TABLE OF CONTENTS

Chapter No.	Title	Page No.
1	**Introduction to Cyber Security**	**01-28**
	1.1 Definition, Objectives, and Scope of Cyber Security 1.2 Security Principles: Confidentiality, Integrity, Availability (CIA Triad) 1.3 Types of Cyber Threats and Attacks 1.4 Cyber Security Domains and Ecosystem 1.5 Legal, Ethical, and Social Issues in Cyber Security	
2	**Network Security Fundamentals**	**29-43**
	2.1 Network Architecture and Vulnerabilities 2.2 Firewalls, IDS, and IPS Systems 2.3 Virtual Private Networks (VPNs) 2.4 Secure Socket Layer (SSL) and Transport Layer Security (TLS) 2.5 Denial of Service (DoS) and Distributed DoS Attacks	
3	**Cryptography and Encryption Techniques**	**44-55**
	3.1 Classical and Modern Cryptography 3.2 Symmetric vs. Asymmetric Encryption 3.3 Public Key Infrastructure (PKI) 3.4 Digital Signatures and Certificates 3.5 Hashing Algorithms and Message Authentication Codes	
4	**Operating System and Application Security**	**56-66**
	4.1 OS-Level Security Models and Mechanisms 4.2 Windows and Linux Security Tools 4.3 Secure Coding Principles 4.4 Vulnerability Assessment and Patch Management 4.5 Application-Level Attacks	
5	**Cyber Threat Intelligence and Incident Response**	**67-77**
	5.1 Threat Identification and Analysis 5.2 Cyber Threat Intelligence Lifecycle	

	5.3 Incident Detection and Handling 5.4 Digital Forensics Basics 5.5 Security Information and Event Management (SIEM) Tools	
6	**Cloud and Virtualization Security**	**78-87**
	6.1 Cloud Service Models (IaaS, PaaS, SaaS) 6.2 Cloud Security Architecture and Challenges 6.3 Virtualization Threats and Countermeasures 6.4 Cloud Data Protection and Encryption 6.5 Shared Responsibility Model	
7	**IOT and Mobile Device Security**	**88-97**
	7.1 IoT Architecture and Vulnerabilities 7.2 Embedded Systems and Sensor Network Threats 7.3 Mobile OS Security Models (Android, iOS) 7.4 Mobile App Security Testing 7.5 Security Frameworks for IoT Systems	
8	**Cyber Laws, Ethics, and Governance**	**98-108**
	8.1 IT Act 2000 and its Amendments (India) 8.2 International Cyber Laws and Conventions 8.3 Cyber Crime Investigation Procedures 8.4 Ethical Hacking and Responsible Disclosure 8.5 Privacy Laws and Data Protection (GDPR, HIPAA, etc.)	
9	**Artificial Intelligence and Machine Learning in Cyber Security**	**109-117**
	9.1 Role of AI/ML in Threat Detection 9.2 Predictive Security Analytics 9.3 Automated Intrusion Detection Systems 9.4 Deep Learning for Malware Analysis 9.5 Adversarial Attacks and AI Model Security	
10	**Emerging Trends and Case Studies**	**118-125**
	10.1 Blockchain and Decentralized Security 10.2 Quantum Cryptography 10.3 Zero Trust Architecture 10.4 Cyber Security in Critical Infrastructures 10.5 Real-World Case Studies and Cyber Breach Analysis	