificate from IIT Hyderabad**, adding credibility and recognition to your skills.

The clock's ticking!. Join Us

Registration Ends on
15 APR 2025

Course Starts on
02 MAY 2025

Duration
16 Weeks
Online, 8-10 hours a week

Program fee
₹ 75,000 + GST
*Application Fee ₹1000

Course Offerings
Fueling Your Learning Journey

From basics to advanced hacks, here's what you'll master:

Phase 1 — 16 Hours

AI Fundamentals

- **Machine Learning Basics**
  Understand ML types, training methods, feature engineering, metrics (2 Hrs)
- **Deep Learning Essentials**
  Master neural networks, activation functions, loss functions, optimization (2 Hrs)
- **Advanced ML Concepts**
  Learn ensemble methods, transfer learning, DL architectures, evaluation
- **AI Ethics and Bias**
  Understand fairness, bias detection, responsible AI, transparency

Cybersecurity Fundamentals

- **Network Security**
  Master TCP/IP, protocols, network architecture, traffic analysis
- **Security Controls**
  Implement authentication, authorization, access control, policies
- **Threat Landscape**
  Identify attack types, threat actors, vectors, risk assessment
- **Security Operations**
  Execute incident response, log analysis, monitoring, threat intel

Phase 2 — 24 Hours

IDS

- **ML-based IDS Architecture**
  Design ML-IDS architecture, implement detection systems
- **Real-time Detection Systems**
  Build real-time detection, optimize performance
- **Hybrid Detection Approaches**
  Combine multiple detection methods, enhance accuracy

IoT Security

- **Edge Device Protection**
  Secure IoT devices, implement edge protection
- **Lightweight ML Models**
  Deploy efficient models, optimize for constraints
- **Distributed Detection**
  Implement distributed security, coordinate detection

Anomaly Detection

- **Statistical Methods**
  Apply statistical anomaly detection methods

Behavior Analysis

- **User Behavior Analytics**
  Profile user behavior, detect anomalies

Course Offerings
Fueling Your Learning Journey

From basics to advanced hacks, here's what you'll master:

Phase 2 — 24 Hours

Anomaly Detection

- Deep Learning Approaches
  Implement DL-based anomaly detection
- Autoencoder-based Detection
  Use autoencoders for anomaly detection
- Real-time Implementation
  Deploy real-time anomaly detection systems

Behavior Analysis

- System Behavior Profiling
  Monitor system behavior, identify patterns
- Network Behavior Analysis
  Analyze network behavior, detect threats

Biometric Authentication

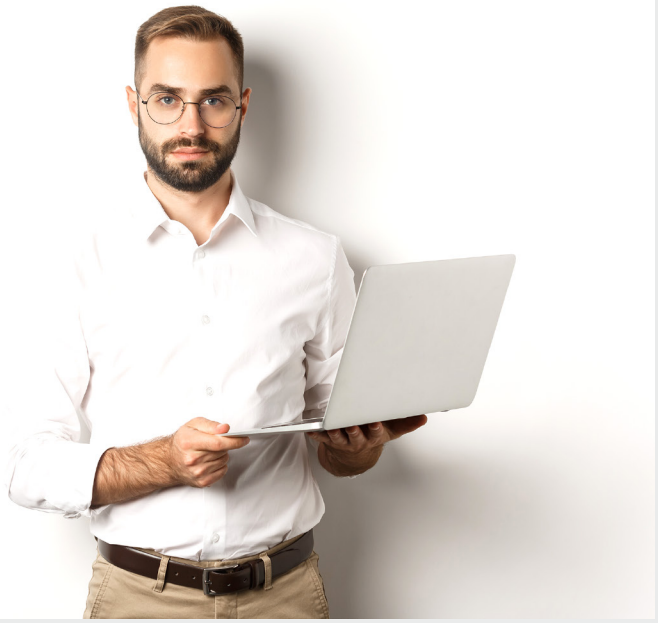
- Facial Recognition
  Implement facial recognition systems
- Multimodal Biometrics
  Combine multiple biometric factors
- Anti-spoofing Techniques

Vulnerability Scanning

- ML-enhanced Scanning
  Improve scanning with ML techniques
- Automated Assessment
  Automate vulnerability assessment
- Risk Prioritization

Supply Chain Attacks

- Software Supply Chain Attacks
  Software Supply chain attacks and how to protect against them
- Performance Optimization
  Optimize system performance



Course Offerings
Fueling Your Learning Journey

From basics to advanced hacks, here's what you'll master:

Phase 3 — 10 Hours

Adversarial Attacks

- White-box Attacks
  Understand and implement white-box attacks
- Black-box Attacks
  Master black-box attack techniques
- Transfer Attacks
  Execute transfer attack methods
- Physical Attacks
  Implement physical adversarial attacks

Data Poisoning

- Training Data Poisoning
  Understand training data poisoning
- Label Flipping
  Implement label flipping attacks
- Backdoor Attacks
  Execute backdoor attack techniques
- Clean Label Attacks
  Master clean label poisoning

Model Extraction

- API-based Extraction
  Extract models via API attacks
- Side-channel Attacks
  Implement side-channel attacks
- Membership Inference
  Execute membership inference attacks
- Architecture Reconstruction
  Reconstruct model architectures

Advanced Attacks

- Model Inversion
  Implement model inversion attacks
- Distillation Attacks
  Execute distillation attacks
- Trojan Attacks
  Implement trojan attack methods
- Privacy Leakage
  Understand privacy leakage attacks

Course Offerings
Fueling Your Learning Journey

From basics to advanced hacks, here's what you'll master:

Phase 4 — 20 Hours

Differential Privacy

- DP Fundamentals
  Master DP concepts and mathematics
- Privacy Budgeting
  Implement privacy budget management
- DP-SGD Implementation
  Deploy DP-SGD in practice
- Privacy Analysis
  Analyze privacy guarantees

Federated Learning

- FL Architecture
  Design FL systems architecture
- Secure Aggregation
  Implement secure aggregation protocols
- Cross-silo FL
  Deploy cross-silo FL systems
- Privacy Guarantees
  Ensure FL privacy guarantees

Robust Defenses

- Input Sanitization
  Implement input sanitization methods
- Model Hardening
  Apply model hardening techniques
- Certified Defenses
  Deploy certified defense methods
- Detection Methods
  Implement attack detection systems

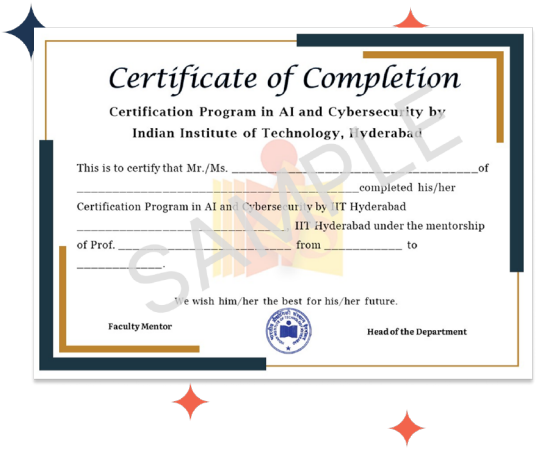
Adversarial Training

- PGD Training
  Execute PGD adversarial training
- Ensemble Training
  Implement ensemble defenses
- Verification Methods
  Apply verification techniques
- Robustness Evaluation
  Evaluate model robustness

Benefits
Certificate Recognition

Elevate your career with the Certification Program in AI and Cybersecurity by IIT Hyderabad. Designed for professionals aiming to excel in the fields of cybersecurity and artificial intelligence, this program offers a comprehensive and hands-on learning experience. Participants will master the skills needed to tackle real-world challenges in network security, threat detection, and AI-driven cybersecurity solutions, paving the way for a rewarding and impactful career.

This program stands out for its focus on practical applications, live industry insights, and advanced tools, making it the ideal choice for professionals ready to advance their expertise.



Industry-Relevant Insights: Benefit from live industry applications and case studies guided by top experts and practitioners.

Prestigious Certification: Earn recognition with a certificate from IIT Hyderabad, enhancing your professional credentials and career prospect

Skill Covered

- Fundamentals of AI
- Core cybersecurity concepts
- Intrusion detection system development and optimization
- IoT security techniques
- Statistical and deep learning for anomaly detection
- Behavior analysis
- Biometric authentication
- Vulnerability scanning and assessment
- Adversarial attack countermeasures
- Data poisoning mitigation
- Model extraction prevention
- Advanced adversarial attack countermeasures
- Differential privacy techniques
- Federated learning
- Robust defense development
- Adversarial training techniques

About CyberAI

Elevate your career with the Certification Program in AI and Cybersecurity by IIT Hyderabad. Designed for professionals aiming to excel in the fields of cybersecurity and artificial intelligence, this program offers a comprehensive and hands-on learning experience. Participants will master the skills needed to tackle real-world challenges in network security, threat detection, and AI-driven cybersecurity solutions, paving the way for a rewarding and impactful career.

This program stands out for its focus on practical applications, live industry insights, and advanced tools, making it the ideal choice for professionals ready to advance their expertise.

OUR VISION

To lead the world in creating a secure digital future by merging Artificial Intelligence and Cybersecurity, empowering professionals to outpace tomorrow's challenges today.

OUR VALUES

- Purpose-Driven Innovation
- Empowerment Through Knowledge
- Integrity in Action
- Excellence for the Future
- Community & Collaboration

OUR MISSION

To equip ambitious minds with cutting-edge skills in AI and cybersecurity. Through hands-on learning, we empower learners to lead the charge in the digital frontier with resilience and innovation.

CyberAI

4th Floor, Tower E,
TRP Building,
IITH, Kandi, Sanga Reddy,
Telangana, 502284