

TABLE OF CONTENTS

Unit No.	Title	Page No.
Part I: Fundamentals of IoT Security		
1	Introduction to IoT and Security Landscape 1.1 Overview of Internet of Things (IoT) 1.2 Architecture and Components of IoT Systems 1.3 Key Security Challenges in IoT 1.4 Threat Modeling and Attack Surfaces	1
2	IoT Communication Protocols and Vulnerabilities 2.1 Overview of IoT Communication Layers 2.2 Common IoT Protocols: MQTT, CoAP, Zigbee, LoRa, 6LoWPAN 2.3 Security Gaps in Communication Channels 2.4 Case Study: Exploiting Weak Encryption in IoT Devices	26
3	Security Requirements and Objectives in IoT Systems 3.1 CIA Triad: Confidentiality, Integrity, Availability 3.2 Authentication and Authorization in IoT 3.3 Data Privacy and Trust Models 3.4 Resilience and Fault Tolerance	51
Part II: Core Security Mechanisms		
4	Cryptography for IoT Security 4.1 Lightweight Cryptography for Constrained Devices 4.2 Symmetric vs. Asymmetric Encryption Techniques 4.3 Key Management in IoT Networks 4.4 Post-Quantum Cryptography Approaches	77
5	Authentication and Identity Management 5.1 Device Identity Lifecycle 5.2 Mutual Authentication and Zero-Trust Models 5.3 Biometric and Blockchain-Based Authentication 5.4 Federated Identity in IoT Ecosystems	96
6	Secure Communication Protocols 6.1 TLS/DTLS for IoT 6.2 End-to-End Encryption (E2EE) 6.3 Secure Routing Protocols 6.4 Certificate and Token-Based Security	115

Part III: Advanced Techniques and Frameworks		
7	Blockchain and Distributed Ledger for IoT Security 7.1 Overview of Blockchain Principles 7.2 Smart Contracts for Device Management 7.3 Consensus Mechanisms for IoT Scalability 7.4 Blockchain Use Cases in IoT Security	145
8	Artificial Intelligence and Machine Learning in IoT Security 8.1 Anomaly Detection using ML Algorithms 8.2 Intrusion Detection Systems (IDS) 8.3 Federated Learning for Privacy-Preserving Security 8.4 Case Studies: AI-driven Threat Prediction	163
9	Fog and Edge Computing Security 9.1 Edge Security Architecture 9.2 Data Protection in Edge Analytics 9.3 Secure Virtualization and Containers 9.4 Trust Management in Distributed Edge Systems	182
10	Quantum-Safe Security for IoT 10.1 Threats of Quantum Computing 10.2 Quantum Key Distribution (QKD) 10.3 Post-Quantum Algorithms for IoT 10.4 Future of Quantum-Resistant IoT	201
Part IV: Security Management and Compliance		
11	IoT Risk Assessment and Threat Modeling 11.1 STRIDE and DREAD Models 11.2 Risk Mitigation Strategies 11.3 Threat Intelligence Sharing Platforms 11.4 Tools for IoT Security Analysis	223
12	IoT Security Testing and Forensics 12.1 Penetration Testing Techniques 12.2 Firmware Reverse Engineering 12.3 Network Forensics and Log Analysis 12.4 Tools and Frameworks for IoT Forensics	229
13	Regulatory Frameworks and Compliance 13.1 Global IoT Security Standards (ISO, NIST, ETSI) 13.2 GDPR and Data Privacy Regulations 13.3 Industry Best Practices and Guidelines 13.4 Security Certification Programs	236

Part V: Emerging Trends and Future Directions		
14	Secure IoT Architectures and Design Patterns 14.1 Security by Design 14.2 Hardware Root of Trust (TPM, HSM) 14.3 Secure Firmware Updates and Over-the-Air (OTA) Mechanisms 14.4 Interoperability and Standardization Challenges	243
15	Case Studies and Real-World Applications 15.1 Smart Home Security 15.2 Industrial IoT (IIoT) Cybersecurity 15.3 Healthcare IoT and Medical Device Protection 15.4 Smart Cities and Critical Infrastructure	249
16	Future Challenges and Research Opportunities 16.1 Autonomous IoT Security Systems 16.2 Integration of 6G and IoT Security 16.3 Ethical and Legal Implications 16.4 Vision for Secure IoT Ecosystem	255
	Appendices Appendix A: IoT Security Tools and Frameworks Appendix B: Common IoT Attack Vectors Appendix C: Glossary of Terms Appendix D: Bibliography and References	260