17792

BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – M.Tech.(RA)-2024
Course Name – Privacy and Security in IoT
Course Code - MEC30306B
(Semester III)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A

(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) Define cyber-physical system.
a) Cyber model with text inputs
b) Integration of computation with physical processes
c) Standalone wireless router
d) Mobile hotspot with browser

(ii) List components in IoT architecture.
a) Keyboard and monitor
b) Sensors, network, and actuators
c) Mouse and webcam
d) Hub and switch

(iii) Describe effect of Sybil attack in networks.
a) Delays email notifications
b) Creates multiple fake identities
c) Formats memory card
d) Disables LED brightness

(iv) Summarize purpose of Sybil detection.
a) Identify strong signals
b) Detect time drift
c) Validate real node identities
d) Enable screen timeout

(v) Solve malware threat in smart TV.
a) Reduce screen brightness
b) Disconnect from network and scan
c) Increase volume
d) Install extra apps

(vi) Use Merkle trees in blockchain.
a) Verify transactions efficiently
b) Play background audio
c) Display system errors
d) Organize dropdown

(vii) Demonstrate use of TLS protocol.
a) Secure message exchange
b) Compress file size
c) Highlight shortcuts
d) Zoom screen

(viii) Judge security of signature algorithm.
a) Check forgery resistance and integrity
b) Estimate design size
c) Measure pixel value
d) Adjust contrast

(ix) Assess message authentication process.

a) Confirm hash and source
b) Test keyboard
c) Adjust UI zoom
d) Reduce fan

(x) Solve location privacy issue in smart transport.

a) Use location obfuscation techniques
b) Apply barcode login
c) Switch to airplane mode
d) Restart infotainment

(xi) Categorize privacy threats in WBSN.

a) Data leakage, spoofing, identity theft
b) Overheating, lagging, UI freeze
c) Brightness drop, layout glitch
d) Icon deletion, app loss

(xii) Distinguish dissemination with and without privacy.

a) Unprotected sharing reveals identity
b) Privacy mode uses blue light
c) UI display becomes compact
d) LEDs start blinking

(xiii) Apply authentication to smart homes.

a) Use facial recognition or PIN
b) Adjust screen brightness
c) Add text watermark
d) Sort image gallery

(xiv) Use authentication for device pairing.

a) Verify identities before connection
b) Clear sound log
c) Change visual font
d) Rotate 3D object

(xv) Categorize security functions.

a) Animation, updates, history
b) Firewall, IDS, auth, encryption
c) Print, scan, copy
d) Brightness, sound

Group-B

(Short Answer Type Questions) 3 x 5=15

2. List different types of hash functions used in IoT security. (3)

3. Define participatory sensing in the context of IoT. (3)

4. Define authentication in the context of IoT. (3)

5. Analyze the security roles of IoT lower and higher protocol layers. (3)

6. Compare the effectiveness of signature-based and behavior-based intrusion detection in IoT. (3)

OR

Evaluate robustness of Sybil attack detection in vehicular networks. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Define IoT security and outline its key challenges. (5)
8. Evaluate the effectiveness of authenticated encryption in protecting real-time IoT data. (5)
9. Create a privacy-aware participatory sensing framework for urban monitoring. (5)
10. Compare framework-based and ad-hoc approaches for managing trust in IoT systems. (5)
11. Define secure IoT database and explain its core functionalities. (5)
12. Analyze how malware propagates in IoT networks and identify its control methods. (5)

OR

Compare traditional IT network security and IoT network robustness. (5)

****