

Artificial Intelligence in Cybersecurity for Risk Assessment and Transparent Threat Detection Frameworks.

Chapter	Title	Page No.
1	Bayesian Deep Learning for Probabilistic Risk Assessment and Attack Surface Reduction in Cyber-Physical Systems	12
2	Hybrid Machine Learning Models Combining Support Vector Machines and Deep Reinforcement Learning for Cyber Risk Profiling	42
3	Graph-Based Risk Analysis Using Graph Neural Networks for Mapping Cyber Threat Propagation in Large-Scale Networks	72
4	AI-Enhanced Attack Graphs Using Markov Decision Processes for Proactive Threat Hunting and Risk Forecasting	107
5	Fuzzy Logic and Evolutionary Computation for Adaptive Cyber Risk Management in Dynamic Cloud Environments	139
6	Convolutional and Transformer-Based Deep Learning Architectures for Real-Time Anomaly Detection in Network Traffic	170
7	AI-Driven SIEM (Security Information and Event Management) Systems Using Long Short-Term Memory (LSTM) for Log-Based Threat Detection	200
8	Generative Adversarial Networks (GANs) for Augmenting Cyber Threat Intelligence and Enhancing Detection of Evasive Malware.	233
9	Reinforcement Learning for Automated Intrusion Detection and Adaptive Defence in Zero-Day Attack Scenarios	263
10	Natural Language Processing-Based AI for Real-Time Phishing and Social Engineering Attack Detection in Email and Messaging Systems	292
11	Transformer-Based Threat Intelligence Frameworks Using BERT and GPT for Dark Web Analysis and Cybercrime Prediction	324

12	Explainable AI (XAI) for Cybersecurity Decision-Making Using SHAP and LIME for Transparent Threat Detection	354
13	Multi-Agent AI Systems for Coordinated Threat Response Using Deep Q-Networks (DQN) and Swarm Intelligence	387
14	Cyber Deception Strategies Using AI-Powered Honeypots and Generative Models for Attacker Behaviour Profiling	423
15	Federated Learning for Distributed Threat Intelligence Sharing Across Global Cybersecurity Networks	456
16	Post-Quantum Cryptography and Quantum Machine Learning for Resilient Encryption in AI-Driven Cybersecurity	489
17	Neural Cryptographic Protocols Using Secure Multi-Party Computation (SMPC) for Encrypted Data Processing in AI-Driven Security Systems	519