

TABLE OF CONTENTS

Unit No.	Title	Page No.
1	Foundations of Internet of Things Security 1.1 Evolution and Growth of IoT Systems 1.2 IoT Ecosystem Components and Communication Models 1.3 Security Objectives and Design Principles 1.4 Unique Constraints and Challenges in IoT Security 1.5 Threat Landscape and Attack Surfaces	01-17
2	IoT Architectures and Security Frameworks 2.1 Layered and Service-Oriented IoT Architectures 2.2 Edge, Fog, and Cloud-Based IoT Models 2.3 Security-by-Design Architectural Principles 2.4 Reference IoT Security Architectures 2.5 Comparative Analysis of Architectural Security Models	18-32
3	Threats, Vulnerabilities, and Risk Analysis 3.1 Classification of IoT Threats and Attacks 3.2 Hardware, Firmware, and Software Vulnerabilities 3.3 Network and Protocol-Level Attacks 3.4 Application and Data-Centric Attacks 3.5 Risk Assessment and Threat Modeling Techniques	33-48
4	Cryptographic Techniques for IoT Security 4.1 Role of Cryptography in IoT 4.2 Lightweight Symmetric Encryption Algorithms 4.3 Public Key Cryptography for Resource-Constrained Devices 4.4 Hash Functions, Digital Signatures, and MACs 4.5 Key Management and Distribution Mechanisms	49-61
5	Authentication and Identity Management 5.1 Identity Management in IoT Environments 5.2 Device and User Authentication Mechanisms 5.3 Mutual Authentication Protocols 5.4 Credential Management and Secure Provisioning 5.5 Zero-Trust and Decentralized Identity Models	62-76

6	Access Control and Authorization Models 6.1 Access Control Requirements in IoT 6.2 Role-Based and Attribute-Based Access Control 6.3 Capability-Based and Policy-Based Models 6.4 Context-Aware Access Control 6.5 Enforcement and Scalability Challenges	77-91
7	Secure Communication Protocols 7.1 Overview of IoT Communication Protocols 7.2 Security in MQTT, CoAP, and AMQP 7.3 DTLS and TLS for IoT Networks 7.4 Secure Routing in Low-Power and Lossy Networks 7.5 Protocol Vulnerabilities and Countermeasures	92-107
8	Hardware and Embedded System Security 8.1 Secure Boot and Trusted Firmware 8.2 Hardware Root of Trust 8.3 Physical Attacks and Tamper Resistance 8.4 Secure Firmware Updates and Patch Management 8.5 Side-Channel Attacks and Mitigation Techniques	108-122
9	Data Security, Privacy, and Trust Management 9.1 IoT Data Lifecycle and Security Requirements 9.2 Data Confidentiality, Integrity, and Availability 9.3 Privacy-Preserving Data Collection and Processing 9.4 Trust and Reputation Models 9.5 Regulatory Compliance and Privacy Protection	123-138
10	Network Security and Intrusion Detection 10.1 IoT Network Topologies and Security Issues 10.2 Secure Routing and Traffic Monitoring 10.3 Intrusion Detection and Prevention Systems 10.4 Anomaly and Botnet Detection 10.5 Case Studies of IoT Network Attacks	139-153
11	Artificial Intelligence and Machine Learning for IoT Security 11.1 Role of AI in IoT Security 11.2 Machine Learning-Based Threat Detection 11.3 Deep Learning for Intrusion and Malware Detection	154-168

	11.4 Federated and Distributed Learning Models 11.5 Adversarial Attacks and Model Robustness	
12	Blockchain-Based Security Solutions for IoT 12.1 Fundamentals of Blockchain Technology 12.2 Blockchain-Enabled IoT Security Architectures 12.3 Decentralized Identity and Access Control 12.4 Smart Contracts for Security Automation 12.5 Performance and Scalability Challenges	169-185
13	Security in IoT Applications and Domains 13.1 Smart Home and Consumer IoT Security 13.2 Healthcare and Medical IoT Systems 13.3 Industrial and Manufacturing IoT Security 13.4 Smart Cities and Transportation Systems 13.5 Lessons from Real-World Deployments	186-201
14	Standards, Regulations, and Future Directions 14.1 IoT Security Standards and Frameworks 14.2 Regulatory and Compliance Requirements 14.3 Certification and Interoperability Issues 14.4 Emerging Threats and Research Challenges 14.5 Future Trends in IoT Security	202-217
	Glossary of Terms	218
	Bibliography	221
	Index	223