CONTENTS

Chapter No.	Title	Page No
I	**Foundations of Cloud Infrastructure and Security**	01-40
	1.1 Introduction to Cloud Computing	
	1.2 Service Models – IaaS, PaaS, SaaS	
	1.3 Deployment Models – Public, Private, Hybrid, Multi-cloud	
	1.4 Shared Responsibility Model for Cloud Security	
	1.5 Cloud Virtualization and Container Security	
	1.6 Cloud Networking and Storage Security Issues	
	1.7 Identity and Access Management (IAM) in Cloud	
	1.8 Threat Landscape – Malware, DDoS, Insider Attacks	
	1.9 Compliance and Regulatory Standards (ISO, GDPR, HIPAA)	
	1.10 Limitations of Traditional Cloud Security Approaches	
II	**Artificial intelligence for cloud security**	41-81
	2.1 Basics of Artificial Intelligence and Machine Learning	
	2.2 Role of AI in Cybersecurity and Cloud Security	
	2.3 Supervised Learning for Threat Detection	
	2.4 Unsupervised Learning for Anomaly Detection	
	2.5 Reinforcement Learning for Adaptive Defense	
	2.6 Natural Language Processing for Log and Threat Intelligence	
	2.7Deep Learning Architectures for Cybersecurity (CNN, RNN, LSTM, GNN)	
	2.8 Security Dataset Preparation and Feature Engineering	
	2.9 Predictive Models for Threat Forecasting	
	2.10 Challenges in AI Adoption for Cloud Security	
III	**AI-driven proactive security mechanisms**	82-130
	3.1 AI-based Intrusion Detection and Prevention Systems	
	3.2 AI for User and Entity Behavior Analytics (UEBA)	
	3.3 Automated Vulnerability Scanning and Patch Management	
	3.4 AI for Malware and Zero-day Threat Detection	
	3.5 Predictive Analytics for Cloud Workload Protection	
	3.6 AI-Enhanced Access Control and Policy Enforcement	

3.7 AI for Cloud Network Monitoring and Traffic Analysis
3.8 Intelligent Encryption and Data Privacy Enhancements
3.9 AI Integration in Cloud-native Security (AWS, Azure, GCP)
3.10 AI-driven Incident Response and Digital Forensics

IV **Adversarial AI and Proactive Defense in Cloud Security** **131-165**
4.1 Adversarial Machine Learning – Concepts and Threats
4.2 Evasion and Poisoning Attacks against AI Models
4.3 AI for Phishing and Social Engineering Defense
4.4 Reinforcement Learning for Proactive Threat Hunting
4.5 Generative AI for Red Teaming and Attack Simulation
4.6Automated Security Orchestration and AI-driven SOAR Platforms
4.7 Edge AI for Cloud-Edge Integrated Security
4.8 Privacy-preserving AI (Federated Learning, Differential Privacy)
4.9 Blockchain-AI Hybrid Models for Cloud Security
4.10 Ethical, Legal, and Governance Issues in AI-driven Security

V **Applications, Case Studies, and Future Trends** **166-195**
5.1 AI in Multi-cloud and Hybrid Cloud Security
5.2 AI for Cloud-native DevSecOps Pipelines
5.3 Case Study: AI-driven Security in AWS Cloud
5.4 Case Study: AI-driven Security in Microsoft Azure
5.5 Case Study: AI-driven Security in Google Cloud
5.6 AI for Cloud-based IoT and Edge Security
5.7 Autonomous AI-driven Cyber Defense Systems
5.8 Sustainable AI Models for Green Cloud Computing
5.9 Future Trends in AI for Proactive Cloud Defense
5.10 Research Challenges and Emerging Opportunities