Cyber Security in AI & ML

By Dr. Vishwanath Rao

1: Introduction to Cybersecurity Basics

- Overview of cybersecurity fundamentals
- Common cybersecurity threats and vulnerabilities
- Importance of cybersecurity in AI and ML applications

2: Introduction to AI and ML

- Basic concepts of artificial intelligence and machine learning
- Applications of AI and ML in various industries
- Potential security risks associated with AI and ML technologies

3: Security Risks in AI and ML Systems

- Data poisoning attacks
- Model evasion attacks
- Adversarial attacks
- Privacy concerns in AI and ML

4: Secure Development Practices

- Secure coding practices for AI and ML systems
- Model validation and verification techniques
- Secure deployment strategies

5: Threat Detection and Prevention

- Intrusion detection systems for AI and ML
- Anomaly detection techniques
- Threat intelligence and threat hunting in AI systems

6: Data Security in AI and ML

- Data encryption techniques
- Secure data storage and transmission
- Data anonymization and de-identification methods

7: Securing AI Infrastructure

- Securing cloud-based AI services
- Containerization and microservices security
- Secure configuration management

8: Compliance and Regulatory Considerations

- Overview of relevant regulations (e.g., GDPR, CCPA)
- Compliance requirements for AI and ML systems
- Ethical considerations in AI and ML security

9: Incident Response and Recovery

- Incident response planning for AI and ML security incidents
- Recovery strategies for compromised AI and ML systems
- Post-incident analysis and lessons learned

10: Future Trends and Advanced Topics

- Emerging threats in AI and ML security
- Advanced techniques for securing AI and ML systems
- Research directions in AI and ML security