



AI Enhanced Cyber Threat

by **Veena K., R. Shalini**

ISBN-13	9789355388247
ISBN-10	9355388241
Edition	First
Format	Both
Publishing Year	2025
Categories	New Arrivals, Book Store, Sathyabama Series
Original Price	₹148.00
Discounted Price	₹125.80
Stock Status	In Stock (5 available)

Description

AI Enhanced Cyber Threat In the rapidly evolving digital landscape. Artificial intelligence (AI) presents a double – edged sword. While it serves as the foundation for next-generation defense systems. It is simultaneously being weaponized by adversaries to create sophisticated, adaptive, and highly evasive cyber threats. AI Enhanced cyber threats offers a vital, comprehensive analysis of this critical intersection. This book meticulously explores the emerging methodologies where Ai and Machine Learning are used to launch automated spear-phishing campaigns, craft polymorphic malware, and bypass conventional security measures. Crucially, it provides IT professionals, security analysis, and researchers with actionable, cutting-edge strategies to counter these advanced threats. From implementing adversarial training to fortify defense models to establishing secure deployment practices in complex IoT and cloud environments, this text is the definitive guide to building an intelligent, resilient, and adaptive cybersecurity posture in the AI age. **Salient Features:**

- **Comprehensive threat analysis:** In-depth exploration of how adversaries utilize AI to automate attacks, enhance phishing efficacy, and deploy adaptive malware.
- **Advanced Mitigation Strategies:** Detailed coverage of AI-powered defense mechanisms, including Adversarial training to improve model resilience against attacks.
- **Real-time security implementation:** Focus on deploying AI-powered anomaly detection systems for continuous, real-time monitoring ongoing compliance in modern infrastructure.
- **Secure IoT and cloud deployment:** best practices for secure configuration of cloud services, network segmentation, and ensuring ongoing compliance in modern infrastructure.

- **Data security fundamentals:** Insights on establishing effective patch management processes and conducting regular security audits and risk assessments.
- **Ideal for:** undergraduate and postgraduate students, researchers, cybersecurity professionals, and network administrators seeking to master the principles of AI-driven security.

About the Author(s)

Veena K.

R. Shalini