Subject: Mobile and IOT Security								
Program: M.Sc. in CyberSecurity			**Subject Code:**			**Semester: II**		
Teaching Scheme				**Examination Evaluation Scheme**				
Lecture	**Tutorial**	**Practical**	**Credits**	**University Theory Examination**	**University Practical Examination**	**Continuous Internal Evaluation (CIE)- Theory**	**Continuous Internal Evaluation (CIE)- Practical**	**Total**
4	**0**	**2**	**5**	**40**	**40**	**60**	**60**	**200**

COURSE OBJECTIVES:

- Understand the security risks and challenges associated with mobile and IoT devices and applications.
- Develop skills to perform vulnerability assessments and penetration testing on mobile and IoT environments.
- Learn how to configure secure wireless networks and implement encryption mechanisms for mobile and IoT devices and applications.
- Understand the fundamentals of mobile and IoT malware and how to analyze and detect potential threats.
- Develop skills to investigate and respond to security incidents on mobile and IoT devices and networks.

Content

Course Content

W - Weightage (%) , **T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction to IoT and Mobile Security** • Understanding the IoT ecosystem and its components • Importance of security in IoT and mobile devices • Overview of challenges and vulnerabilities in IoT and mobile environments **IoT Architecture and Protocols** • IoT architecture layers (perception, network, application) • Communication protocols used in IoT (MQTT, CoAP, etc.) • Security considerations at each layer of the IoT architecture	25	6
2	**Mobile Devices in IoT Networks** • Role of mobile devices in IoT ecosystems • Mobile-to-IoT interactions and security implications • Integration of mobile apps with IoT devices and platforms **IoT Device Security** • Security measures for IoT devices (authentication, encryption, access control) • Firmware and software update mechanisms for IoT devices • Secure boot, hardware-based security, and tamper resistance	25	9

3	**IoT Network Security** • Securing IoT communication protocols (TLS/SSL, DTLS) • Threats to IoT networks (DDoS attacks, eavesdropping) and mitigation strategies • Network segmentation and isolation for IoT devices **Mobile App Security for IoT** • Designing secure mobile applications for IoT interactions • Secure coding practices for mobile app development in IoT contexts • API security and data encryption in mobile-to-IoT communications	**25**	**10**
4	**Privacy and Data Protection in IoT and Mobile** • Data privacy concerns in IoT ecosystems • Compliance with data protection regulations (GDPR, CCPA) • Secure handling and storage of sensitive data in mobile and IoT contexts **IoT and Mobile Threat Landscape** • Analysis of common threats and attacks targeting IoT and mobile environments • Case studies of security incidents and breaches in IoT and mobile domains • Vulnerability assessment and risk management in IoT and mobile security	**25**	**10**

TEXTBOOKS:

1. "Mobile Security and Privacy: Advances, Challenges and Future Research Directions" by Man Ho Au, Raymond Choo, and Isaac Woungang
2. "Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations" edited by Fei Hu
3. "IoT Security: Practical Guide Book" by René J. Michotte and Konstantin Mikhaylov
4. "Mobile and IoT Security" by Subramanyam Ranganathan
5. "Securing the Internet of Things: A Standardization Perspective" by Shancang Li and Li Da Xu

List of Practical:

1. Setting up a secure mobile device configuration and hardening the OS and applications.
2. Conduct vulnerability assessments and penetration testing of mobile and IoT devices.
3. Analyzing network traffic on mobile and IoT devices to identify potential security risks.
4. Performing static and dynamic analysis of mobile applications to detect vulnerabilities and potential malware.
5. Implementing encryption and data protection mechanisms for mobile and IoT devices and applications.
6. Configuring secure wireless networks for mobile and IoT devices.
7. Using tools like Wireshark and tcpdump to capture and analyze mobile and IoT network traffic.
8. Configuring virtual private networks (VPNs) and tunneling protocols for secure mobile and IoT communication.
9. Analyzing mobile and IoT malware samples using tools like VirusTotal and Yara.
10. Developing and implementing security policies and procedures for mobile and IoT environments.
11. Configuring secure access controls and authentication mechanisms for mobile and IoT

devices and applications.

12. Configuring firewalls and intrusion detection systems for mobile and IoT networks.
13. Conducting security audits and assessments of mobile and IoT environments using tools like Nmap and Metasploit.
14. Implementing disaster recovery and incident response plans for mobile and IoT environments.
15. Investigating and responding to security incidents on mobile and IoT devices and networks.