GUJARAT TECHNOLOGICAL UNIVERSITY
Syllabus for Integrated MSc, 9th Semester
Branch: Computer Science
Subject Name: IOT Security
Subject Code: 1390308

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	ESE (V)	PA (I)	
3	0	2	4	70	30	30	20	150

Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
1	**Introduction to IoT Security:** Overview of IoT: Architecture, Applications, Components, and Ecosystem; Security Challenges in IoT: Scale, heterogeneity, limited resources, and connectivity; Key Security Principles: Confidentiality, Integrity, Availability (CIA triad); IoT; IoT Security Requirements: Authentication, encryption, secure data transmission, privacy.	6	10
2	**IoT Security Threats and Vulnerabilities:** Types of security threats in IoT: Attacks like eavesdropping, spoofing, DoS, man-in-the-middle, etc, Vulnerabilities in IoT devices: hardware, software, network; Case studies of IoT security breaches	6	15
3	**Cryptography and Security Protocols for IoT:** Introduction to Cryptography: Symmetric and asymmetric encryption, hashing algorithms; Security protocols such as SSL/TLS, IPsec and their IoT applications; Lightweight cryptography for IoT devices; Public Key Infrastructure in IoT	9	20
4	**Authentication and Access Control in IoT:** Device Authentication: X.509 certificates, password-based, biometric authentication; Access Control Models: Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC); Implementing secure access to IoT devices and networks using OAuth 2.0; Security of IoT Device Lifecycle	6	15
5	**IoT Security in Cloud and Edge Computing:** Security challenges in cloud-based IoT systems; Edge computing in IoT: Benefits and security considerations; Hybrid architectures and security measures; Data protection, encryption, and secure data storage in cloud and edge	6	15

	environments		
6	**IoT Security Management and Frameworks:** IoT security management lifecycle; IoT security frameworks like NIST and ETSI; IoT security standards and regulations (e.g., GDPR, IoT Cybersecurity Improvement Act)	06	15
7	**Future Trends and Emerging Technologies in IoT Security:** Advances in IoT security technologies such as AI, Blockchain, Machine Learning; Future challenges and innovations in IoT security; Securing 5G-enabled IoT devices	03	10

Reference Books:

1. "IoT Security: Practical Guide for Developers" by John C. G. | Wiley.
2. "Security and Privacy for the Internet of Things" by Fei Hu. | CRC Press
3. "Internet of Things Security: Challenges, Advances, and Applications" by Nadeem Javaid | Springer
4. "IoT Security Issues" by J. E. C. Garcia, R. J. L. Castro, and R. A. M. Garcia | Elsevier
5. "The Internet of Things: A Security Perspective" by Sudhir Kumar Sharma | CRC Press

Course Outcome:

1. Describe the various security challenges faced by IoT systems and the fundamental concepts of IoT security
2. Recognize various security threats, attacks, and vulnerabilities in IoT systems and apply appropriate risk mitigation strategies
3. Implement cryptographic techniques and authentication protocols to secure IoT devices and communication channels.
4. Design and implement secure communication strategies, using protocols like MQTT, CoAP, TLS, and apply network security principles to protect IoT systems.
5. Analyze IoT security breaches and vulnerabilities using case studies and suggest effective countermeasures based on established security standards

List of Experiments:

1) Configure and secure IoT devices (e.g., Raspberry Pi, Arduino) by setting up secure boot, software updates, and user authentication
2) Set up Transport Layer Security (TLS) or Secure Socket Layer (SSL) to secure communication between IoT devices and servers
3) Implement and test OAuth 2.0 for secure authentication and authorization in IoT systems
4) Overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques
5) Use Wireshark to capture and analyze IoT network traffic to detect vulnerabilities and attacks,

such as Man-in-the-Middle (MITM).

6) Simulate Distributed Denial of Service (DDoS) attacks on IoT devices and implement countermeasures to protect against such attacks
7) Implement security features in the MQTT protocol (e.g., using TLS) to secure message transmission between IoT devices and servers
8) Set up a firewall and intrusion detection system (IDS) to monitor and secure IoT networks.
9) Implement data anonymization techniques and encrypt sensitive data stored and transmitted by IoT devices.
10) Use Kali Linux to perform penetration testing on IoT devices and systems to identify and fix vulnerabilities.

List of open-Source software/learning Websites:

- OpenSSL: https://www.openssl.org/
- Wireshark: https://www.wireshark.org/
- Mosquitto (MQTT Broker): https://mosquitto.org/
- Zephyr RTOS: https://www.zephyrproject.org/
- https://owasp.org/www-project-internet-of-things/
- Suricata (IDS/IPS): https://suricata-ids.org/