

TABLE OF CONTENTS

Chapter No.	Title	Page No.
1	Introduction to AI, ML, and Network Security	1-15
	1.1 Fundamentals of AI and ML	
	1.2 Overview of Network Security Principles	
	1.3 Intersection of AI/ML and Network Security	
	1.4 Case Studies Highlighting AI in Cybersecurity	
2	Data Acquisition and Preprocessing for Network Security	16-26
	2.1 Collecting Network Traffic and Log Data	
	2.2 Data Cleaning and Normalization Techniques	
	2.3 Feature Extraction from Network Data	
	2.4 Handling Imbalanced Datasets in Security Contexts	
3	Machine Learning Techniques in Network Security	27-39
	3.1 Supervised Learning for Intrusion Detection	
	3.2 Unsupervised Learning for Anomaly Detection	
	3.3 Reinforcement Learning in Adaptive Security Systems	
	3.4 Evaluation Metrics for Security-focused ML Models	
4	Deep Learning Applications in Network Security	40-53
	4.1 Convolutional Neural Networks for Packet Analysis	
	4.2 Recurrent Neural Networks for Sequence Modeling	
	4.3 Autoencoders for Anomaly Detection	
	4.4 Generative Adversarial Networks in Security Testing	
5	Ai-Driven Intrusion Detection and Prevention Systems	54-65
	5.1 Designing Intelligent IDS/IPS	
	5.2 Real-time Threat Detection Mechanisms	
	5.3 Integration of AI Models into Existing Security Infrastructure	
	5.4 Performance Optimization and Scalability Considerations	
6	Adversarial Machine Learning in Network Security	66-77
	6.1 Understanding Adversarial Attacks on ML Models	
	6.2 Defense Mechanisms Against Adversarial Threats	
	6.3 Robustness Testing of Security Models	
	6.4 Case Studies on Adversarial ML in Network Security	

7	Ethical, Legal, and Privacy Considerations	78-87
7.1	Ethical Implications of AI in Security	
7.2	Data Privacy Laws and Compliance (e.g., GDPR)	
7.3	Bias and Fairness in Security Algorithms	
7.4	Responsible AI Deployment in Network Security	
8	Emerging Trends and Future Directions	88-98
8.1	AI in IoT and Edge Computing Security	
8.2	Quantum Computing Impacts on Network Security	
8.3	Integration of AI with Blockchain for Security	
8.4	Predictive Analytics for Proactive Threat Management	