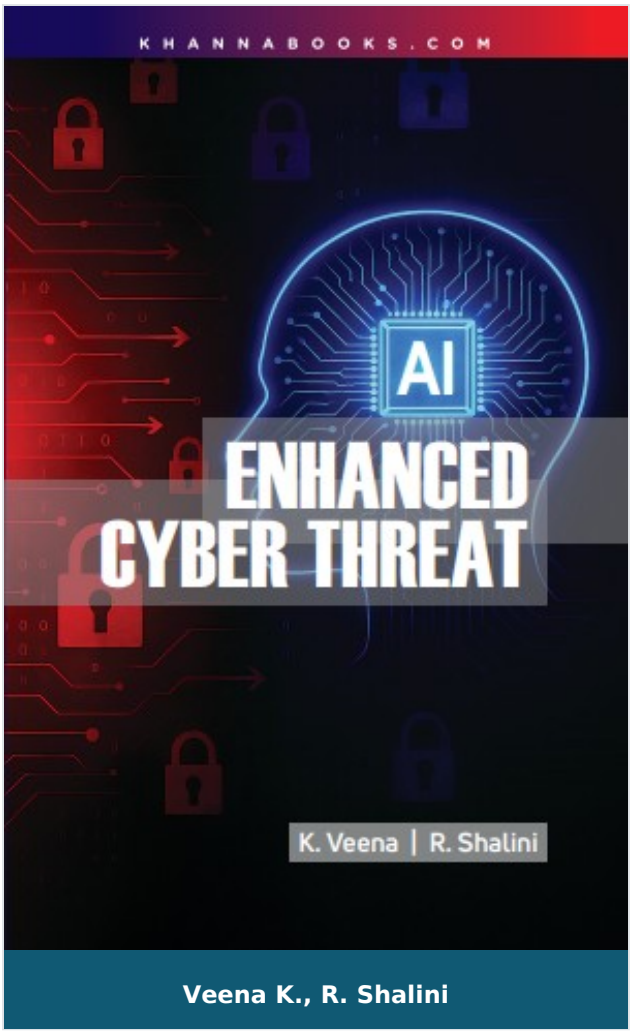


Veena K., R. Shalini

AI Enhanced Cyber Threat

Author :	Veena K., R. Shalini
ISBN 13 :	978-93-55388-24-7
ISBN 10 :	9355388241
E-ISBN 13 :	978-93-55388-24-7
Edition :	First
Pages :	100
Type of book :	Physical
Year :	2025
Language :	English
Publisher :	Khanna Publishing House
M.R.P :	Rs 148.00
Categories :	New Arrivals, Book Store, Sathyabama Series
Condition Type :	New
Country Origin :	India

Khanna Publishing House

4C/4344, Ansari Road, Daryaganj, New Delhi-110002

Email: contact@khannabooks.com | Tel: 011-2324 44 47 - 48 | Mobile: +91-99109 09320

Product 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.

Khanna Publishing House
4C/4344, Ansari Road, Daryaganj, New Delhi-110002
Email: contact@khannabooks.com | Tel: 011-2324 44 47 - 48 | Mobile: +91-99109 09320

- **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 conduction regular security audits and risk assessments.
- I**deal for:** undergraduate and postgraduate students, researchers, cybersecurity professionals, and network administrators seeking to master the principles of AI-driven security.

Khanna Publishing House

4C/4344, Ansari Road, Daryaganj, New Delhi-110002

Email: contact@khannabooks.com | Tel: 011-2324 44 47 - 48 | Mobile: +91-99109 09320

Table Of Contents

- Preface
- Introduction and problem solving
- Fundamentals of cybersecurity
- Impact of AI on cybersecurity
- Secure web and application security
- Cyber threats

Author

Veena K.

Dr. R. Shalini Associate Professor, Dept of CSE, Sathyabama Institute Of Science and technology Dr. K. Veena Associate professor, Dept of CSE, Sathyabama Institute Of science and technology

R. Shalini

Dr. R. Shalini Associate Professor, Dept of CSE, Sathyabama Institute Of Science and technology Dr. K. Veena Associate professor, Dept of CSE, Sathyabama Institute Of science and technology

Khanna Publishing House

4C/4344, Ansari Road, Daryaganj, New Delhi-110002

Email: contact@khannabooks.com | Tel: 011-2324 44 47 - 48 | Mobile: +91-99109 09320