AI Security, Compliance, and Explainability Training (2 Day)

Overview

In this AI course, attendees learn AI's role in various sectors, best practices for system security, and the intricacies of AI design and deployment. Students also explore the AI auditing processes and understand the importance of making AI transparent through explainability techniques. This course is ideal for professionals seeking a straightforward understanding of responsible AI development.

Skills Gained

- Understand the foundational principles of AI ethics and recognize the regulatory standards and compliance requirements for AI across sectors
- Identify threats and challenges associated with AI cybersecurity
- Implement best practices for enhancing the security of AI systems
- Grasp processes and components of AI auditing
- Understand the techniques and challenges related to making AI models transparent and explainable

Who Can Benefit

- AI and Machine Learning Practitioners
- IT Regulatory and Compliance Officers
- Cybersecurity Professionals
- Decision Makers and Executives

Prerequisites

Students should have:

- Foundational Knowledge in AI and Machine Learning
- Familiarity with Data Management
- Basic Cybersecurity Concepts

COURSE OUTLINE

Ethics and Regulation

- Principles of AI Ethics
- Regulatory Compliance in AI Systems
- Case studies of AI non-compliance
- Addressing Regulatory and Compliance

Security and Privacy

- AI Cybersecurity
- Best practices for securing AI systems

Secure AI Design and Deployment

- Best Practices in AI Development
- Bias and discrimination in AI
- Ethical dilemmas in AI deployment

AI auditing and certification

- Organizational roles in AI ethics and compliance
- Implementing AI ethics guidelines and checklists
- Key Components of an AI Audit
- Steps in the AI Auditing

AI Explainability (XAI)

- Basics of Explainable AI (XAI)
- Techniques and methods for explainability
- Generative AI Explainability
- Importance of XAI in various